Difference fields and descent of difference varieties

Extended abstract. Corrected on 14 January 2010.

Zoé Chatzidakis*(CNRS - Université Paris 7)

Joint work with Ehud Hrushovski. Section 1 consists of algebraic preliminaries on difference fields. Section 2 explicits the connection between difference varieties and difference field extensions, via their "function field", and introduces algebraic dynamics. Section 3 contains the main results, Theorems 3.1 and 3.7, as well as definitions of internal and one-based extensions.

1 Preliminaries

Definition 1.1. A *difference field* is a field K with a distinguished endomorphism σ. (Then σ will of course be injective, but not necessarily surjective.) If $\sigma(K) = K$ then K is a *inversive* difference field.

Any difference field has an inversive closure, which is unique up to K-isomorphism. Difference fields are naturally structures in the language $\{+, -, \cdot, 0, 1, \sigma\}$.

1.2. The study of difference algebra was started by Ritt in the 30's, in parallel with differential algebra. Extensive work was done by Richard Cohn, and you can find most of the algebraic results I cite in his book [4].

1.3. Examples
1. $\mathbb{C}(t)$, where $\sigma|_{\mathbb{C}} = id$, $\sigma(t) = t + 1$. This example is where difference fields acquired their names, from difference equations:

$$y(t+1) - y(t) = g(t)$$

2. $\mathbb{C}(t)$, where $\sigma|_{\mathbb{C}} = id$, $\sigma(t) = qt$, where $0 \neq q \in \mathbb{C}$, q not a root of unity (q-difference equations).
3. K a field of characteristic $p > 0$, $q = p^n$, and $\sigma_q = \mathrm{Frob}^n : x \mapsto x^q$. Note that if K is not perfect, then σ_q is not onto. Note also that each σ_q is definable in the (pure) field K.

1.4. Difference polynomials, difference equations, σ-topology, etc. Given a difference field K, a *difference polynomial*, or σ-polynomial, $f(X_1, \ldots, X_n)$ over K, is simply a polynomial

*partially supported by ANR-06-BLAN-0183

over K in the variables $X_1, \dots, X_n, \sigma(X_1), \dots, \sigma(X_n), \sigma^2(X_1), \dots, \sigma^i(X_j) \dots$. The highest m such that a variable $\sigma^m(X_j)$ occurs non-trivially is called the *order* of the σ-polynomial.

A *difference equation*, or *σ-equation* is then just an equation $f(X_1, \dots, X_n)$ where f is a difference polynomial. The zero-sets of difference polynomials in a difference field K are called σ-closed - this defines a topology on K^n, analogous to the Zariski topology, and called the σ-topology; and the topology is Noetherian. This topology plays the same role in our context as the Zariski topology does in the pure algebraic context.

One can define notions analogous to those defined in classical algebraic geometry: difference varieties, generics of difference varieties, field of definition, dominant σ-morphism, σ-rational map, etc.

Definition 1.5. An *existentially closed difference field* (e.c.) is an inversive difference field (K, σ) such that every finite system of difference equations with coefficients in K which has a solution in some inversive difference field extending K, has a solution in K.

E.c. difference fields were sometimes called *generic difference fields*. They form an elementary class, whose theory (= system of axioms) is called ACFA. It is convenient to work inside a "large" e.c. difference field $(\mathcal{U}, \sigma)$, where by large I mean playing the role of a universal domain, e.g. for some large cardinal κ, every system of $< \kappa$ σ-equations (with parameters) which has a solution in some difference field extending $\mathcal{U}$ already has a solution in $\mathcal{U}$. Observe that a *Difference Nullstellensatz* holds: σ-closed subsets of $\mathcal{U}^n$ are in one-to-one correspondence with *perfect σ-ideals of* $\mathcal{U}[X_1, \dots, X_n]_\sigma$.

1.6. Some more results. While derivations extend uniquely from a field to the algebraic closure, this is not the case with endomorphisms or automorphisms: the endomorphism σ of a field K can have several non-isomorphic extensions to the algebraic closure K^{alg} of K. This makes their study sometimes challenging, and is at the source of the differences in behaviour - eg, failure of quantifier elimination.
In particular, observe that some choice has to be made: the isomorphism type of the algebraic closure of the prime field is an invariant of $(\mathcal{U}, \sigma)$. It turns out that the completions of ACFA are obtained by describing this isomorphism type, and this implies (with the same proofs as for pseudo-finite fields) that the theory ACFA is decidable. In fact, many proofs for e.c. difference fields are very similar to those given for pseudo-finite fields. Hrushovski shows in [5] that non-principal ultraproducts of the difference fields K_q of example 3 are e.c.: in other words, the automorphism σ of $\mathcal{U}$ can be thought of as a *non-standard Frobenius*.

