The model theory of difference fields
Notes on lectures given at Tokay University (Tokyo, Japan), September 97
Zoé Chatzidakis

Introduction. A difference field is a field with a distinguished automorphism σ. They were first studied by Ritt in the 30's. A good reference for the algebraic results is Cohn's book [C]. Interest in the model theory of difference fields started at the end of the eighties, particularly during the MSRI logic year, because of two questions.

The first question stemmed from the failure of Zil'ber's conjecture: there is a strongly minimal theory extending the theory of algebraically closed fields of any given characteristic. People were looking at the possibility of finding a non-definable automorphism σ of $\tilde{\mathbb{F}}_p$ (the algebraic closure of the field $\mathbb{F}_p$ with p elements), such that $\mathrm{Th}(\tilde{\mathbb{F}}_p, +, \cdot, \sigma)$ is strongly minimal. This question sofar remains open.

The second problem had to do with the difference fields $K_q = (\tilde{\mathbb{F}}_p, +, \cdot, \sigma_q)$, where q is a power of p and $\sigma_q : x \mapsto x^q$ is a power of the Frobenius automorphism $x \mapsto x^p$. The hope was to generalise the work of Ax on finite fields to these structures, and in particular to describe the theory of the non-principal ultraproducts of the difference fields K_q.

These questions led Macintyre, Van den Dries and Wood to look for a model companion of the theory of difference fields, and to prove various results (decidability, description of the completions, etc ...) for this theory, henceforth called $ACFA$. For details and attribution of results, see Macintyre's paper [M95]. I should also mention that the second problem was solved recently, by Hrushovski [H96] and Macintyre [M97], showing that non-principal ultraproducts of K_q's are models of $ACFA$.

In 94, Hrushovski and myself started looking at stability-type properties of the theory $ACFA$. Our main result is a trichotomy result for types of rank 1 for models of characteristic 0, which was later partially extended to the case of positive characteristic with the help of Peterzil (see [CH] and [CHP]). It has some applications to the description of types of finite rank, and to groups definable in models of $ACFA$. These results were used by Hrushovski to find explicit bounds in the Manin-Mumford conjecture, see [H95].

This paper gives a survey of the results obtained to-date.

1. Description and elementary results on the theory $ACFA$.

(1.1) Some examples.

(1) The shift operator. Consider the field $K = \mathbb{C}(t)$, and define σ by

$$\sigma|_{\mathbb{C}} = id, \qquad \sigma(t) = t + 1.$$

The name "difference field" originated from this example: an equation of the form $P(f(t), f(t+1), \dots, f(t+n)) = 0$, where f is the unknown function to be found and P is a polynomial over K, is called an algebraic difference equation. One can replace K by other fields, e.g., the field of meromorphic functions on $\mathbb{C}$ or on $\mathbb{R}$.

(2) Let K be a field, K^s its separable closure and $\sigma \in \mathcal{G}al(K^s/K)$. Then (K^s, σ) is a difference field. Note that because the algebraic closure $\tilde{K}$ of K is purely inseparable over

K^s, σ extends uniquely to an automorphism of $\tilde{K}$. One often identifies $\mathcal{G}al(K^s/K)$ and $\mathrm{Aut}(\tilde{K}/K)$.

The structures K_q described above are a particular example.

(1.2) Definitions, notation and some basic algebraic results. In the literature, a difference field is a field K with a distinguished monomorphism σ. If σ is onto, then (K, σ) is called a reflexive difference field. However, a simple inductive limit argument shows that every difference field has a unique (up to isomorphism) reflexive closure. We will assume in what follows, that **all difference fields are reflexive**. The references are to Cohn's book [C].

Let K be a difference field, and let $\bar{X} = (X_1, \dots, X_n)$ be indeterminates. A difference polynomial over K in $X_1, \dots, X_n$ is an ordinary polynomial with coefficients in K, in the variables $X_1, \dots, X_n, \sigma(X_1), \dots, \sigma^i(X_j), \dots$. The ring of those difference polynomials is denoted $K[X_1, \dots, X_n]_\sigma$, and σ extends naturally to $K[X_1, \dots, X_n]_\sigma$, in the way suggested by the names of the variables.

