Difference fields, torsors and descent

Zoé Chatzidakis
CNRS - Université Paris 7

La Roche Modnet Workshop, 20 - 25 April 2008

(Joint with E. Hrushovski)

Preliminaries

A difference field is a field with a distinguished automorphism, σ.
Language: $\{+, -.\cdot, 0, 1, \sigma, \sigma^{-1}\}$. Here are some classical examples:

- $\mathbb{C}(t)$, $\sigma_{|_{\mathbb{C}}} = id$, $t \mapsto t + 1$.
  (Difference equations: $y(t+1) - y(t) = f(t)$)
- $\mathbb{C}(t)$, $\sigma_{|_{\mathbb{C}}} = id$, $t \mapsto qt$, where $0 \neq q \in \mathbb{C}$, and usually q is not a root of 1.
  (q-difference equations).
- $\mathbb{F}_p^{alg}$, $\sigma = \mathrm{Frob}_p$

Difference algebra was first studied by Ritt in the 1930's, in parallel with differential algebra. One of the main references of the subject is *Difference algebra*, by Richard Cohn.

Difference polynomials = polynomials in X, X^{σ}, X^{σ^2}, ...
Action of σ on the ring of difference polynomials over a difference field K. Notions of σ-ideals, prime σ-ideals, σ-topology on K^n (a Noetherian topology), σ-closed sets (sets of zeroes of difference polynomials), σ-varieties (=irreducible σ-closed sets) etc.

Existentially closed difference fields

An existentially closed difference field (e.c.) is a difference field K such that every finite system of difference equations which has a solution in a difference field extending K, has a solution in K.

They play the role of universal domains, provided they are saturated enough. *Nullstellensatz* for e.c. difference fields.

Elementary invariants: the behaviour of σ on the algebraic closure of the prime field.

Notation and conventions

$\mathcal{U}$: large e.c. difference field containing all fieds considered.
$\mathrm{Fix}(\sigma) = \{a \in \mathcal{U} \mid \sigma(a) = a\} \quad := F$
If K is a difference field and a a tuple in $\mathcal{U}$, then
$K(a)_\sigma = K(\sigma^i(a))_{i\in\mathbb{Z}}$, the difference field generated by a over K.

If V is a difference variety defined over K, then a is a generic of V over K iff V is the smallest σ-closed set defined over K which contains a.
Given a tuple a and a difference field K, then the locus of a over K, $\mathrm{Locus}(a/K)$ [resp. $\mathrm{Locus}_\sigma(a/K)$] is the smallest algebraic [resp. σ-closed] set defined over K and containing a.

Unless otherwise mentionned, maps between σ-varieties are rational σ-morphisms (i.e., given by quotients of difference polynomials) and are dominant. If a_i is a generic of V_i/K for $i = 1, 2$, then a morphism $V_1 \to V_2$ defined over K gives rise to a K-embedding of $K(a_2)_\sigma$ into $K(a_1)_\sigma$, and viceversa.

Main result

Theorem

Let $K_1 \subset K_2$ be algebraically closed subfields of $\mathrm{Fix}(\sigma)$, and let V_i be σ-varieties defined over K_i, $i = 1, 2$. Assume that V_1 dominates V_2, and $\dim(V_2) > 0$, V_2 of finite order. Then V_2 dominates some V_3 defined over K_1 and with $\dim(V_3) > 0$.

Translation in terms of difference fields:

Let $K_1 \subset K_2$ be algebraically closed subfields of $\mathrm{Fix}(\sigma)$, and let a, b be tuples in $\mathcal{U}$ such that $b \downarrow_{K_1} K_2$ and $a \in K_2(b)_\sigma$, $a \notin K_2$. Then there is $c \in K_2(a)_\sigma$ such that $c \downarrow_{K_1} K_2$ (and in fact one can choose c in the perfect hull of $K_1(b)_\sigma$).

Here, $b \downarrow_{K_1} K_2$ means that

$$tr.deg(K_2(b)_\sigma / K_2) = tr.deg(K_1(b)_\sigma / K_1),$$

b is independent from K_2 over K_1.

To prove this theorem, one reduces to the case where V_2 is *primitive*, that is, any proper quotient V_3 of V_2 (defined over K_2) has dimension 0 or $\dim(V_2)$. Then one of the main results of difference field theory, plus a new result, tell us that we are reduced to one of the following cases

1. The extension $K_2(a)_\sigma/K_2$ is foreign to $\mathrm{Fix}(\sigma)$.
2. The extension $K_2(a)_\sigma/K_2$ is qf-internal to $\mathrm{Fix}(\sigma)$. (Definition to follow).