2 Difference varieties and their function field, algebraic dynamics.

Let V be a difference variety defined over a difference field K. We define the *function field* of V as follows: take (in $\mathcal{U}$) a generic point a of V over K, and let

$$K(V)_\sigma = K(a)_\sigma := K(\sigma^i(a))_{i \in \mathbb{N}}$$

be the difference field generated by a over K. Then a σ-rational dominant map $f : W \to V$ defined over K corresponds (dually) to a K-embedding of $K(V)_\sigma$ into $K(W)_\sigma$. And birational equivalence corresponds to $K(W)_\sigma \simeq_K K(V)_\sigma$. Note that here we do not necessarily have that W and W^σ are σ-birationally equivalent: this will only be the case if $a \in K(\sigma(a))_\sigma$.

One could of course allow also functions involving σ^{-1}, in which case the appropriate function field would be the inversive closure of the one defined above.

2.1. By an *algebraic dynamics* over a field K, I mean an algebraic variety V (preferably absolutely irreducible), together with a dominant rational map $\phi : V \to V$, both defined over K. If L is an overfield of K, then the system (V, ϕ) can naturally be viewed as an algebraic dynamics over L, and I won't distinguish between the two. A *morphism* from (V, ϕ) to (W, ψ) is a dominant rational map $h : V \to W$ such that $h\phi = \psi h$.

An algebraic dynamic (V, ϕ) defines naturally a difference variety, by the equation

$$x \in V \wedge \sigma(x) = \phi(x).$$

To such a (V, ϕ) corresponds a difference field in the following way. Write $K(V) = K(a)$ (i.e., a a generic of V), define σ to be the identity on K, and $\sigma(a) = \phi(a)$. Then if h and W are as above, $h(a) = b$ will satisfy $\psi(y) = y \wedge y \in W$. For more details, see [2].

3 Descent results (for algebraic dynamics)

Theorem 3.1. *Let $K_1 \subseteq K_2$ be fields (algebraically closed; or K_2/K_1 regular), and let (V_i, ϕ_i) be algebraic dynamics defined over K_i, $i = 1, 2$. Assume that (V_1, ϕ_1) dominates (V_2, ϕ_2), with* $\dim(V_2) > 0$. *Then (V_2, ϕ_2) dominates an algebraic dynamics (V_3, ϕ_3) defined over K_1, and with* $\dim(V_3) > 0$.

3.2. Remarks. The hypotheses of this theorem do arise in nature, in fact in a result of M. Baker [1]. Assume that $K_2 = K_1(t)$, $V_2 = \mathbb{P}^n$, fix some d, and let S_d be the set of points of $\mathbb{P}^n(K_2)$ which are represented by polynomials of degree $\leq d$. Then S_d is naturally the image of the K_1-rational points of some algebraic set defined over K_1. The existence of *sufficiently* many arbitrarily long sequences of points P_i with $\phi(P_i) = P_{i+1}$ and which lie in S_d, will then imply the existence of a difference variety (V_1, ϕ_1) defined over K_1, and which dominates (V_2, ϕ_2^m) for some m. In Baker's result, he takes for K_2 a function field in 1 variable, $n = 1$, and ϕ_2 of degree > 1; his assumptions on the set of canonical height 0 then imply that for some d, S_d contains arbitrarily long sequences as above, and allows one to be in the situation of the theorem.

One of the tools used in the proof is the following

Theorem 3.3. *(***The dichotomy theorem***) Let K be a difference field, and L a finitely generated difference field extension of K, of finite transcendence degree. Then there are difference fields $L_0 = K \subset L_1 \subset \cdots \subset L_m = L$ such that for every i, the extension L_{i+1}/L_i is either*

- *algebraic, or*

- *qf-internal to a fixed field* Fix(τ)*, or*
- *one-based.*

3.4. Comments. There are two important notions appearing in this result, the one of *qf-internal to a field*, and the one of *one-based*, and I will define them below. The dichotomy theorem was first proved in a weaker form (the L_i's were contained in L^{alg}, not necessarily in L).

3.5. Definitions. (1) If $\tau = \sigma^n\mathrm{Frob}^m$, then we know that $\mathrm{Fix}(\tau) = \{a \in \mathcal{U} \mid \tau(a) = a\}$ is a (pseudo-finite) field. We say that M/K is *qf-internal to* Fix(τ), if for some difference field N containing K and which is free from M over K, we have $M \subset N\mathrm{Fix}(\tau)$. We will say that it is *almost-internal to* Fix(τ) if it is contained in M_0^{alg}, for some extension M_0/M which is qf-internal to Fix(τ).
(2) We say that M/K is *one-based* if whenever $M_1, \dots, M_r$ are K-isomorphic copies of M (within $\mathcal{U}$), and $N = \sigma(N)^{alg}$ contains K, $C = (M_1 \cdots M_r)^{alg} \cap N$, then $(M_1 \cdots M_r)^{alg}$ and N are free over C. A definable set S is *one-based* if whenever $a_1, \dots, a_r \in S$, K is a difference field containing the parameters needed to define S, M is the algebraic closure of the difference field generated by $a_1, \dots, a_r$ over K and $N = \sigma(N)^{alg}$ is a difference field, then M and N are linearly disjoint over their intersection. A one-based subgroup B of an algebraic group G has the following property: if $X \subset B^n$ is irreducible σ-closed, then X is a coset of a σ-closed subgroup of B^n.