Note: As defined, σ is not onto. It is sometimes convenient to consider the reflexive closure of this ring, namely $K[\sigma^i(X_1), \dots, \sigma^i(X_n)]_{i \in \mathbb{Z}}$, but we will not do this here.

There is a natural notion of σ-ideal, i.e., an ideal closed under σ, of reflexive σ-ideal ($a \in I \iff \sigma(a) \in I$). The analog of a radical ideal is called a perfect σ-ideal: a σ-ideal I is perfect if $a \in I$ whenever $a^j \sigma^i(a) \in I$ for some $i, j \in \mathbb{N}$). Note that a prime σ-ideal is perfect.

$K[X_1, \dots, X_n]_\sigma$ does not satisfy the ascending chain condition on σ-ideals; however it satisfies it for perfect σ-ideals, and therefore for prime σ-ideals.

This allows one to define σ-closed sets and σ-varieties in affine n-spaces. They correspond dually to perfect σ-ideals and prime reflexive σ-ideals, and define a noetherian topology

Let K be a difference field, a a tuple of elements (in some difference field extending K). We denote by $K(a)_\sigma$ the difference field generated by a over K, by $acl_\sigma(Ka)$ its algbraic closure, and by $deg_\sigma(a/K)$ the transcendence degree of $K(a)_\sigma$ over K.

If a is a single element and $deg_\sigma(a/K)$ is infinite, then a is called transformally transcendental. The elements $\sigma^j(a)$, $j \in \mathbb{Z}$, are then algebraically independent over K. If $deg_\sigma(a/K)$ is finite, then a is called transformally algebraic.

There is a natural notion of transformal transcendence basis, and transformal dimension.

(1.3) An axiomatisation of the theory $ACFA$.

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

(i) K is an algebraically closed field,

(ii) $\sigma \in \mathrm{Aut}(K)$,

(iii) if U and V are varieties defined over K, with $V \subseteq U \times \sigma(U)$ projecting generically onto U and $\sigma(U)$, then there is a tuple a in K such that $(a, \sigma(a)) \in V$.

Here, by a variety, we mean an irreducible Zariski closed set, i.e., a set defined by polynomial equations, and which is not the proper union of two smaller Zariski closed sets. The set $\sigma(U)$ is the variety obtained from U by applying σ to the coefficients of the defining polynomials of U. Note that (iii) is indeed a conjunction of first-order sentences, since (by classical results on polynomial rings over fields) the fact that polynomials $f_1(\bar{X}), \dots, f_n(\bar{X})$ generate a prime ideal of $K[\bar{X}]$ is an elementary condition on the coefficients of $f_1, \dots, f_n$. Similarly for the inclusion of ideals in $K[\bar{X}]$.

Theorem. $ACFA$ is the model companion of the theory of difference fields.

Proof. (Sketch) We first need to show that every difference field embeds in a model of $ACFA$. Axioms (i) and (ii) pose no problem, as every automorphism of a field extends to its algebraic closure. Let U and V be as in (iii). Choose a generic point (a, b) of V over K, in some field containing K. Then a is a generic of U, and b is a generic of $\sigma(U)$. By elementary properties of algebraically closed fields, the isomorphism $\tau : K(a) \to K(b)$ which extends σ on K and sends a to b, extends to an automorphism of the algebraic closure of $K(a, b)$.

This shows that every difference field embeds in a model of $ACFA$. It remains to show that the models of $ACFA$ are existentially closed. Let $(K, \sigma) \models ACFA$, let $\varphi(x)$, x a tuple of variables, be a quantifier-free formula with parameters in K, and assume that $\varphi(x)$ has a solution in some difference field (L, σ) extending K. The usual trick of replacing the inequality $y \neq 0$ by $\exists z\ yz - 1 = 0$, shows that one can assume that $\varphi(x)$ is a conjunction of σ-equations. Let $a \in L$ satisfy φ. For n large enough, the σ-ideal I generated by the set

$$\{f(X, \sigma(X), \dots, \sigma^n(X)) \mid f(Y, Y_1, \dots, Y_n) \in K[Y, Y_1, \dots, Y_n],\ f(a, \sigma(a), \dots, \sigma^n(a) = 0\}$$

is precisely the prime σ-ideal of difference polynomials over K annulled by a. Thus any point satisfying these equations will satisfy $\varphi(x)$.

