Introduction to difference algebra and model theory of difference fields

Zoé Chatzidakis (CNRS - Université Paris 7)
Workshop in Orsay, 5-9 December 2011.

Introduction

These notes reflect and complement my talks on introductory material on difference fields, as well as those on groups definable in ACFA. This is the final version. The main algebraic reference is [Co], the main model-theoretic one is [CH].

Updated 15 December 2011.

Things to read:
3.2 is the main tool in proving that certain systems of difference equations have solutions.
3.15 till the end of the section define the rank based on $\downarrow$, give examples and compute some ranks. It also gives the definitions of *internality*, and *modularity*. 3.18 describes the first step of the semi-minimal analysis of a type of finite rank.

Notation

$x, y, z,\ a, b, c$	(finite) tuples of variables, of elements
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$	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
A^s	separable closure of the field A
$K[X_1, \ldots, X_n]_\sigma$	$= K[X_1, \ldots, X_n, X_1^\sigma, \ldots, X_n^\sigma, \ldots, X_i^{\sigma^j}, \ldots]$ = difference polynomial ring in $X_1, \ldots, X_n$
$I(S)$	ideal of polynomials vanishing on the set S
$I_\sigma(S)$	ideal of difference polynomials vanishing on the set S
$I(a/K)$	ideal of polynomials over K vanishing at a
$I_\sigma(a/K)$	ideal of difference polynomials over K vanishing at a
$K(A)_\sigma$	smallest (inversive) difference field containing $K(A)$ $= K(\sigma^i(A) \mid i \in \mathbb{Z})$, with the action of σ
$K(A)_{\sigma+}$	$= K(\sigma^i(A) \mid \imath \in \mathbb{N})$
$\mathrm{acl}(A)$	= model-theoretic algebraic closure of A = smallest algebraically closed inversive difference field containing A.
U^σ	variety conjugate of U under σ
$U(K)$	points of the algebraic set U with their coordinates in K
qf-Diag(E)	set of quantifier-free $\mathcal{L}_\sigma(E)$-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
$\mathrm{Fix}(\tau)$	$\{a \in \mathcal{U} \mid \tau(a) = a\}$
$M \prec N$	M is an elementary substructure of N, $M \equiv_M N$.

1 Difference algebra

Rings are commutative with 1.

1.1. Difference rings. A *difference ring* is a ring R with a distinguished endomorphism σ. It is naturally a structure of the language $\mathcal{L}_\sigma = \{+, -, \cdot, \sigma, 0, 1\}$. A *difference field* is a difference ring which is a field. Note that the endomorphism σ must then be injective, but will not necessarily be onto.

If σ is onto, then we say that R is *inversive*. Every difference ring R is contained in a smallest inversive difference ring R^{inv}, the *inversive hull* of R, which is unique up to R-isomorphism. The difference ring R^1 is the pushout of the diagram

$$\begin{array}{ccc} & & R \\ & & \uparrow \\ \sigma(R) & \hookrightarrow & R \end{array}$$

where the horizontal arrow is the natural inclusion $\sigma(R) \subset R$ and the vertical arrow is the isomorphism σ^{-1}. Thus the pairs $(\sigma(R), R)$ and (R, R^1) are isomorphic via σ^{-1}. The ring R^1 can be defined as the quotient of $R \times R$ by the ideal $I = \{(r, 0) - (0, \sigma(r)) \mid r \in R\}$, the subring R being identified with $(R \times 0) + I$. The map $\sigma^{-1} : R \to R^1$ is then defined by $\sigma^{-1}((r, 0) + I) = (0, r) + I$.
One builds in the same fashion R^2, R^3, etc., and defines $R^{inv} = \bigcup_n R^n$. Since each R^n is isomorphic to R, it follows that any $\forall\exists$ statement true in R will be true in R^{inv}, and in particular:
– If R is a domain, so is R^{inv},
– If R is a field, so is R^{inv}.

A *σ-ideal* of R is an ideal I satisfying $\sigma(I) \subseteq I$. Thus R/I is also a difference ring.

Let I be a σ-ideal. If $\sigma(a) \in I$ implies $a \in I$, then I is a *reflexive* ideal. If for all $n > 0$, $a\sigma(a)^n \in I$ implies $a \in I$, then I is a *perfect ideal*. Note that a perfect σ-ideal is reflexive and radical. A *prime σ-ideal* is a σ-ideal which is prime and reflexive. It follows that a perfect σ-ideal is an intersection of prime σ-ideals.

1.2. Difference polynomial rings. Let R be a difference ring, $X = (X_1, \ldots, X_n)$ a tuple of indeterminate. The difference ring $R[X]_\sigma$ is the polynomial ring over R in the indeterminates $X, X^\sigma, X^{\sigma^2}, \ldots$, where the action of σ is the one suggested by the names of the indeterminates: σ extends σ on K, and sends X^{σ^i} to $X^{\sigma^{i+1}}$.

If $0 \neq f(X) \in K[X]_\sigma$ and $1 \leq i \leq n$, the largest m such that X^{σ^m} appears non-trivially in $f(X)$ is called the *order of $f(X)$ in X_i*.

1.3. Noetherianity? Let K be a difference field, and $X = (X_1, \ldots, X_n)$ be indeterminates. Then the collection of σ-ideals of $K[X]_\sigma$ does not satisfy the ascending chain condition (the ideal $(X_1 X_1^{\sigma^2}, X_1 X_1^{\sigma^3}, \ldots)$ is not finitely generated as a σ-ideal. However, the collection of *perfect* σ-ideals of $K[X]_\sigma$ satisfies the ascending chain condition. (More generally, if R has the acc on perfect ideals, so does $R[X]_\sigma$). This will have consequences for the σ-topology defined below.

1.4. Let $\mathcal{U}$ be a large inversive algebraically closed difference field. In analogy with the Zariski topology on cartesian powers of $\mathcal{U}$, we define the σ-topology, as follows:

A basic *σ-closed* subset of $\mathcal{U}^n$ will be

$$V(I) = \{a \in \mathcal{U}^n \mid f(a) = 0 \ \forall f(X) \in I\} \tag{1}$$

where $I \subset \mathcal{U}[X]_\sigma$.

Note that if $f(a)\sigma(f(a))^m = 0$, then $f(a) = 0$. It follows that if $S \subset \mathcal{U}^n$ and

$$I_\sigma(S) = \{f \in \mathcal{U}[X]_\sigma \mid f(a) = 0 \ \forall a \in S\}$$

then $I_\sigma(S)$ is a perfect σ-ideal. Hence, the σ-topology on $\mathcal{U}^n$ is Noetherian: a strictly decreasing chain of σ-closed subsets of $\mathcal{U}^n$ gives a strictly increasing chain of perfect ideals of $\mathcal{U}[X]_\sigma$.

The usual properties of the Zariski topology immediately generalise to the σ-topology. Irreducible σ-closed sets will correspond to σ-prime ideals; every σ-closed set will have finitely many irreducible components; etc. If $\mathcal{U}$ is existentially closed, there will be a Nullstenllensatz: the correspondence between irreducible closed sets and prime σ-ideals is then a bijection.

From now, all difference fields are inversive. We will work in a large algebraically closed difference field $\mathcal{U}$, which will contain all fields considered.

1.5. Notation. E a difference subfield of $\mathcal{U}$, a an n-tuple of elements of $\mathcal{U}$, $A \subset \mathcal{U}$. Then $E[A]_\sigma$ denotes the inversive difference ring generated by A over E, and $E(A)_\sigma$ the difference field generated by A over E, i.e., $E[A]_\sigma = E[\sigma^i(A) \mid i \in \mathbb{Z}]$, $E(A)_\sigma = E(\sigma^i(A) \mid i \in \mathbb{Z})$. We will also sometimes use non-inversive structures: $E(A)_{\sigma+} = E(\sigma^i(A) \mid i \geq 0)$.

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

We also define an action of σ on the polynomial ring $K[X]$: $f^\sigma(X)$ is the polynomial obtained from $f(X)$ by applying σ to the coefficients of f.

1.6. Transformal transcendence. Let E be a difference subfield of $\mathcal{U}$, and a an element of $\mathcal{U}$. 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 iff all its elements are.

If (the singleton) 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 the inversive closure of $E(X)_\sigma$.

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

1.7. Transformally algebraic elements. Let a be an element of $\mathcal{U}$, E a difference subfield of $\mathcal{U}$, and assume that a is transformally algebraic over E. Let m be least such that some non-zero difference polynomial $f(X) = F(X, X^\sigma, \ldots, X^{\sigma^m})$ is 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 $F^\sigma(\sigma(a), \ldots, \sigma^{m+1}(a)) = 0$, so that the minimal polynomial of $\sigma^{m+1}(a)$ over $E(a, \ldots, \sigma^m(a))$ divides $F^\sigma(\sigma(a), \ldots, \sigma^m(a), Y)$, 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 $E(a, \ldots, \sigma^{n-1}(a))$ must stabilize.

This discussion generalises to finite tuples: let a be a finite tuple of elements of $\mathcal{U}$, which are transformally algebraic over E. Then for some $m > 0$, $\sigma^m(a) \in E(a, \sigma(a), \ldots, \sigma^{m-1}(a))^{alg}$. Furthermore, if $d_m = [E(a, \ldots, \sigma^m(a)) : E(a, \ldots, \sigma^{m-1}(a))]$, then

$$\begin{aligned} d_{m+1} = [E(a, \ldots, \sigma^{m+1}(a)) : E(a, \ldots, \sigma^m(a))] \\ \leq [E(\sigma(a), \ldots, \sigma^{m+1}(a)) : E(\sigma(a), \ldots, \sigma^{m+1}(a))] \\ = [E(a, \ldots, \sigma^m(a)) : E(a, \ldots, \sigma^{m-1}(a))] = d_m. \end{aligned}$$

Hence, the numbers d_m eventually stabilize, and their eventual value is called the *limit degree of a over E*, denoted $\mathrm{ld}(a/E)$.