In case 1 we can weaken the hypothesis of K_1, K_2 algebraically closed, to the extension K_2/K_1 being regular.

Original motivation of the study

Theorem (M. Baker)

Let K/k be a regular extension of transcendence degree 1, *finitely generated, $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ defined over K, with* $\deg(\phi) > 1$. *Let h be the canonical height $\mathbb{P}^1(K) \to \mathbb{R}$ associated to this data. If there is $P \in \mathbb{P}^1(K)$ with $h(P) = 0$ and $\{\phi^n(P) \mid n \in \mathbb{N}\}$ infinite, then ϕ descends to k.*

It turns out that under the hypotheses of Baker's theorem, if the conclusion of the theorem is false, then for some n, the difference variety

$$V_2 := \{x \in \mathbb{P}^1 \mid \sigma(x) = \phi^n(x)\}$$

is dominated by a difference variety defined over k.

qf-internality

Definition

Let K be a difference field, a a finite tuple in $\mathcal{U}$ such that $tr.deg(K(a)_\sigma/K) < \infty$. Then the extension $K(a)_\sigma/K$ is qf-internal to $\mathrm{Fix}(\sigma) = F$ if for some finite $A \subset \mathcal{U}$ and $L = K(A)_\sigma$ with $a \mathop{\smile\!\!\!\!\!\!|}_K L$, we have $L(a)_\sigma = L(b)_\sigma$ for some tuple b in F.

Some comments:

– it makes sense for other *fixed fields* in positive characteristic,

– stronger than the usual definition of internality, which only requires $a \in \mathrm{dcl}(Lb)$.

Galois theory

Assume that $K(a)_\sigma/K$ is qf-internal to F, and that $K(a)_\sigma \cap F = K \cap F$, $K(a)_\sigma/K$ a regular extension. Our assumptions imply that $K(a)_\sigma$ is finitely generated over K as a field, and we may therefore assume that $K(a)_\sigma = K(a)$. Consider the set Q of tuples of $\mathcal{U}$ with the same σ-locus as a over K, and let $L = K(Q)_\sigma = K(Q)$. Let $\underline{Q}$ be the Zariski closure of Q.

We are interested in $\mathcal{G} = \mathrm{Aut}_\sigma(L/K)$. We show that there is a qf-definable group G of some algebraic group $\underline{G}$ defined over K, acting on $\underline{Q}$, everything being defined over K, and such that

$$(\mathcal{G}, Q) \simeq (G, Q).$$

This is fairly standard (Hrushovski, Kamensky), the only difficulty is to make sure that everything is done with rational functions (and not only constructively). One important observation is that there is some finite tuple b in Q^m such that $L = FK(b)$. Thus, if P denotes the σ-locus of b over FK, an element τ of $\mathcal{G}$ is uniquely deetermined by the pair $(b, \tau(b))$. One shows that P is a $\mathcal{G}$-torsor, and that there is an algebraic group $\underline{H}$ defined over F, such that $H = \underline{H}(F) \simeq \mathrm{Aut}_{\mathcal{G}}(P)$, i.e., P is a (G, H)-bitorsor. Note that $G \simeq H^{op}$

If $F \cap K$ is pseudo-finite and K is algebraically closed, then one shows that $(Q, \mathcal{G}) \simeq (V, G)$, where V is defined by $x \in \underline{G} \wedge \sigma(x) = g_0 x$, for some $g_0 \in \underline{G}(K)$.
In general, no such result. However

Our particular case

If $K \subset F$ is algebraically closed, then

1. $\mathcal{G}$ is abelian,
2. $L = FK(a)$ for any $a \in Q$,
3. Q is K-isomorphic to $\{g \in \underline{G} \mid \sigma(g) = g + g_0\}$ for some $g_0 \in \underline{G}(K)$, and $\mathcal{G} = \underline{G}(F)$, $\mathrm{Aut}_\sigma(K(a)/K) = \underline{G}(K)$.