Let U be the variety defined over K with generic $(a, \sigma(a), \dots, \sigma^{n-1}(a))$, and V the variety defined over K with generic $(a, \sigma(a), \dots, \sigma^{n-1}(a), \sigma(a), \dots, \sigma^n(a))$. Then U and V satisfy the hypotheses of axiom (iii), and therefore there is a tuple b in K such that $(b, \sigma(b)) \in V$. Then $b = (c, \sigma(b), \dots, \sigma^{n-1}(b))$ for some c, and $K \models \varphi(c)$.

(1.4) The Frobenius automorphisms. Before continuing with the elementary properties of $ACFA$, we will now state precisely the result of Hrushovski, from which follows that non-principal ultraproducts of K_q's are models of $ACFA$. Macintyre's proof is more direct. It is then a consequence of Tchebotarev's theorem on the distribution of primes that $ACFA$ is exactly the theory of all non-principal ultraproducts of K_q's, see [M95].

Theorem ([H96]). Let U, V be varieties with $V \subseteq U \times \sigma(U)$, and assume that the projections are onto and have finite fibers. Let $d_1 = [K(V) : K(U)]$, $d_2 = [K(V) : K(\sigma(U))]_i$ (purely inseparable degree); let $c = d_1/d_2$ and $d = dim(V)$. Then for some constant $C > 0$, depending on the two varieties U and V, and which remains bounded when U and V move inside an algebraic family of varieties,

$$\left| Card(\{a \in \tilde{\mathbb{F}}_p^n \mid (a, a^q) \in V\}) - cq^d \right| \leq Cq^{d-1/2}.$$

(1.5) Properties of the theory $ACFA$. It turns out that many of the proofs of Ax for pseudo-finite fields generalise to models of $ACFA$. The results here appear in [M95]. Let us first start with an easy one, which has important consequences:

(1) Let (K_1, σ_1) and (K_2, σ_2) be models of $ACFA$, and let E be a common sub-difference field. Then

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

Proof. The left to right implication is almost immediate. For the other one, moving K_2 by some E-isomorphism, we may assume that $E = \tilde{E}$ and that K_1 and K_2 are linearly disjoint over E. This implies that the ring $K_1 \bigotimes_E K_2$ is a domain. Define $\sigma(a \otimes b) = \sigma_1(a) \otimes \sigma_2(b)$ for $a \in K_1$ and $b \in K_2$; then σ extends to an automorphism of the quotient field L of $K_1 \bigotimes_E K_2$, which agrees with σ_1 on K_1 and σ_2 on K_2. Now, (L, σ) embeds in a model (M, σ) of $ACFA$, and by model-completeness we have $(K_1, \sigma_1) \prec (M, \sigma)$, $(K_2, \sigma_2) \prec (M, \sigma)$.

(2) From the above one deduces immediately that the completions of $ACFA$ are obtained by specifying what is the action of σ on the algebraic closure of the prime field ($\tilde{\mathbb{Q}}$ or $\tilde{\mathbb{F}}_p$). This then entails the decidability of the theory $ACFA$, as well as of its extensions $ACFA_0$ and $ACFA_p$ obtained by specifying the characteristic of the field.

(3). It also gives a description of the types. Let E be a difference field, a and b two tuples from a model K of $ACFA$ containing E. Then $tp(a/E) = tp(b/E)$ if and only if there is an isomorphism φ from the difference field $acl_\sigma(Ea) = \widetilde{E(a)_\sigma}$ onto the difference field $acl_\sigma(Eb)$ which is the identity on E and sends a to b.

(4) Let us also note that if E is an algebraically closed difference field, then $ACFA \cup qftp(E) \vdash tp(E)$, where $qftp(E)$ denotes the quantifier-free type of E.

(5) If $(K, \sigma) \models ACFA$, then the subfield $Fix(\sigma)$ of K fixed by σ is a pseudo-finite field.