Replacing σ by σ^{-1} one defines in the same way the *inverse limit degree* of a over E, $\mathrm{ild}(a/E)$, as the eventual value of $[E(a, \ldots, \sigma^m(a)) : E(\sigma(a), \ldots, \sigma^m(a))]$. We also define $deg_\sigma(a/E) = tr.deg(E(a)_\sigma/E)$, the *$\sigma$-degree*. (If a is not transformally algebraic, we set it equal to $+\infty$).

1.8. Exercise. Let E be a difference subfield of $\mathcal{U}$, a a tuple in $\mathcal{U}$ such that $\sigma(a) \in E(a)^{alg}$. Then

(i) $a \in E(\sigma(a))^{alg}$. [Hint: Consider the tr.deg. over E]

(ii)
$$\frac{[E(a, \sigma(a), \sigma^2(a)) : E(a, \sigma(a))]}{[E(a, \sigma(a), \sigma^2(a)) : E(\sigma(a), \sigma^2(a))]} = \frac{[E(a, \sigma(a)) : E(a)]}{[E(a, \sigma(a)) : E(\sigma(a))]} = \frac{\mathrm{ld}(a/E)}{\mathrm{ild}(a/E)}.$$

[Hint: Compute $[E(a, \sigma(a), \sigma^2(a)) : E(\sigma(a))]$ in two different ways.]

(iii) If $b \in E(a)^{alg}$, then $\mathrm{ld}(b/E(a)_\sigma) = \mathrm{ild}(b/E(a)_\sigma)$.

1.9. One can also show that $\mathrm{ld}(a/E)$, $\mathrm{ild}(a/E)$ are invariant of the extension $E(a)_\sigma/E$, i.e., do not depend on the choice of generators of $E(a)_\sigma$ over E, and that limit degrees and inverse limit degrees are *multiplicative in towers* ($\mathrm{ld}(a, b/E) = \mathrm{ld}(a/E)\mathrm{ld}(b/E(a)_\sigma)$). There are also notions of reduced [inverse] limit degrees, by considering the degree of separability instead of the degree.

1.10. Extensions of σ to the algebraic closure of a difference field. Let E be a difference field, and fix some extension of σ to the algebraic closure E^{alg} of E. The other extensions of σ to E^{alg} are of the form $\tau\sigma$, where $\tau \in \mathrm{Aut}(E^{alg}/E)$. Then

$$(E^{alg}, \sigma) \simeq_E (E^{alg}, \tau\sigma) \iff \exists \rho \in \mathrm{Aut}(E^{alg}/E)\ \tau = \rho\sigma(\sigma\rho)^{-1}.$$

1.11. Definition. Let E' be an algebraic extension of E. We say that E' is *finite σ-stable* (over E) if $\sigma(E') = E'$ and $[E' : E]$ is finite. Note that this corresponds to $\mathrm{ld}(E'/E) = 1$ ($= \mathrm{ild}(E'/E)$). If E' is finite σ-stable over E, then so is its normal closure E'' over E, and the σ-stability of E'' does not depend on the extension of σ to E'. This follows easily from the fact that if $\alpha \in E'$, and $P(X) \in E[X]$ is the minimal polynomial of α over E, then $\sigma(\alpha)$ is a root of $P^\sigma(X) = 0$, and $E(\alpha) \models \exists x\ P^\sigma(x) = 0$. Hence the same is true of every E-conjugate of $E(\alpha)$. It follows that the splitting field of $P(X) = 0$ contains all roots of $P^\sigma(X) = 0$, and shows that the normal closure of E' over E is also finite σ-stable.

If M is an algebraic extension of E, define $\mathrm{Core}(M/E)$ to be the union of all finite σ-stable separable extensions of E contained in M. Note that, by the above, if M is normal over E, then $\mathrm{Core}(M/E)$ does not depend on the extension of σ to M.

Theorem. (Babbitt) Two extensions of σ to E^{alg} are E-isomorphic if and only if their restrictions to

Core(E^{alg}/E) are isomorphic.
In particular, if E has no proper finite σ-stable extension, then all extensions of σ to E^{alg} are E-isomorphic.

1.12. Some additional definitions. In model theory, it is convenient to use the language of algebraic geometry à la Weil. Thus our varieties will be defined in terms of coordinates, and defined by polynomial equations. We will use the large algebraically closed difference field $\mathcal{U}$ as a universal domain. Varieties will always be reduced.

If V is a variety defined by a radical ideal $I \subset \mathcal{U}[X]$, then the *field of definition* of V, or of I, is the smallest subfield K of $\mathcal{U}$ such that $I \cap K[X]$ generates I. We use the same notation V for V_K or $V_{\mathcal{U}}$: for us, V is the set of points in the appropriate cartesian power of $\mathcal{U}$ which are annihilated by all elements of I.

In model theory we reach an ambiguity, defined vs definable. So, I will say that V is *defined over* L if L contains the field of definition of V (i.e., $I \cap L[X]$ generates I); we will say that V is *definable over* L if V is the set of elements of $\mathcal{U}$ which are annihilated by all elements of $I \cap L[X]$. The difference between the two notions appears in positive characteristic: if a is transcendental, then the variety $\{a\}$ is definable over $\mathbb{F}_p(a^p)$ but not defined over $\mathbb{F}_p(a^p)$.

A *generic* of the irreducible variety V over a field L (containing the field of definition of V) is a point of V such that $I(a/L) =_{\text{def}} \{f(X) \in L[X] \mid f(a) = 0\}$ equals $I \cap L[X]$. In other words, the specialisation $L[V] \to L[a]$ which sends $X + I(V)$ to a is an isomorphism.

Given a tuple a in $\mathcal{U}$ and the subfield L, we will also speak of the *algebraic locus* of a over L, Locus(a/L), as the variety defined by the ideal $I(a/L)$. Thus, by definition, a will be a generic of Locus(a/L) over L.

The same terminology generalises to the context of difference fields. We will speak of the *field of definition of a difference variety*, of the *diference locus* (Locus$_\sigma$) of a tuple over a difference field, of a *generic of an irreducible difference variety*, and define $I_\sigma(a/E)$.

2 Model theory of difference fields - basic results

2.1. Definition. An *existentially closed (e.c.) difference field* is a difference field K such that every finite system of σ-equations[1] and inequations (over K) which has a solution in some difference field extending K, has already a solution in K. Note that because of the equivalence $x \neq 0 \iff \exists y\ xy = 1$, we can restrict ourselves to systems of σ-equations.

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

(1) K is an algebraically closed field.

(2) σ is an automorphism of K.

(3) If U and V are absolutely irreducible (affine) varieties defined over K, with $V \subseteq U \times U^\sigma$, such that the projections of V to U and to U^σ are dominant, then there is a tuple a in K such that $(a, \sigma(a)) \in V$.

Explanation of the axioms

[1] = difference equations

— σ extends to an automorphism of $K[X]$ which leaves the elements of X fixed. Thus, if $I \subset K[X]$ is the ideal of polynomials defining U, then $\sigma(I)$ defines an absolutely irreducible variety U^σ, with $U^\sigma(\mathcal{U}) = \sigma(U(\mathcal{U}))$.

— 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 (a, b) is a generic of V over K, then a is a generic of U over K, and b a generic of U^σ over K.

One can show that the scheme of axioms (3) is first-order. The property "U an absolutely irreducible variety" is a first-order property (quantifier-free in the language of fields) of the coefficients of a set of polynomials whose vanishing defines U; similarly for the fact that the projection maps are dominant.

2.3. Proof that every difference field embeds in a model of ACFA. 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 a with $(a, \sigma(a)) \in V$.

Let (a, b) be a generic of V over K (recall, we work in $\mathcal{U}$, which in particular is a large algebraically closed field). Then a is a generic of U over K, and b is a generic of U^σ over K. This exactly says that $I(b/K) = \sigma(I(a/K))$, so that σ extends uniquely to a K-isomorphism of fields $\tau : K(a) \to K(b)$ sending a to b. Let $L = K(a, b)^{alg}$. 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, namely a.

We have shown that every instance of axiom (3) is satisfiable in some difference field containing K. Hence, starting from an enumeration of all instances of axiom (3) with coefficients in K, and applying a tower of such constructions, we can build a difference field K^1 containing K, which is algebraically closed, and such that every instance of axiom (3) with coefficients in K has a solution in K^1. Iterating the construction, we find an algebraically closed difference field K^2 containing K^1 and such that every instance of axiom (3) with coefficients in K^1 has a solution in K^2. Etc. Then $\bigcup_{n\in\mathbb{N}} K^n$ is our desired model of ACFA.

2.4. Proof that models of ACFA are e.c.. Assume $K \models$ ACFA, let $f_1(X), \ldots, f_m(X) \in K[X]_\sigma$, and assume that there is a difference field L containing K, and a tuple a in L such that $f_1(a) = \cdots = f_m(a) = 0$. We want to show that there is such an a in K.

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

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

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

Then $\sigma(b) = (\sigma(a), \ldots, \sigma^\ell(a))$ 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 $c \in K^{n\ell}$ such that $(c, \sigma(c)) \in V$. Then c can be written $(d, \sigma(d), \ldots, \sigma^{\ell-1}(d))$. Since $I(c, \sigma(c)/K)$ contains $I(b, \sigma(b)/K)$, we get that $I(d, \sigma(d), \ldots, \sigma^\ell(d)/K)$ contains $I(a, \sigma(a), \ldots, \sigma^\ell(a)/K)$, and therefore that $f_1(d) = \cdots = f_m(d) = 0$.

2.5. Corollaries/Remarks.

(1) The proof of the consistency shows that each instance of axiom (3) can be satisfied in an extension of finite transcendence degree over K. This implies that:

(i) If M is a model of ACFA containing K, and M_0 is the subfield of M generated by all elements of M which are transformally algebraic over K, then M_0 is a model of ACFA, and in fact $M_0 \prec M$, see below.

(ii) To axiomatise ACFA, we may restrict instances of axiom (3) to varieties U, V with $\dim(U) = \dim(V)$. Thus the induced projections are generically finite.

(2) ACFA axiomatises the class of e.c. difference fields (called *difference closed* by Scanlon). This implies that the theory ACFA is model complete, see next paragraph for some explanations. In particular, any inclusion between two models is elementary. It also implies that every formula is equivalent to an existential formula, but we will be able to refine this, see below 3.4.