3.6. Diophantine geometers will have recognized from this last property of one-based groups that they are instrumental in applications such as Mordell-Lang for function fields or Manin-Mumford. The notion of field internality is related to iso-constantness, maybe in a twisted form: If $M = K(V)_\sigma$, and $F = \mathrm{Fix}(\tau)$, then M/K is qf-internal to F if and only if the σ-variety V is σ-birationally isomorphic to $W(F)$ for some algebraic variety W defined over F. Here, $W(F)$ is the difference variety defined by $x \in W \wedge \tau(x) = x$.

3.7. The case of Theorem 3.1 when $\deg(\phi_2) > 1$ will be a consequence of the following more general result:

Theorem. *Let K_1, K_2 be difference subfields of some e.c. difference field $\mathcal{U}$, let V_i be difference varieties defined over K_i, $i = 1, 2$, and assume that*

- *K_2 is a regular extension of $K := K_1 \cap K_2$, and K_2/K is qf-internal to* Fix(τ) *(for some fixed τ).*
- *The extension $K_2(V_2)_\sigma/K_2$ is not almost internal to* Fix(τ).
- *There is a dominant σ-morphism (defined over K_1K_2) from V_1 to V_2 (where the V_i's are now viewed as difference varieties over K_1K_2).*

Then V_2 dominates some difference variety V_3 which is defined over K. Moreover, the extension $K_2(V_2)_\sigma/K(V_3)_\sigma$ is almost internal to Fix(τ).
Furthermore, if $\tau = \sigma$ and $K_2(V_2)_\sigma/K_2$ is a finitely generated field extension*, then so is the extension $K(V_3)_\sigma/K$, and the extension $K_2(V_2)_\sigma/K_2(V_3)_\sigma$ is almost qf-internal to* Fix(σ).

3.8. Let us see how it applies to algebraic dynamics (V_i, ϕ_i) defined over K_i, $i = 1, 2$ and shows Theorem 3.1 when $\deg(\phi_2) > 1$. In that particular case, we have K_i, $i = 1, 2$, are contained in $\mathrm{Fix}(\sigma)$, and $K_i(V_i)_\sigma = K_i(V_i)$, and (V_1, ϕ_1) dominates (V_2, ϕ_2). The conclusion implies that (V_2, ϕ_2) dominates some (V_3, ϕ_3), with $\deg(\phi_3) = \deg(\phi_2)$.

3.9. The case of $\deg(\phi_2) = 1$ is done entirely differently when the extension $K_2(V_2)_\sigma/K_2$ is qf-internal to $\mathrm{Fix}(\sigma)$. (While this condition implies $\deg(\phi_1) = 1$, it is strictly stronger). We must assume that K_2 and K_1 are algebraically closed. We develop some *definable Galois theory*, and show in a first step that (V_2, ϕ_2) is isomorphic to (A, t_a) where A is some commutative algebraic group, and t_a is translation by some element $a \in A(K_2)$. We may assume that A is simple, i.e., equals $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple Abelian variety. After more manipulations, we obtain the result. The proof is particularly easy when $A = \mathbb{G}_a$: if $a = 0$, there is nothing to do, $(V_2, \phi_2) \simeq (\mathbb{G}_a, id)$; if $a \neq 0$, then putting $y = xa^{-1}$, the equation $\sigma(x) = x + a$ becomes $\sigma(y) = y + 1$. This part is still being written.

References

[1] M. Baker, *A Finiteness Theorem for Canonical Heights Attached to Rational Maps over Function Fields*, to appear in J. Reine Angew. Math. Available on arxiv.

[2] Z. Chatzidakis, E. Hrushovski, *Difference fields and descent in algebraic dynamics, I*, Journal of the IMJ, 7 (2008) No 4, 653 – 686.

[3] Z. Chatzidakis, E. Hrushovski, D*ifference fields and descent in algebraic dynamics, II*, Journal of the IMJ, 7 (2008) No 4, 687 – 704.

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

[5] E. Hrushovski, *The first-order theory of the Frobenius*, preprint, available on `arxiv`.