(6). It turns out that the algebraic closure (in the model-theoretic sense) of a set A coincides with the algebraic closure (in the ordinary field sense) of the difference field generated by A (which we denote by $acl_\sigma(A)$). Indeed, let $A = acl_\sigma(A) \subseteq K \models ACFA$ and $b \in K \setminus A$, $B = acl_\sigma(Ab)$; let B_1 be an A-isomorphic copy of B, linearly disjoint over A. As in (1), there is a model of $ACFA$ containing the difference fields B and B_1. By (3), $tp(B_1/A) = tp(B/A)$, which shows that $tp(b/A)$ is not algebraic.

2. Independence and rank

(2.1) Definition of independence. Let A, B and C be subsets of a model K of $ACFA$. We say that A and B are independent over C ($A \perp_C B$), if $acl_\sigma(CA)$ and $acl_\sigma(CB)$ are linearly disjoint over $acl_\sigma(C)$. This notion has all the usual properties of independence in algebraically closed fields.

(2.2) The independence theorem. Let $E = acl_\sigma(E) \subseteq K$, let a, b, c_1 and c_2 be tuples from K such that a, b, c_1 and c_2 are independent over E and $tp(c_1/E) = tp(c_2/E)$. Then there is c (in some elementary extension of K) independent from (a, b) over K, and realising $tp(c_1/acl_\sigma(Ea)) \cup tp(c_2/acl_\sigma(Eb))$.

(2.3). From a result of Kim-Pillay [KP], we then deduce that independence coincides with non-forking, and that any completion of $ACFA$ is simple.

We already know that $ACFA$ is unstable, since any model defines a pseudo-finite field, and pseudo-finite fields are unstable by a result of Duret [D]. Simplicity is weaker than stability. However, many of the techniques of stability theory generalise to its context. In our situation, it turns out that we have some definability of non-forking. The independence theorem is essential for the study of definable groups. Indeed, one can generalise to the context of simple theories the concepts of generic types and of their stabilizers. It is also used in the proof of the following two results:

(2.4) Let K be a model of $ACFA$.

(1) $\mathrm{Th}(K)$ has elimination of imaginaries.

(2) Let $S \subseteq Fix(\sigma)^n$ be definable in K. Then S is definable in the pure field $Fix(\sigma)$ (with additional parameters from $Fix(\sigma)$).

(2.5) Definition of the SU-rank. We define a rank based on forking in the usual way, that is, for p a type over E, realised by a tuple a,

— $SU(p) = SU(a/E) \geq 0$,

— $SU(p) \geq \alpha$ for α a limit ordinal, if and only if $SU(p) \geq \beta$ for every $\beta < \alpha$,

— $SU(p) \geq \alpha + 1$ if and only if there is $F \supseteq E$ such that $a \not\downarrow_E F$ and $SU(a/F) \geq \alpha$.

Then, $SU(p)$ is the least ordinal α such that $SU(p) \not\geq \alpha + 1$.

(2.6) This rank shares the properties of the usual U-rank, and in particular, the Lascar rank inequality: if a, b are tuples and E a set, then $SU(a/Eb) + SU(b/E) \leq SU(a, b/E) \leq SU(a/Eb) \oplus SU(b/E)$, where $\oplus$ denotes the natural sum on ordinal numbers.

(2.7) Some examples. Let E be a difference subfield of a model K of $ACFA$ and a a tuple in K. From the definition of the SU-rank, it is clear that

— $SU(a/E) = 0 \iff a \in acl_\sigma(E)$.

— $SU(a/E) = 1 \iff a \notin acl_\sigma(E)$ and for every $F \supseteq E$, either $a \downarrow_E F$ or $a \in acl_\sigma(F)$.

We defined earlier an invariant of $tp(a/E)$: $deg_\sigma(a/E)$. It has some relation with SU-rank, since forking is defined in terms of forking in algebraically closed fields. For instance, one has, for $E \subseteq F$ difference fields and a a tuple with $deg_\sigma(a/E) < \infty$,

$$a \not\downarrow_E F \iff deg_\sigma(a/F) < deg_\sigma(a/E),$$

which implies

$$SU(a/E) \leq deg_\sigma(a/E).$$

Thus in particular, every non-algebraic type containing the equation $\sigma(x) = x^2 + 1$ has SU-rank 1. This inequality can be strict: let a be a non-algebraic realisation of $\sigma^2(x) = x^2 + 1$ (we assume the characteristic is different from 2); then $SU(a/\emptyset) = 1$ even though $deg_\sigma(a/acl_\sigma(\emptyset)) = 2$.