(3) If $V \subset U \times U^\sigma$ is as in axiom (3), and K is a model of ACFA, then the set of $a \in U(K)$ such that $(a, \sigma(a)) \in V$, denoted $(U, V)^\sharp$ by Scanlon in his talk, is Zariski dense in U.

(4) It was crucial that the variety V is absolutely irreducible, so that we would be sure that any generic of V projects onto a generic of U and onto a generic of U^σ.

2.6. Existentially closed models of an inductive theory. Suppose we have a first-order theory T in a language $\mathcal{L}$, which is *inductive* (i.e., any union of a chain of models is a model; equivalently, which is axiomatised by sentences $\forall\exists$). Within the class $\mathcal{K}$ of all models of T, we consider the subclass $\mathcal{K}_{ec}$ of *existentially closed* structures in $\mathcal{K}$ (a structure K in $\mathcal{K}$ is e.c. if any existential $\mathcal{L}(K)$-formula which is satisfiable in some member of $\mathcal{K}$ containing K, is already satisfiable in K). Since T is inductive, every member of $\mathcal{K}$ is contained in a member of $\mathcal{K}_{ec}$ (exercise: start with K, and build K^1 such that every existential $\mathcal{L}(K)$-formula which has a solution in some structure of $\mathcal{K}$ containing K, has a solution in K^1; etc.).

IF the class $\mathcal{K}_{ec}$ admits an axiomatisation, i.e., if there is some theory T' (containing T) whose models are exactly the members of $\mathcal{K}_0$, then T' is *model-complete*, i.e.: whenever $M \subset N$ are models of T' then $M \prec N$. A consequence of this is that, modulo T', every formula $\varphi(x)$ is equivalent to an existential formula[2]. Equivalently: if T' is model-complete, then every formula $\varphi(x)$ is equivalent to a universal formula. The theory T' is then called the *model companion* of T.

Working with a model complete theory is not quite as good as working with a theory which has quantifier-elimination. But it has still the nice property: if you work inside a large model M, and suddenly decide to enlarge it to a larger model M^*, the validity of first-order formulas is the same in M and in M^*: if $a \in M$, then $M \models \varphi(a)$ if and only if $M^* \models \varphi(a)$.

Some examples. Here are a few examples of theories with $\mathcal{K}_{ec}$ axiomatisable:
Theory of abelian groups, $\mathcal{K}_{ec} = \{\text{divisible abelian groups}\}$,
Theory of fields, $\mathcal{K}_{ec} = \{\text{algebraically closed fields}\}$,
Theory of differential fields of characteristic 0, $\mathcal{K}_{ec} = \{\text{differentially closed fields of characteristic 0}\}$,
Theory of ordered fields, $\mathcal{K}_{ec} = \{\text{real closed fields}\}$ (language of ordered rings).

And here are two examples of theories where $\mathcal{K}_{ec}$ is NOT axiomatisable:
Theory of groups,
Theory of fields with two commuting automorphisms.

[2]Actually, it is not only a consequence, it is an alternate definition of model completeness.

3 Lecture 2 - Model theory of difference field (ctd)

3.1. Theorem. Let K be an algebraically closed difference field. Then ACFA $\cup$ qf-Diag(K) is complete in the language $\mathcal{L}_\sigma(K)$. In other words, if M_1 and M_2 are two models of ACFA which contain K, then they are $\mathcal{L}_\sigma(K)$-elementary equivalent, they satisfy the same $\mathcal{L}_\sigma$-sentences with parameters in K, denoted $M_1 \equiv_K M_2$.

Proof. Consider $M_1 \otimes_K M_2$. Because K is algebraically closed, this is a domain, which contains isomorphic copies of M_1 and M_2. Moreover there is a unique automorphism of $M_1 \otimes_K M_2$ which extends the given automorphisms of M_1 and M_2. Hence the difference domain $M_1 \otimes_K M_2$ is contained in some e.c. M_3. But then we have $M_1 \prec M_3$, $M_2 \prec M_3$, which implies in particular $M_1 \equiv_K M_2$.

3.2. An important property. *Let K be an algebraically closed difference field, and M a model of ACFA containing it, which is sufficiently saturated. Let L be a difference field containing K. Then there is a K-embedding of L inside $\mathcal{U}$.*

Proof. The proof of consistency of ACFA shows that L embeds in some model M_1 of ACFA. By Thm 3.1, we have $M_1 \equiv_K M$. The saturation of M implies that there is a K-embedding of M_1 inside M.

Alternate proof: This follows from the saturation of M. Consider qf-Diag(L). We wish to show that M can be made into a model of this set of $\mathcal{L}_\sigma(L)$-sentences. By compactness, it suffices to consider a finite fragment of it: but a finite fragment will simply be a finite collection of difference equations and inequations with coefficients in K, and such a system, having a solution in L will have a solution in M.

3.3. Definition of types. Let A be a subset of $\mathcal{U} \models$ ACFA, and a a tuple in A. (Usually, we pass to the structure generated by A, and even to the difference subfield generated by A).

(1) The quantifier-free type of a over A, $qftp(a/A)$, is the set of quantifier-free formulas of $\mathcal{L}_\sigma(A)$ (= $\mathcal{L}_\sigma$ with new constants for the elements of A) satisfied by a in $\mathcal{U}$. Thus it is a set of quantifier-free formulas, in some tuple x of variables of the same length as a.

(2) The type of a over A, $tp(a/A)$, is the set of all $\mathcal{L}_\sigma(A)$-formulas satisfied by a in $\mathcal{U}$. Hence it is a set of $\mathcal{L}_\sigma(A)$-formulas, containing ACFA, and which is maximal consistent: if $\varphi(x) \in \mathcal{L}_\sigma(A)$, then either φ or $\neg\varphi$ belongs to $tp(a/A)$, depending on whether $\mathcal{U} \models \varphi(a)$ or $\mathcal{U} \models \neg\varphi(a)$.

(3) The set $S_n(A)$ of all n-types over A (in the n-tuple of variables x) is endowed with a topology, with basic open (and closed) sets $\langle\varphi(x)\rangle_A = \{p \in S_n(A) \mid \varphi(x) \in p(x)\}$, where $\varphi(x) \in \mathcal{L}_\sigma(A)$. Then $S_n(A)$ is compact and Hausdorff for that topology.

(4) A type $p \in S_n(A)$ is *algebraic* if it has only finitely many realisations. It is then an isolated point in $S_n(A)$: there is an $\mathcal{L}(A)$-formula $\varphi(x)$ which together with the elementry diagram of A, implies $p(x)$; we say that φ *isolates* p.

3.4. Corollary. Let K be an algebraically closed difference field.

(1) The completions of ACFA are given by describing the isomorphism type of the algebraic closure of the prime field. For instance, the formula $\exists y\ y^2 = -1 \wedge \sigma(y) = -y$ describes the action of σ on the field obtained by adjoining a square root of -1. It will in particular imply that the fixed field is either of characteristic 2, or does not contain a square root of -1. More examples below.

(2) Let a, b be tuples in $M \models$ACFA. Then

$$tp(a/K) = tp(b/K) \iff K(a)^{alg}_{\sigma} \simeq_K K(b)^{alg}_{\sigma}$$

by a K-isomorphism sending a to b.

(3) $\mathrm{acl}(K) = K$.

(4) Let $\varphi(x)$ be an $\mathcal{L}_\sigma$-formula. Then, modulo ACFA, $\varphi(x)$ is equivalent to a formula $\exists y\ \psi(x, y)$, where $\psi(x, y)$ is quantifier-free, and whenever (a, b) satisfies ψ (in some difference field), then b generates a finite σ-stable extension of the difference field generated by a.

(5) If $\mathcal{U}$ is e.c., then every definable subset of $\mathcal{U}^n$ is of the form $\pi(W)$, where $\pi : \mathcal{U}^{n+m} \to \mathcal{U}^n$ is the projection, W is defined by σ-equations, and $\pi|_W$ has finite fibers.

Proof. (1) Clear from 3.1.

(2) 3.1 tells us that any embedding f of E into another model $\mathcal{U}'$ of ACFA will be an elementary isomorphism, i.e., given a formula $\varphi(x) \in \mathcal{L}$ and a in E, we will have $\mathcal{U} \models \varphi(a)$ iff $\mathcal{U}' \models \varphi(f(a))$. Apply this to the algebraically closed difference field $E = K(a)^{alg}_{\sigma}$, and to a K-isomorphism $f : K(a)^{alg}_{\sigma} \to K(b)^{alg}_{\sigma}$ sending a to b.

(3) Assume that $\alpha \notin K$. Let M be a model of ACFA containing K and α. As in (1), $M \otimes_K M$ embeds into a model N of ACFA, in which there is a new realisation of $tp(\alpha/K)$: thus α cannot be algebraic over K, since otherwise, $tp(\alpha/K)$ would have the same finite number of realisations in any model of ACFA containing K (3.1).

(4) This will be clear from (2), using also 1.11. By compactness, it is enough to show that for each type p (over $\emptyset$) and a realising p in some model M of ACFA, there is a formula $\theta_p(x)$ of the required form which is satisfied by a and implies either $\varphi(x)$ or $\neg\varphi(x)$. Let k be the prime subfield of M. Then Babbitt's theorem and (2) tell us that the isomorphism type of the difference field $\mathrm{Core}(k(a)^{alg}/k(a)_\sigma)$ completely determines $tp(a/\emptyset)$. The isomorphism type of this extension is described by formulas of the required form (see below), and a finite fragment $\theta_p(x)$ will imply φ or its negation. The set of types containing the formula $\varphi(x)$ is covered by finitely many such open sets $\theta_p(x)$, say corresponding to the types $p_1, \ldots, p_r$, and therefore $\varphi(x)$ is equivalent to $\bigvee_{i=1}^{r} \theta_{p_i}(x)$.

(5) Clear from (4).

3.5. Describing the algebraic closure of $E(a)_\sigma$. First of all note that in positive characteristic p, an automorphism σ of a field has a unique extension to its perfect closure: $\sigma(a^{1/p}) = \sigma(a)^{1/p}$.