Proof. 1. $\sigma \in \mathcal{G}$ because Q is defined over $\mathrm{Fix}(\sigma)$, and also $\sigma \in Z(\mathcal{G})$. Pick $a \in Q$, let X be the orbit of a under $Z(\mathcal{G})$. Then $X^\sigma = X$ since $\sigma \in Z(\mathcal{G})$; furthermore, since X is definable over $K(a)$, we know that it is definable over $F \cap K(a)^{alg} = K$. Hence $Z(\mathcal{G}) = \mathcal{G}$, which shows 1. The other items follow because the right action and left action are the same. If $q_0 \in \underline{Q}(K)$, then let $h_0 \in \underline{G}(\mathcal{U})$ be such that $h_0 \cdot q_0 = q \in Q$; then $\sigma(q) = \sigma(h_0) \cdot q_0 = \sigma(h_0)h_0^{-1} \cdot q$, i.e., via $h \mapsto h \cdot q_0$, Q is isomorphic to $\{g \in \underline{G} \mid \sigma(g) = \sigma(h_0)h_0^{-1}g\}$.

End of the proof

We have b independent from K_2 over K_1, and $a \in K_2(b)_\sigma$, with $K_2(a)_\sigma/K_2$ qf-internal to F; if $K_2(a)_\sigma \cap F \neq K_2$, then take an element $c \in K_2(a)_\sigma \cap F$, $c \notin K_2$. Then c is a generic of the difference variety $x \in \mathbb{A}^1 \wedge \sigma(x) = x$ over K_2, and we are done. So we may assume that $K_2(a)_\sigma \cap F = K_2$, and by the above, after some work, we can assume that a, b are generics (over K_2, $K_3 = K_3^{alg} = K_1(b)^{alg} \cap F$) of the translation varieties X, Y respectively:

$$X := \{y \in B \mid \sigma(y) = y + b_0\} \qquad Y := \{x \in A \mid \sigma(x) = x + a_0\},$$

where A, B are connected commutative algebraic groups, defined over K_2, K_3 resp., and $a_0 \in A$, $b_0 \in B$, A without proper non-trivial quotients (because $K_2(a)_\sigma/K_2$ primitive).

If $A = \mathbb{G}_a$, then we are done: we know that $a_0 \neq 0$; then a/a_0 is a solution of the equation $\sigma(x) = x + 1$ which is defined over K_1.
So, assume that $A = \mathbb{G}_m$, or A a simple Abelian variety.

Let Z be the σ-locus of (a, b) over F^{alg}, a subset of $X \times Y \subset A \times B$, and $C_0 = \mathrm{Stab}(Z)$. Then C_0 projects onto some definable subgroup A_0 of $A(F) = \mathrm{Aut}_\sigma(F(a)/F)$ of bounded index (if $tp(a'/F^{alg}) = tp(a/F^{alg})$, then some F-automorphism τ of $\mathcal{U}$ takes a to a'); on the other hand, clearly C_0 projects onto $\mathrm{Aut}_\sigma(F(b)/F)$, the latter containing $B(K_3)$. This implies that the Zariski closure C of C_0 is a subgroup of $A \times B$ which projects onto A and onto B. Hence, if $D \leq B$ is defined by $1 \times D = C \cap (1 \times B)$, and $\pi : B \to B/D$ is the natural projection, then $(id \times \pi)$ is the graph of a group homomorphism $f : A \to B/D$ with finite kernel. Replacing B by $B^{Frob_p^m}$ if necessary, we may assume that f is an (algebraic) group morphism. Then B/D is semi-abelian, which implies that B/D and π are defined over K_3.

A and B/D are isogenous; hence there is a semi-abelian variety A' defined over $K_1 = K_2 \cap K_3$, and epimorphisms $f_2 : A \to A'$ and $f_3 : B/D \to A'$ with finite kernels. $(f_2, f_3\pi)(C)$ is then the graph of an isogeny $\tilde{f} : A' \to A'$ (defined over K_1).

We therefore have that $\dim(C) = \dim(B)$ equals the dimension of the Zariski closure $\underline{Z}$ of Z; as $\underline{Z}$ is connected, it is a translate of C. Going back to the original problem, and remembering that C_0 must be quantifier-free definable, and thus equals $C(F)$, we obtain that $Z = (a, b) + C_0$.

Let $f_1 = f_3\pi : B \to A'$, $g = \tilde{f} f_2 : A \to A'$. As $Z^\sigma = Z$, we have $(\sigma(a) - a, \sigma(b) - b) = (a_0, b_0) \in C_0$. Applying (g, f_1), we obtain that $f_1(b_0) = g(a_0) \in K_3 \cap K_2 = K_1$. Hence g sends X to $\{x \in A' \mid \sigma(x) = x + g(a_0)\}$, which is defined over K_1.