One can also show that the SU-rank of an element transformally transcendental over the difference field E is ω: let a be such an element, and consider the sequence (b_i), $i \in \mathbb{N}$, defined by $b_0 = a$, $b_{i+1} = \sigma(b_i) - b_i$. Then the fields $L_i = E(b_i)_\sigma$ form a decreasing sequence of subfields of $E(a)_\sigma$, with $tr.deg(L_i/L_{i+1}) = 1$. By additivity of rank, we obtain

$SU(a/L_i) = i$, which implies that $SU(a/E) \geq \omega$. On the other hand, $SU(a/E) \ngeq \omega + 1$ since if $a \not\perp_E F$ then $deg_\sigma(a/F) < \infty$, which implies that $SU(a/F) < \omega$.

This gives: $SU(a/E) < \omega \iff deg_\sigma(a/E) < \infty$.

(2.8) Groups of finite SU-rank. The techniques developped in [HP94] generalise easily to the $ACFA$ context, and give:

Let G be a group of finite SU-rank defined over a model K of $ACFA$. There is an algebraic group H defined over K, and a definable group homomorphism f from some definable subgroup G_0 of G into H, with $\ker(f)$ finite central.

Note that $f(G_0)$ has infinite index in H, since the latter has SU-rank $\omega dim(H)$. However, if H_0 is the smallest quantifier-free definable subgroup of H containing $f(G_0)$, then $f(G_0)$ has finite index in H_0, and $SU(G) = SU(H_0)$.

3. Study of types of finite rank. In this chapter we will study types of finite SU-rank. First a reduction to types of SU-rank 1:

(3.1) Proposition. Let $E = acl_\sigma(E)$ and a a tuple with $0 < SU(a/E) < \omega$. Then there is a tuple b independent from a over E, and an element $c \in acl_\sigma(Eab) \setminus acl_\sigma(Eb)$ such that $SU(c/Eb) = 1$.

(3.2) The geometry. Let p be a type of SU-rank 1 over $E = acl_\sigma(E)$, and let P be the set of realisations of p. Then acl_σ can be used to define on P a pre-geometry. Namely, for $A \subseteq P$, define $c\ell(A) = acl_\sigma(EA) \cap P$. Then $c\ell$ satisfies the following properties, for $a, b \in P$ and $A \subseteq P$:

(i) $A \subseteq c\ell(A)$; $c\ell(c\ell(A)) = c\ell(A)$;

(ii) If $a \in c\ell(A \cup \{b\}) \setminus c\ell(A)$, then $b \in c\ell(A \cup \{a\})$;

(iii) If $a \in c\ell(A)$, then $a \in c\ell(B)$ for some finite subset B of A.

The pre-geometry $(P, c\ell)$ will be a geometry if $c\ell(\{a\}) = \{a\}$ for every $a \in P$. Otherwise, one can always quotient by the equivalence relation "having the same closure" to obtain a geometry. There are various types of geometries: disintegrated, non-trivial locally modular, and non-locally modular. A priori this division seems tautological. It turns out however that in many situations this trichotomy corresponds to three completely distinct structure types: in the disintegrated case, there is no structure at all; in the non-trivial locally modular case, there is somewhere a module but no other structure; and in the third case some field is definable.

The properties necessary to obtain this trichotomy, were developped in [HZ]. Since $ACFA$ is unstable, there is another property, weaker than local modularity, which we will use.

(3.3) Various notions of modularity. Let p be a type of rank 1 over E, P the set of its realisations, and let $c\ell$ be defined as above. Recall first that p is trivial, if $c\ell(A) = \bigcup_{a \in A} c\ell(\{a\})$.

(1) p is locally modular if whenever $A, B \subseteq P$, then A and B are independent over $c\ell(A) \cap c\ell(B)$.