We have some tuple a, and wish to describe its type over the difference field K. We have already described the K-isomorphism type of $K(a)_\sigma$ via the quantifier-free type of a over K. By Babbitt's theorem, it suffices to describe the isomorphism type of $\mathrm{Core}(K(a)^{alg}_{\sigma}/K(a)_\sigma)$; and to do that, it suffices to describe the isomorphism type of L, for any finite σ-stable Galois extension L of $K(a)_\sigma$.

Take such an L, and write it $L = K(a)_\sigma(\alpha)$; replacing α by some $\sigma^m(\alpha)$, we may assume that the minimal polynomial of α over $K(a)_\sigma$ has its coefficients in $K(a)_{\sigma+}$; let $P(X, Y), Q(X, Y) \in K(X)_\sigma[Y]$ be such that $P(a, Y)$ is the minimal monic polynomial of α over $K(a)_\sigma$, and $\sigma(\alpha) = Q(a, \alpha)$. Thus our formula describing $L/K(a)_\sigma$ (up to conjugation by an element of $\mathcal{G}al(L/K(a)_\sigma)$) is: $\exists y\ P(a, y) = 0 \wedge \sigma(y) = Q(a, y)$ (plus maybe some formulas saying that the denominators appearing in P and Q are non-zero).

3.6. Other remarks. Let E be a difference subfield of $\mathcal{U}$, a a tuple in $\mathcal{U}$.

(1) $qftp(a/K)$, the quantifier-free type of a over E, determines the isomorphism type (over E) of the difference field $E(a)_\sigma$. Indeed, the difference domain $E[a]_{\sigma+}$ is the structure generated by a over E, and therefore its isomorphism type is determined by $qftp(a/E)$. Passing to its field of fractions and to its inversive hull, we get the result.

(2) Babbitt's theorem 1.11 implies that if $E(a)_\sigma$ has no proper finite σ-stable extension, then

$$\text{ACFA} \cup qftp(a/E) \vdash tp(a/E).$$

(3) The proof of (4) is an instance of a general model-theoretic reasoning. Assume that you have a set of formulas Δ which is closed under finite conjunctions. Assume that you can show that every type can be axiomatised (over your original theory T) by formulas in Δ. You can then conclude that every formula is equivalent modulo T to a finite disjunction of formulas in Δ.

We take for Δ, the set of formulas which describe finite σ-stable Galois extensions of the difference field generated by a; since the composite of two finite σ-stable Galois extensions is also finite σ-stable Galois, Δ is closed under conjunctions.

From now on, the difference field $\mathcal{U}$ will be a model of ACFA

3.7. Independence. We already saw in 3.4 that model-theoretic algebraic closure was what we expected it to be: $\text{acl}(A)$ is the field-theoretic closure of the inversive difference field generated by A. We define an independence notion on subsets of $\mathcal{U}$ as follows:
Let $A, B, C \subset \mathcal{U}$. We say that A and B are *independent over* C if the fields $\text{acl}(CA)$ and $\text{acl}(CB)$ are free (or equivalently, linearly disjoint) over $\text{acl}(C)$. We denote it by $A \downarrow_C B$.

3.8. Properties. This independence notion, being based on the independence in ACF, has all the good properties of algebraic independence. In particular it is symmetric, and *transitive*: if $B' \subset B$, then

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

Note also that by definition

$$A \downarrow_C B \iff \text{acl}(C, A) \downarrow_{\text{acl}(C)} \text{acl}(C, B)$$

and that

$$\text{acl}(C, A) = (\text{acl}(C)\text{acl}(A))^{alg}.$$

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 $C \subseteq A \cap B$. Consider the difference domain $A \otimes_C B$: by 3.2, there is a B-embedding of A into $\mathcal{U}$. The image A' of A under this embedding is independent from B over C, and $tp(A'/C) = tp(A/C)$.

Assume that a is a finite tuple, $A \subset B$ are difference subfields of $\mathcal{U}$, with A algebraically closed. Then

$$a \downarrow_A B \iff I_\sigma(a/A)B[X]_\sigma = I_\sigma(a/B).$$

In case A is not algebraically closed, independence can also be expressed in terms of transformal bases and transcendence degrees. Select a transformal transcendence basis b of a over A. Then $a \downarrow_A B$ iff the elements of b remain transformally independent over B, and $deg_\sigma(a/A(b)_\sigma) = deg_\sigma(a/B(b)_\sigma)$.

3.9. Stationarity of non-forking extensions? Recall that if $a \downarrow_A B$ one says *a is independent from B over A*, or *$tp(a/B)$ does not fork over A*, or *is a non-forking extension of $tp(a/A)$*.

Definition. A type (over a set A) is *stationary* if it has a unique non-forking extension to any set containing A.

We saw that in ACF (the theory of algebraically closed fields), if A is algebraically closed, then any type over A is stationary. If A is a field which is not algebraically closed, then $tp(a/A)$ will be stationary if and only $A(a) \cap A^s = A$ (i.e., iff $A(a)$ is a primary extension of A).

In ACFA, types over algebraically closed sets are often non-stationary. The typical example is given by any non-algebraic type realised in the fixed field. More later on that topic.

In analogy, we will say that a quantifier-free type p (over A) is *stationary* if for any B containing A, it has a unique extension to a quantifier-free type over B which does not fork over A. I.e., we request that q is a quantifier-free type over B which contains A and is such that if a realising q, then $a \downarrow_A B$.

Then clearly we have: If $A = \mathrm{acl}(A)$, then any quantifier-free type over A is stationary. If A is a difference field, a a tuple, then $qftp(a/A)$ is stationary in case $A(a)_\sigma$ is a primary extension of A. (This is actually not a necessary condition).

3.10. The independence theorem. There is an important result which allows to circumvent the fact that most types are not stationary.

Theorem. Let $E = \mathrm{acl}(E) \subset A, B \subset \mathcal{U}$, and assume that $A \downarrow_E B$. Let c_1, c_2 be tuples realising the same type over E, with $c_1 \downarrow_E A$ and $c_2 \downarrow_E B$. Then there is $c \downarrow_E AB$ which realises $tp(c_1/\mathrm{acl}(A)) \cup tp(c_2/\mathrm{acl}(B))$.

Proof. Without loss of generality, A and B are algebraically closed difference fields. Replace c_i by $\mathrm{acl}(Ec_i) = C_i$. By hypothesis, there is an E-isomorphism $C_1 \to C_2$ which sends c_1 to c_2.

Let C be a field which is E-isomorphic to C_1, and is free from (AB) over E. This isomorphism gives us an extension σ_1 of $\sigma|_E$ to C, and σ_1 is compatible with $\sigma|_{\mathrm{acl}(AB)}$ (because of the freeness assumptions). One now uses the fact that $(AC)^{alg}(BC)^{alg} \cap (AB)^{alg} = AB$ to extend $\sigma_1 \cup \sigma|_{\mathrm{acl}(AB)}$ to an automorphism σ_2 of $(ABC)^{alg}$ in such a way that the given isomorphism $C_1 \to C$ extends to an isomorphism $((AC_1)^{alg}, \sigma) \to ((AC)^{alg}, \sigma_2)$, and similarly for $(BC)^{alg}$. To do that, if $\varphi_i : C_1 \to C$ was the original E-isomorphism, we just extend $\varphi_i \cup id_A$ to a field isomorphism ψ_1 defined on $(C_1A)^{alg}$; this ψ_1 induces an extension of $\sigma_1 \cup \sigma|_A$ on $(AC)^{Alg}$. One does the same with $(BC)^{alg}$ and verifies that these extensions of $\sigma_1 \cup \sigma|_{\mathrm{acl}(AB)}$ are compatible.

3.11. This result has multiple uses. It allows to define the correct notion of stabilisers of types in a group. It is also used in the proof that any completion of ACFA eliminates imaginaries. An important consequence of elimination of imaginaries is that if $\mathcal{U}$ is a saturated model of ACFA, and $S \subset \mathcal{U}^n$ is $\mathcal{U}$-definable, then there is a tuple a such that S is a-definable, and every automorphism of (the difference field) $\mathcal{U}$ which leaves S invariant, fixes the tuple a elementwise.

Another way of stating the independence theorem, more model-theoretic: let c be a finite tuple. Assume that $p_1(x)$ is a non-forking extension of $tp(c/E)$ to A, and $p_2(x)$ is a non-forking extension of $tp(c/E)$ to B. Then there is a non-forking extension $q(x)$ of $tp(c/E)$ to AB which contains $p_1(x) \cup p_2(x)$.

3.12. Reducts of $\mathcal{U}$. Let $n > 1$ and consider the difference field $(\mathcal{U}, \sigma^n)$. It is a reduct of $\mathcal{U}$, i.e., has less structure than the $\mathcal{L}_\sigma$-structure $(\mathcal{U}, \sigma)$. As $(\mathcal{U}, \sigma)$ is a model of ACFA, so is $(\mathcal{U}, \sigma^n)$. We will denote this reduct by $\mathcal{U}[n]$.

Sketch of proof. Let (M,τ) be difference field containing $(\mathcal{U},\sigma^n)$. One can then show that there is a field N containing M, and $\rho \in \mathrm{Aut}(N)$ such that

$$(M,\tau) \subset (N,\rho^n) \text{ and } (\mathcal{U},\sigma) \subset (N,\rho).$$

As $\mathcal{U}$ is e.c. in N, every system of σ^n-equations over $\mathcal{U}$ having a solution in M has a solution in $\mathcal{U}$. This shows that $\mathcal{U}[n]$ is e.c.

Corollary (char $p>0$). Let $m>0$ and n be integers, and consider $\tau = \sigma^m \mathrm{Frob}^n$. Then $(\mathcal{U},\tau) \models$ ACFA.

Proof. $(\mathcal{U},\tau)$ is definable in $\mathcal{U}[m]$.

3.13. The fixed field(s). Consider $F = \mathrm{Fix}(\sigma) = \{a \in \mathcal{U} \mid \sigma(a) = a\}$, the *fixed field*. As Tom mentionned, this field is pseudo-finite: perfect (if the characteristic is $p>0$, then $F^p = F$); $\mathcal{G}al(F^{alg}/F) \simeq \hat{\mathbb{Z}}$; and F is PAC: every absolutely irreducible variety defined over F has an F-rational point.

Proof. Perfectness is clear. $\mathcal{G}al(F^{alg}/F)$ is topologically generated by σ, so F has at most one extension of degree n for each $n>1$. Considering the difference field extension $\mathcal{U}(t_1,\ldots,t_n)$ of $\mathcal{U}$ where $\sigma(t_i) = t_{i+1}$ for $i<n$, $\sigma(t_n) = t_1$ shows that F has an algebraic extension of degree exactly n.

Consider an absolutely irreducible variety U defined over F, and let V be the diagonal of U. By ACFA, there is $a \in \mathcal{U}$ such that $(a,\sigma(a)) \in V$, i.e., $a \in U(F)$.

Assume that the characteristic is $p>0$, and let τ be as in the corollary above. Then also $\mathrm{Fix}(\tau)$ is pseudo-finite.

3.14. Important properties of fixed fields. Let $F = \mathrm{Fix}(\sigma)$. Proofs can be easily generalised to the other fixed fields. The first thing to notice is that

If K is a difference subfield of $\mathcal{U}$, then F and K are linearly disjoint over their intersection $F \cap K$. So in particular, $F \downarrow_{F\cap K} K$.

Indeeed, we need to show that if $c_1,\ldots,c_n \in F$ are linearly independent in the $F\cap K$-vector space F, they remain linearly independent in the K-vector space FK. We take a minimal n such that there is a counterexample $c_1,\ldots,c_n$ and let $a_1,\ldots,a_n \in K$ such that $\sum_i c_i a_i = 0$, and $a_1 \neq 0$. Wlog, $a_1 = 1$. Applying σ we get the equation $\sum_i c_i \sigma(a_i) = 0$. Substracting this equation from the first one, we get a linear dependence relation of length $\leq n-1$ (since $a_1 = 1 = \sigma(a_1)$), contradiction.

F is stably embedded*, i.e., for every n, every $\mathcal{U}$-definable subset of F^n is definable with parameters from F (and in fact, in the case of* $\mathrm{Fix}(\sigma)$ *or of* $\mathrm{Fix}(\sigma\mathrm{Frob}^n)$ *one can show that it is definable in the pure field language).*

Proof. I told you that every completion of ACFA eliminates imaginaries. Let $S \subset F^n$ be definable. Note that σ is an automorphism of the $\mathcal{L}_\sigma$-structure $\mathcal{U}$ (since it commutes with $\sigma\ldots$), and it leaves S invariant. This implies that it fixes the canonical parameter[3] of the definable set S, i.e., that canonical parameter must be in F.

One of the consequences of stable embeddedness is the following: if $a \in \mathcal{U}$, then $tp(a/F \cap \mathrm{acl}(a)) \vdash tp(a/F)$.

[3]If S is defined by $\varphi(x,a)$, and E is the equivalence relation $E(y,z) : \forall x\ \varphi(x,y) \leftrightarrow \varphi(x,z)$, then the canonical parameter of S, $\ulcorner S \urcorner$, is the E-equivalence class of a.

In a stable theory all definable sets are stably embedded (and even, all sets). The converse is false: stable embeddability does not imply stability!!

3.15. The SU-rank. The definition of independence/non-forking allows one to define a notion of rank, i.e. a fonction from types of tuples to the class of ordinals. The rank of a type p (over a set A), will equal $\mathrm{SU}(a/A)$ for any realisation a of p in $\mathcal{U}$. It is defined by induction:

(i) $\mathrm{SU}(a/A) \geq 0$

(ii) If α is a limit ordinal, then $\mathrm{SU}(a/A) \geq \alpha$ if and only if $\mathrm{SU}(a/A) \geq \beta$ for all $\beta < \alpha$,

(iii) $\mathrm{SU}(a/A) \geq \alpha + 1$ if and only if there is some $A \subset B \subset \mathcal{U}$ such that $a \not\downarrow_A B$ and $\mathrm{SU}(a/B) \geq \alpha$.

Then $\mathrm{SU}(a/A)$ is the smallest ordinal α such that $\mathrm{SU}(a/A) \not\geq \alpha + 1$. There is such an α, and one can show that if m is the transformal transcendence degree of a over $\mathrm{acl}(A)$, then

$$\omega m \leq \mathrm{SU}(a/A) < \omega(m+1).$$

3.16. Examples.
If a is transformally algebraic over A, then one shows easily that $\mathrm{SU}(a/A) \leq deg_\sigma(a/A)$.

Also, if a is a transformally transcendental element, then $\mathrm{SU}(a/A) = \omega$: define by induction $a_1 = \sigma(a) - a$, $a_{i+1} = \sigma(a_i) - a_i$. We get then a descending chain of difference field extensions of A: $A(a)_\sigma \supset A(a_1)_\sigma \supset A(a_2)_\sigma \ldots$, each difference field in this sequence being of transcendence degree 1 over the next one. So, $\mathrm{SU}(a/Aa_i) = i$ for every i, which implies $\mathrm{SU}(a/A) \geq \omega$. On the other hand, if $B \supset A$ is such that $a \not\downarrow_A B$, then $deg_\sigma(a/B) < \infty$, so that $\mathrm{SU}(a/B) < \omega$; this shows that $\mathrm{SU}(a/A) \not\geq \omega + 1$, i.e., $\mathrm{SU}(a/A) = \omega$.

Let us look more closely at types of finite rank, one shows easily:
$\mathrm{SU}(a/A) = 0$ if and only if $a \in \mathrm{acl}(A)$;
$\mathrm{SU}(a/A) = 1$ if and only if $a \notin \mathrm{acl}(A)$, and for every $B \supset A$, either $a \downarrow_A B$, or $a \in \mathrm{acl}(B)$.
Also, we have additivity of the rank: if $\mathrm{SU}(ab/A) < \omega$, then $\mathrm{SU}(ab/A) = \mathrm{SU}(a/A) + \mathrm{SU}(b/Aa)$ $(= \mathrm{SU}(b/A) + \mathrm{SU}(a/Ab))$.
Exercise. Show the following:
if $\sigma^2(a) = a^2$ and $a \notin \mathrm{acl}(E)$, then $\mathrm{SU}(a/E) = 1$,
if $\sigma^2(a) = a + 1$, then one can have $\mathrm{SU}(a/E) = 2$.

3.17. Canonical bases. Let $K \subset L \subset \mathcal{U}$ be (perfect) difference fields, and a a tuple in $\mathcal{U}$. Consider the difference locus of a over L, $\mathrm{Locus}_\sigma(a/L)$, i.e., the σ-closed set defined by the σ-ideal $I_\sigma(a/L)$ of difference polynomials over L which vanish on a. This has a smallest field of definition L_0, i.e., a difference subfield L_0 of L such that $I_\sigma(a/L)$ is generated by its intersection with $L_0[X]_\sigma$. This field is called the *canonical base of* $qftp(a/L)$ (quite a mouthful), denoted (by me) qf-$\mathrm{Cb}(a/L)$.

Its algebraic closure, $\overline{\mathrm{Cb}}(a/L) = \mathrm{acl}(L_0)$ is the smallest algebraically difference subfield L' of $\mathrm{acl}(L)$ satisfying $A \downarrow_{L'} L$. One can use this alternate definition to define $\overline{\mathrm{Cb}}$, so that it makes sense also for infinite tuples.

3.18. Semi-minimal analysis. If $\mathrm{SU}(a/A) < \omega$, one can show that there is some B independent from a over A, and $b \in \mathrm{acl}(Ba)$ such that $\mathrm{SU}(b/B) = 1$. (This is a property of supersimple theories, and can also be showed by hand). This is the start of an analysis of $tp(a/A)$: one can repeat the

procedure with $tp(a/Bb)$, and get a sort of skew tower. Here is a procedure which is less fine, but does not necessitate to increase the base.

Consider $C = \overline{\mathrm{Cb}}(Bb/Aa)$ (as defined just above). So, this is an algebraically closed difference field containing A, and one can show: *For some m, if $B_1b_1, \ldots, B_mb_m$ are independent realisations of $tp(Bb/\mathrm{acl}(Aa))$, then $C \subset \mathrm{acl}(B_1b_1 \ldots B_m, b_m)$.* In fact, for $m = \mathrm{SU}(C/A)$, writing $D = B_1 \cdots B_m$, one has that

$$D \mathop{\smile\!\!\!\!\!\!|}_A a \quad \text{and} \quad \mathrm{acl}(CD) = \mathrm{acl}(Db_1 \ldots, b_m),$$

i.e., C and the tuple $(b_1, \ldots, b_m)$ are equi-algebraic over D.

One then says that $tp(C/A)$ is *almost-internal to the set of A-conjugates of $tp(b/B)$* (quite a mouthful too). If $b \in \mathrm{Fix}(\sigma)$, one says $tp(C/A)$ is almost $\mathrm{Fix}(\sigma)$-internal.

So, we have just found some $C \subset \mathrm{acl}(Aa)$ which is a little special. Iterate the construction until you reach a set which contains $\mathrm{acl}(Aa)$: this is the *semi-minimal analysis of $tp(a/A)$*).

3.19. Modularity/One-basedness. Let $A \subset \mathcal{U}$, and $S \subset \mathcal{U}^n$ be $\mathrm{Aut}(\mathcal{U}/A)$-invariant. Eg, A-definable, or an intersection of A-definable sets, or a union of such. We say that S is *modular* (the usual terminology is *one-based*) if whenever $a_1, \ldots, a_m \in S$, and $A \subset C \subset \mathcal{U}$, then $a_1, \ldots, a_m \mathop{\smile\!\!\!\!\!\!|}_D C$ where $D = \mathrm{acl}(Aa_1 \ldots a_m) \cap C$. In other words, $\overline{\mathrm{Cb}}(a_1 \ldots a_m/C) \subset \mathrm{acl}(Aa_1 \ldots a_m)$.

If p is a type over A, we say that p is modular if the set of its realisations is modular.

3.20. Properties. Assume that p does not fork over $A_0 \subset A$. Then p is modular if and only if $p|A_0$ is modular.

The class of modular sets is stable under union and fibration (if $tp(a/A)$ and $tp(b/Ab)$ are modular, then so is $tp(ab/A)$).

4 Lecture 3 - Groups definable in ACFA

As before we work in a sufficiently saturated e.c. difference field $\mathcal{U}$.

4.1. Definition. A group definable in $\mathcal{U}$ is a definable subset $G \subset \mathcal{U}^n$, together with a definable ternary subset $\Gamma \subset G^3$ which is the graph of a group operation. In particular, for any $x, y \in G$, there are unique z_1, z_2, z_3 in G such that $\Gamma(x, y, z_1) \wedge \Gamma(x, z_2, y) \wedge \Gamma(z_3, x, y)$.

4.2. Theorem (Kowalski-Pillay). G as above, defined over $E = \mathrm{acl}(E)$. There is an algebraic group H, a definable subgroup G_0 of finite index in G, and a definable homomorphism f $G_0 \to H(\mathcal{U})$ with finite kernel, everything being defined over E.

Sketch of proof. Let a_1, a_2, a_3 be generics of G which are independent over E. By generic I mean that we take elements of G which have maximal SU-rank over E. I denote the group operation of G by $\cdot$, the inverse map by $^{-1}$. Now define b_1, b_2, b_3 by $a_1 \cdot a_2 = b_3$, $a_1 \cdot a_3 = b_2$ and $a_2^{-1} \cdot a_3 = b_1$. Then $b_1 = b_2^{-1} \cdot b_3$.

Consider the following triples:
(a_1, a_2, b_3);
(a_1, a_3, b_2);
(a_2, a_3, b_1);
(b_1, b_2, b_3).
Then in any triple, any element is algebraic (in the sense of acl) over E union the other two. E.g., $a_2 \in \mathrm{acl}(E, a_1, b_3)$. For simplicity, I will now assume that $tr.deg(E(a)_\sigma/E) < \infty$, and, replacing the

points $g \in G$ by $(g, \sigma(g), \ldots, \sigma^m(g))$ for some m if necessary, that for all $g \in G$, $\sigma(g) \in E(g)^{alg}$. Thus, working now in ACF, and observing that $\mathrm{acl}(E, a_1, b_2) = E(a_1, b_2)_\sigma^{alg}$ is therefore equals to $E(a_1, b_2)^{alg}$, we now get that in any triple, any element is algebraic (in the sense of field-theoretic algebraic closure) over E union the other two. This gives us what is called a *group configuration* in ACF. A theorem of Hrushovski tells us that there is an algebraic group H defined over E, and independent generics a_1', a_2', a_3' of $H(\mathcal{U})$ such that, setting $b_1' = {a_2'}^{-1} a_3'$, $b_2' = a_1' a_3'$ and $b_3' = a_1' a_2'$, we have

$$E(a_i)^{alg} = E(a_i')^{alg}, \qquad E(b_i)^{alg} = E(b_i')^{alg}$$

for $i = 1, 2, 3$.

We now go back to ACFA and work in the group $G \times H(\mathcal{U})$, with group law denoted by $\cdot$. Let $p = tp(a_1, a_1'/E)$, $q = tp(a_2, a_2'/E)$ and $r = tp(b_3, b_3'/E)$, P, Q, R their sets of realisations. Let us define $S(q, r) = \{(g, g') \in G \times H(\mathcal{U}) \mid \exists (x, x') \in Q, (x, x') \downarrow_E (g, g') \wedge (g, g') \cdot (x, x') \in R\}$. One can then prove that $S(q, r)$ is definable (over E), contains P, and that $S = S(q, r) \cdot S(q, r)^{-1}$ is a group. Quotienting H by $S \cap (1 \times H)$, a finite (central) subgroup of H, and noting that $S \cap (G \times (1))$ is also finite, we obtain that S is the graph of an isogeny from some subgroup G_0 of G to $H(\mathcal{U})$. But, as $(a_1, a_1') \in S$, and a_1 is a generic of G, this subgroup has finite index in G.

In case $\mathrm{SU}(a/E) \geq \omega$, we need to consider infinite tuples instead, but the proof is similar.

4.3. Remark. Assume that $\mathrm{SU}(a/E) = 1$, and $q = tp(a/E)$ is modular non-trivial. I.e.: its set of realisations is modular in the sense defined above, and we can find $a_1, \ldots, a_n$ and a' realising q and such that $a' \in \mathrm{acl}(Ea_1, \ldots, a_n)$ but $a' \notin \mathrm{acl}(Ea_i)$ for any i. Enlarging E by incorporating to it some of the $a_i's$, we may assume that $n = 2$. Let (a_3, a_4) realise $tp(a_1, a_2/\mathrm{acl}(Ea'))$, such that $(a_3, a_4) \downarrow_{Ea'} (a_1, a_2)$. Then $\mathrm{SU}(a_1, a_2, a_3, a_4/E) = 3$, and any three of a_1, a_2, a_3, a_4 are independent over E. We have $\mathrm{acl}(Ea_1a_2) \cap \mathrm{acl}(Ea_3a_4) = \mathrm{acl}(Ea')$, and by modularity, we also have $\mathrm{acl}(Ea_1a_3) \cap \mathrm{acl}(Ea_2a_4) = \mathrm{acl}(Ea_2')$, $\mathrm{acl}(Ea_1a_4) \cap \mathrm{acl}(Ea_2a_3) = \mathrm{acl}(Ea_3')$ for some a_2', a_3' of SU-rank 1 over E. (The computations use the additivity of the SU-rank). We then get a group configuration as above, and therefore a group.

The group configuration is given by the triples:
(a_1, a_2, a_1'); (a_1, a_2', a_3), (a_2, a_2', a_4); (a_1, a_3', a_4); we have two more such triples: (a_1, a_4, a_3') and (a_2, a_3, a_3'). From these we obtain a group (the reasoning is similar to the one in 4.2). From the two additional triples, one can show that the group H has to be abelian.

4.4. Study of definable subgroups of algebraic groups - prolongations. So, from now on, we fix a connected algebraic group G, defined over some $E = \mathrm{acl}(E) \subset \mathcal{U}$.

For each $m \in \mathbb{N}$, we define the group $G_{(m)}$ to be $G \times G^\sigma \times \cdots \times G^{\sigma^m}$, and a group homomorphism $p_m : G \to G_{(m)}$, $g \mapsto (g, \sigma(g), \ldots, \sigma^m(g))$. Observe that $p_m(G)$ is dense in $G_{(m)}$: if $g \in G$ is a generic of G such that the tuples $\sigma^i(g)$, $0 \leq i \leq m$, are algebraically independent over E, then $p_m(g)$ is a generic point of $G_{(m)}$.

Let H be a definable subgroup of G (defined over E). For $m \in \mathbb{N}$, we define $H_{(m)}$ to be the Zariski closure of $p_m(H)$ in $G_{(m)}$. Then $H_{(m)}$ is an algebraic subgroup of $G_{(m)}$, not necessarily connected. We also define

$$\tilde{H}_{(m)} = \{g \in G \mid (g, \sigma(g), \ldots, \sigma^m(g)) \in H_{(m)}\}.$$

The subgroups $\tilde{H}_{(m)}$ form a decreasing sequence of quantifier-free definable subgroups of G containing H, and we let $\tilde{H}$ be their intersection. Since $E[X]_\sigma$ satisfies the ascending chain condition on perfect

σ-ideals, there is an integer m such that $\tilde{H}_{(m)} = \tilde{H}$. Observe that $I_\sigma(H/E) = I_\sigma(\tilde{H}/E)$. If m is such that $\tilde{H} = \tilde{H}_{(m)}$, then

$$SU(H) < \omega \iff deg_\sigma(H) < \infty \iff \dim(H_{(m)}) = \dim(H_{(m+1)}).$$

4.5. There are several equivalent ways of defining generic types in stable groups. However, these notions are in general not equivalent in the context of groups definable in simple theories.

Let H be an E-∞-definable subgroup of G; we will say that $g \in H$ is a *generic* of H (over E) if for every $h \in H$ independent from g over E, gh and h are independent over E. The following observations are immediate:

(1) g and h are independent over E if and only if the tuples $p_m(g)$ and $p_m(h)$ are algebraically independent over E for every $m \in \mathbb{N}$.

(2) g is a generic of H if and only $g \in H$ and $p_m(g)$ is a generic (in the sense of algebraic groups) of $H_{(m)}$ for every $m \in \mathbb{N}$.

(3) g is a generic of H if and only if for every $h \in H$ independent from g over E, hg and h are independent over E.

(4) If H' is a definable subgroup of finite index of H, then any generic of H' is a generic of H. In particular, generics of H are generic in $\tilde{H}$. This implies that $[\tilde{H} : H] < \infty$.

(5) g is a generic of G if and only if g is a generic of the algebraic group G and the tuples $\sigma^m(g)$, $m \in \mathbb{Z}$, are algebraically independent over E.

4.6. Proposition. G has no definable subgroup of finite index.

Proof. Let H be a definable subgroup of finite index of G. Then for every $m \in \mathbb{N}$, $H_{(m)}$ is a definable subgroup of $G_{(m)}$ of finite index, and therefore equals $G_{(m)}$ since $G_{(m)}$ is connected. This shows that H contains generics of G. But, if g is a generic of G, we will show below that $E(g)_\sigma$ has no finite σ-stable extension. Hence $qftp(g/E) \vdash tp(g/E)$ and $H = G$.

Assume that α generates a finite algebraic extension of $E(g)_\sigma$, and let $i < j$ be such that the minimal monic polynomial of α over $E(g)_\sigma$ has its coefficients in $E(\sigma^k(a) \mid i \leq k \leq j)$. Then the minimal polynomial of $\sigma^{j-i+1}(\alpha)$ has its coefficients in $E(\sigma^k(a) \mid j+1 \leq k \leq 2j-i+1)$. As these two fields are free over E, either $\alpha \in E(g)_\sigma$ or $\sigma^{j-i+1}(\alpha) \notin E(g)_\sigma(\alpha)$. This shows that $E(g)_\sigma$ has no proper finite σ-stable extension.

4.7. Theorem. Let G be a simple algebraic group, and H a definable subgroup of G which is Zariski dense in G. Then either $H = G$, or for some $\tau = \sigma^m \mathrm{Frob}^n$ there is an algebraic group G' and an algebraic group isomorphism $f : G \to G'$, a definable subgroup H_1 of finite index in H such that $f(H_1)$ is contained in $G'(\mathrm{Fix}(\tau))$.

Proof. Since every simple algebraic group is isomorphic to one defined over the algebraic closure of the prime field, we may assume that G is defined over the algebraic closure of the prime field. As it suffices to prove the result for the σ^ℓ-closure of H, we may assume that G is defined over $\mathrm{Fix}(\sigma)$ (G is defined over $\mathrm{Fix}(\sigma^\ell)$, work in $\mathcal{U}[\ell]$). We will also assume that H is irreducible for the σ-topology. Consider the algebraic groups $H_{(n)}$, and let ℓ be smallest such that $H_{(\ell)}$ is a proper subgroup of $G^{\ell+1}$ (As H is Zariski dense in G, we know that each $H_{(n)}$ projects onto any of the copies of G). The simplicity of G then implies that $H_{(\ell)}$ is the graph of a group epimorphism $\varphi : G^\ell \to G$ (the product of the first ℓ factors onto the last one), and the minimality of ℓ implies in fact that φ only depends on the first factor, i.e., gives a group isomorphism $G \to G$. So H is defined by $\sigma^\ell(x) = \varphi(x)$. φ is not necessarily an algebraic group isomorphism, since we only know that its graph is algebraic. So it is a constructible

isomorphism, and a fundamental result of the theory of simple algebraic groups says that for some m, n, $\varphi^m = \lambda_h \mathrm{Frob}^n$, where λ_h is conjugation by an element h. Consider the group H' defined by the equation $\sigma^{\ell m}(g) = \varphi^m(g)$; it contains H. Using the axioms for ACFA, there is $u \in G(\mathcal{U})$ such that $\sigma^{\ell m}(u) = h^{-1}\mathrm{Frob}^n(u)$. Then $u^{-1}H'u \subset G(\mathrm{Fix}(\tau))$, where $\tau = \sigma^{\ell m}\mathrm{Frob}^{-n}$.

4.8. Modular groups definable in ACFA.

Theorem. Let G be an algebraic group, H a definable subgroup which is modular, and X a quantifier-free definable subset of G^n. Then $X \cap H^n$ is a Boolean combination of cosets of definable subgroups of H^n. Furthermore, if H is definable over $E_0 = \mathrm{acl}(E_0)$, then all definable subgroups of H^n are definable over E_0.

Proof. (Sketch). We may reduce to the case where H is quantifier-free definable, and irreducible for the σ-topology, and $X \subset H$ is σ-closed ireducible. (Every qf-definable set is a Boolean combination of irreducible σ-closed sets). We assume G, H are definable over some set E_0.

Let E be the smallest algebraically closed difference field over which X is defined and which contains E_0. Let $S = \{h \in H \mid hX = X\}$, fix a generic a of X over E, and a generic g of H over $\mathrm{acl}(Ea)$. Then S is a σ-closed subgroup of H defined over E[4], and $b = ga$ is a generic of H over $\mathrm{acl}(Ea)$. Consider the set $Y = gX$; then b is a generic of Y over $\mathrm{acl}(Eg)$; hence, qf-Cb$(b/\mathrm{acl}(Eg)$ is the field of definition of Y, and by modularity of H, it is contained in $\mathrm{acl}(Eb)$, and therefore in $\mathrm{acl}(Eb) \cap \mathrm{acl}(Eg)$ since Y is definable over $\mathrm{acl}(Eg)$.

Claim. If $\rho \in \mathrm{Aut}(\mathcal{U}/E)$ then $\rho(Y) = Y$ iff $\rho(gS) = gS$.

Proof. Using the fact that X and S are defined over E, we have: $\rho(Y) = Y \iff \rho(g)X = gX \iff g^{-1}\rho(g) \in S \iff \rho(gS) = gS$.

From this one deduces that the fields of definitions of Y and of gS are equi-algebraic over E (and even, equi-definable over E): since every $\rho \in \mathrm{Aut}(\mathcal{U}/E)$ which fixes the canonical parameter of one of the sets fixes the canonical parameter of the other.

Let C be the algebraic closure over E of the canonical parameter of Y. By the remark before the claim, $C \subset \mathrm{acl}(Eb) \cap \mathrm{acl}(Eg)$. From $a \mathop{\smile\!\!\!\!\!\!|}_E b$ and $C \subset \mathrm{acl}(Eb)$ we get $a \mathop{\smile\!\!\!\!\!\!|}_C b$. If $tp(d/Cb) = tp(a/Cb)$, then $qftp(bd^{-1}/Cb) = qftp(g/Cb)$. Let $\rho \in \mathrm{Aut}(\mathcal{U}/Eb)$ which sends a to d. Then $\rho(gS) = gS$ because ρ fixes C, and therefore $bd^{-1} \in gS$, and is generic over C because g was. Now the set of realisations of $tp(a/Cb)$ is dense (for the σ-topology) in X, and this gives $bX^{-1} \subseteq gS$, i.e. applying the inverse map,

$$X \subseteq Sg^{-1}b.$$

But the definition of S and $a \in X$ imply

$$Sa \subseteq X,$$

and therefore $Sa = X$, which is what we wanted to show.

Finally, one can show that all definable subgroups of H are defined over E_0. The element g is a generic of the set gS which, by modularity, is defined over $\mathrm{acl}(E_0 g)$; hence also S is defined over $\mathrm{acl}(E_0 g)$. This being true for any generic g of H, we get that H is defined over E_0.

4.9. Remark. Note that the proof shows that the connected component of the Zariski closure of H must be commutative: the graph of $x \mapsto x^{-1}$ must be a coset of a subgroup. In characteristic 0, the result generalises to arbitray definable X.

[4]This is where we use the fact that X is σ-closed; for a general X, the S obtained with this definition is not necessarily a subgroup.

5 Lecture 4 - Definable subgroups of abelian varieties

We are interested in describing subgroups of Abelian varieties, and determining those which are modular, those which are not. As we saw in the preceding section, definable subsets of modular groups are quite nice.

5.1. Abelian varieties. An abelian variety is a connected algebraic group whose underlying variety is complete and projective. It turns out that the group law is then commutative. Here are some classical results:
Abelian varieties have few endomorphisms (the ring of endomorphisms is finitely generated); If $A \leq B$ are abelian varieties, then A/B is an abelian variety, and there is an abelian subvariety C of B such that $A \cap C$ is finite and $A + C = B$. This means that C and B/A are *isogenous*: the homomorphism $C \to B/A$ (induced by $B \to B/A$) is onto and has finite kernel. An abelian variety is *simple* iff it has no proper abelian subvariety. If A_1, A_2 are simple abelian varieties, then either $\mathrm{Hom}(A_1, A_2) = 0$, or $\mathrm{Hom}(A_1, A_2) \neq (0)$, in which case there is an *isogeny* $f : A_1 \to A_2$, with finite kernel. Any isogeny $f : A \to B$ between two abelian varieties has a ??semi-inverse??, $f' : B \to A$ such that, if $n = \deg(f)$, then $f \circ f' = [n]_B$ and $f' \circ f = [n]_A$ (multiplication by n in B and A respectively). It follows that if A is a simple abelian variety, then $E(A) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ is a division ring. Every abelian variety is isogenous to a direct product of finitely many simple abelian varieties. If $\mathrm{Hom}(A, B) = (0)$, then every connected algebraic subgroup of $A \times B$ is of the form $A_1 \times B_1$ where $A_1 \leq A$ and $B_1 \leq B$.

A references is to S. Lang's book on abelian varieties chapter II.

The study of definable subgroups of abelian varieties reduces to the study of those of simple abelian varieties, and then to the study of the "minimal ones".

5.2. Notation and definitions. Let A and B be abelian varieties. We denote by $\mathrm{Hom}_\sigma(A, B)$ the group of definable (in ACFA) homomorphisms from A to B, by $\mathrm{End}_\sigma(A)$ the ring of definable (in $ACFA$) endomorphisms of A, and set $E_\sigma(A) = \mathbb{Q} \bigotimes \mathrm{End}_\sigma(A)$.

If $f \in \mathrm{Hom}_\sigma(A, B)$, we denote by $\sigma(f)$ the element of $\mathrm{Hom}_\sigma(A^\sigma, B^\sigma)$ with graph the image by σ of the graph of f. Note that $\sigma(f) = \sigma f \sigma^{-1}$, and that if $f \in \mathrm{Hom}(A, B)$, then $\sigma(f) \in \mathrm{Hom}(A^\sigma, B^\sigma)$.

We will say that $f \in \mathrm{Hom}_\sigma(A, B)$ is a *definable isogeny* if it is onto and its kernel is finite.

We say that two subgroups B and C of A are *commensurable*, written $B \sim C$, if $B \cap C$ is of finite index in B and in C. We write $C \lesssim B$ if $C \cap B$ is of finite index in C.

Observe that $\sim$ is an equivalence relation on subgroups of A.

A definable subgroup B of A is *c-minimal* iff every definable subgroup of B is either finite or of finite index in B.

5.3. Lemma. Let A, B be abelian varieties.

(1) Assume that $\mathrm{Hom}(A, B^{\sigma^m}) = (0)$ for every $m \in \mathbb{N}$. Then every definable subgroup C of $A \times B$ is commensurable with a subgroup of the form $C_1 \times C_2$, with C_1 a definable subgroup of A, C_2 a definable subgroup of B. We also have $\mathrm{Hom}_\sigma(A, B) = (0)$ and $\mathrm{End}_\sigma(A \times B) = \mathrm{End}_\sigma(A) \times \mathrm{End}_\sigma(B)$.

(2) Assume that A and B are isogenous. Then $E_\sigma(A) \simeq E_\sigma(B)$.

(3) Let $A_1, \ldots, A_m$ be simple abelian subvarieties of A such that A and $A_1 \times \cdots \times A_m$ are isogenous. Renumbering if necessary, assume that $\{A_1, \ldots, A_n\}$ is maximal such that for all $i \neq j$ and

$k \in \mathbb{N}$, A_i and $A_j^{\sigma^k}$ are not isogenous, and for each $i \leq n$ let $m(i)$ be the number of indices $j \leq m$ such that A_j and $A_i^{\sigma^k}$ are isogenous for some $k \in \mathbb{Z}$. Then

$$E_\sigma(A) \simeq \prod_{i=1}^{n} M_{m(i)}(E_\sigma(A_i)).$$

Proof. (1) Let C be a definable subgroup of $A \times B$. Without loss of generality, C is quantifier-free definable and is connected for the σ-topology (since C is commensurable with $\tilde{C}^0$). Let m be such that $C = \tilde{C}_m$. Then $C_{(m)}$ is a proper subgroup of $A \times B \times A^\sigma \times \cdots \times A^{\sigma^m} \times B^{\sigma^m} \simeq A_{(m)} \times B_{(m)}$. Our hypothesis implies that $\mathrm{Hom}(A_{(m)}, B_{(m)}) = (0)$, and therefore $C_{(m)} = C_1 \times C_2$ where $C_1 \leq A_{(m)}$, $C_2 \leq B_{(m)}$, from which the result follows.

The other items are proved in a similar fashion.

5.4. Theorem. Let A be a simple abelian variety and assume that for every $m > 0$, A and A^{σ^m} are not isogenous. Then A has no proper infinite definable subgroup, and $E_\sigma(A) = E(A)$.

Proof. Every proper subgroup C of $A_{(m)}$ is commensurable to a product of some of the factors; hence, if $C \neq A_{(m)}$, then $p_m^{-1}(C) = (0)$.

Let $f \in E_\sigma(A)$ be non-zero. Multiplying it by $[n]$, we may assume it is in $\mathrm{End}_\sigma(A)$. Let S be its graph, a definable subgroup of $A \times A$, and consider $S_{(m)}$, $\tilde{S}_m$. By the above, $S_{(m)}$ has to be of the form $C_0 \times \cdots \times C_m$ where each C_i is an algebraic subgroup of $A^{\sigma^i} \times A^{\sigma^i}$ of dimension $\dim(A)$ and which projects onto each of the factors; moreover $C_i = C_0^{\sigma^i}$: this is because S is Zariski dense in C_0, and therefore S^{σ^i} is Zariski dense in C_i. From this one deduces that S is the graph of some element of $E(A)$ (thought of as a finite-to-finite isogeny).

5.5. Theorem. Let A be a simple abelian variety, and assume that for some $n > 0$ A and A^{σ^n} are isogenous. Take the least such n, and fix two isogenies $h : A \to A^{\sigma^n}$ and $h' : A^{\sigma^n} \to A$, with $h'h = [m]$ and $hh' = [m]$ (if $A = A^{\sigma^n}$, it is natural to choose $h = h' = id_A$). Then $\tau = h'\sigma^n$ and $\tau' = \sigma^{-n}h$ are in $\mathrm{End}_\sigma(A)$, and $\tau'\tau = \tau\tau' = [m]_A$. Thus τ and τ' are invertible in $E_\sigma(A)$.

(1) The ring $E_\sigma(A)$ is generated over $E(A)$ by τ and τ'. It is naturally isomorphic to the twisted Laurent polynomial ring $E(A)^t[\tau, \tau^{-1}]$, with τ acting on $E(A)$ by conjugation, and $\tau^{-1} = [1/m]\tau'$. Thus it admits a natural $\mathbb{Z}$-grading.

(2) Let B be a definable subgroup of A^k. Then B is commensurable with a finite intersection of kernels of definable homomorphisms $A^k \to A$. If $k = 1$, a single endomorphism suffices, and either $B = A$ or B has finite rank.

(3) Let f be a non-zero element of $\mathrm{End}_\sigma(A)$. Then f is onto and $\ker(f)$ has finite rank. Also, f is invertible in $E_\sigma(A)$ if and only if $\ker(f)$ is finite if and only if f is a homogeneous element of the graded ring $E_\sigma(A)$ (that is, of the form $a\tau^k$ for some $k \in \mathbb{Z}$ and $a \in E(A)$).

(4) The definable subgroup B is c-minimal if and only if it is commensurable with $\ker(f)$, f an element of $\mathrm{End}_\sigma(A)$ irreducible in $E_\sigma(A)$.

5.6. Comments. I am not going to do the proof, it is long and very well done in the original paper [H]. An interesting step in the proof shows that $\ker(f) \lesssim \ker(g)$ if and only if there is $h \in E_\sigma(A)$ such that $g = hf$. From this one deduces that every definable subgroup B of A is commensurable to some

$\ker(f)$ with $f \in \mathrm{End}_\sigma(A)$. ($f = 0$ if $B = A$). This shows that an abelian variety has only countably many definable subgroups.

One can show the following result: Let $0 \to B_1 \to B_2 \to B_3 \to 0$ be a short exact sequence of definable groups. Then B_2 is modular if and only if B_1 and B_3 are modular. So this reduces the study of modular subgroups to c-minimal ones.

5.7. Theorem (ACFA, char. 0). Let A be a simple abelian variety, and B a c-minimal subgroup of A. Let $F = \mathrm{Fix}(\sigma)$ denote the fixed field of σ.

(1) Precisely one of the following happens:

   (a) $B = A$.

   (b) B is modular, of SU-rank 1.

   (c) B is definably isogenous to a subgroup of finite index of $H(F)$, H an algebraic group defined over F.

(2) Case (a) occurs if and only if A and A^{σ^n} are not isogenous for any $n > 0$.

(3) If (c) holds, then A is isomorphic to an abelian variety A' defined over $\mathrm{Fix}(\sigma^m)$ for some m.

Assume that A is defined over $\mathrm{Fix}(\sigma)$.

(4) B is not modular if and only if $B \subseteq \ker(\sigma^M - 1)$ for some $M > 0$ divisible by m.

Proof. (2) Assume that A is not isogenous to A^{σ^n} for any $n \in \mathbb{N}^*$. Then A has no proper definable subgroups (since it is simple), and therefore $B = A$.

Conversely, if A^{σ^n} and A are isogenous for some $n \in \mathbb{N}^*$, then $\mathrm{End}_\sigma(A)$ has a non-homogeneous element g. Then $\ker(g)$ is a proper definable infinite subgroup of A, which shows that A is not c-minimal. This proves (2).

Assume therefore that A is isogenous to A^{σ^n} (n positive and least such).

If B is modular, then its c-minimality implies $SU(B) = 1$.

Assume that B is not modular. We want to show (1)(c) and (3).

Claim. The generics of B are non-orthogonal to the formula $\sigma(x) = x$.

Proof. Some element $a \in B$ realises a type (over some $E = \mathrm{acl}(E)$) which is non-orthogonal to $\mathrm{Fix}(\sigma)$ and has rank 1; so this means: there is a tuple c, with $c \downarrow_E a$, such that $E(c, a)_\sigma$ contains some element b with $\sigma(b) = b$, and $a \in E(c, b)_\sigma^{alg}$[5]. There is a first-order formula in $\mathcal{L}_\sigma(E)$ which expresses this fact, and therefore there is a definable set $D \subset B$ containing a and such that every element in D realises a type of rank 1 which is non-orthogonal to $\sigma(x) = x$. The σ-closure of the definable set $a^{-1}D$ then generates in finitely many steps a definable subgroup of B, which by c-minimality must be commensurable with B. (This is an ACFA analogue of the result for algebraic irreducible varieties containing 0 and is proved in the same fashion).

Then B has a definable subgroup C such that B/C is infinite and internal to F (that is, there is a definable map from some power of F onto B/C). By c-minimality of B, C is finite.

Elimination of imaginaries implies that B/C is isogenous to $H(F)$, where H is an algebraic group defined over F. So we get a definable homomorphism $h : B \to H(F)$ with finite kernel. Then $h(B)$

[5]You can take this as a definition of non-orthogonality to $\mathrm{Fix}(\sigma)$

is c-minimal, and we may assume that H is the Zariski closure of $h(B)$, which implies that H is an abelian variety, A'. Hence $\mathrm{Hom}(A, A'^{\sigma^\ell}) \neq (0)$ for some ℓ, and wma $\mathrm{Hom}(A, A') \neq (0)$.

Thus A' is a simple abelian variety, defined over F, and isogenous to A. This implies that A is isomorphic to an abelian variety A'' defined over some finite extension of F. This gives (3).

(4) We now assume that A is defined over F; by the above, we have a definable isogeny $h : B \to A'(F)$, where A' is defined over F. we may compose this h with an isogeny $A' \to A$, and therefore assume that $A' = A$.

The result will follow from the following claim:

Claim. Let A be an abelian variety defined over F, let B be a definable subgroup of $A(\mathcal{U})$ and $\varphi : B \to A(F)$ a definable homomorphism with finite kernel D. Then $B \subseteq A(\mathrm{Fix}(\sigma^\ell))$ for some ℓ.

Proof. The graph of φ is a definable subgroup of A^2; as there are only countably many of those, it must be defined over F^{alg}. Hence, φ is definable over F^{alg}, say, over $\mathrm{Fix}(\sigma^m)$; working in $\mathcal{U}[m] = (\mathcal{U}, \sigma^m)$ we may therefore assume that φ is defined over $\mathrm{Fix}(\sigma)$. Let $F_0 \prec F$ be such that everything is defined over F_0. Since D is finite, if $b \in B$ then $b \in \mathrm{acl}(F_0(\varphi(b))) = F_0(\varphi(b))^{alg}_\sigma$. By compactness, there is ℓ such that $[F_0(\varphi(b))_\sigma(b) : F_0(\varphi(b))_\sigma] \leq \ell$ for every $b \in B$ and this implies that $b \in \mathrm{Fix}(\sigma^{\ell!})$. (This bound could be higher than $|D|$).

The other direction is clear: $\ker(\sigma^M - 1) = A(\mathrm{Fix}(\sigma^M))$.

References

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

[CHP] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics, Proceedings of the London Math. Society (3) 85 (2002), 257 – 311.

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

[H] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, Ann. Pure Appl. Logic 112 (2001), no. 1, 43 – 115.

[KP] P. Kowalski, A. Pillay, A note on groups definable in difference fields, Proceedings AMS, 130, (2001), 205-212.