(2) p has modular class if whenever $A, B \subseteq P$, then A and B are independent over $acl_\sigma(EA) \cap acl_\sigma(EB)$.

Remark. In a stable context, both notions are equivalent. A trivial type is locally modular. One always has: a locally modular type has modular class. The notion of modular class is connected to one-basedness.

Recall also that two types p and q are orthogonal (denoted by $\perp$), if for every set E containing the sets over which they are defined, if a and b realise non-forking extensions of p and q respectively to E, then $a \mathop{\smile\!\!\!\!\!\!\,|}_E b$. A type is orthogonal to a formula if it is orthogonal to any type containing this formula.

(3.4) Proposition. Let p be a non-trivial type over E, of SU-rank 1, and of modular class. Then p is non-orthogonal to the generic of a definable subgroup of some (simple) commutative algebraic group, i.e., a simple abelian variety, or the multiplicative group $\mathbb{G}_m$, or the additive group $\mathbb{G}_a$; the latter case can only occur in positive characteristic.

4. The trichotomy theorems. As explained above, our hope is that a type of SU-rank 1 would be either locally modular, or that some field would be definable. In characteristic 0, this is indeed the case. In positive characteristic, we obtain a weaker result, but strong enough to still get the semi-minimal analysis of types of finite rank.

(4.1) The trichotomy in characteristic 0. Let p be a type of SU-rank 1 over $E = acl_\sigma(E)$. Then either $p \not\perp (\sigma(x) = x)$, or p is locally modular, stable, stably embedded, and has a unique non-forking extension to any set containinng E.

Also, $p \not\perp (\sigma(x) = x)$ if and only if $deg_\sigma(p) = 1$ and there is an integer N such that $[E(a, \sigma^k(a)) : E(a)] \leq N$ for every $k \in \mathbb{Z}$.

Stably embedded means: (for n the arity of p) if $S \subseteq K^{nm}$ is definable, then $S \cap P^m = S' \cap P^m$ for some S' definable with parameters from P.

Note also that a type can be stably embedded even if it is unstable. Indeed, one can show that if P is the set of realisations of a type p containing the formula $\sigma(x) = x$, then the field generated by P is all of $Fix(\sigma)$. Thus, by (2.4.2), p is stably embedded.

(4.2). This result extends to formulas: if $\varphi(x) \perp (\sigma(x) = x)$, then the set of elements satisfying φ, with the structure inherited from K, is stable and one-based. In the case of groups, this has a striking consequence, by a theorem of Hrushovski-Pillay [HP85]:

Proposition. (char. 0) Let G be a group of finite SU-rank definable in $K \models ACFA$, and assume that the formula defining G is orthogonal to $(\sigma(x) = x)$, and has its paraneters in $E = acl_\sigma(E)$. Let $S \subseteq G^m$ be definable. The S is a Boolean combination of cosets of E-definable subgroups of G^m.

(4.3) The trichotomy in positive characteristic. Let p be a type of SU-rank 1. Then either p has modular class, or p is non-orthogonal to the formula $\sigma^m(x) = x^{p^n}$ for some non-zero $m, n \in \mathbb{Z}$.

Remarks

(1) There are several "fixed" fields in characteristic p, since the Frobenius automorphism $x \mapsto x^p$ is definable. They are all pseudo-finite.

(2) The result obtained in characteristic 0 does not generalise to characteristic $p > 0$. For instance, one can show that the set of realisations of $\sigma(x) = x^p - x$ is unstable, and not

stably embedded either. However, any complete type containing this formula has modular class.

(3) There is a criterion analogous to the one given in characteristic 0 for types non-orthogonal to one of the fixed fields: one replaces algebraic degree by separable degree .

(4) The proof of this result is quite different from the one in zero characteristic. Indeed, one works in a reduct of (K, σ), and looks at the set X of realisations of certain quantifier-free types. On each X^n we put a topology, and show that it satisfies an adapted version of the axioms of Zariski geometries. Then reproduce the proof of [HZ] to obtain a field of rank 1. From the fact that algebraic closure in X is induced by the algebraic closure in K, one obtains eventually a field of SU-rank 1 definable in K, and whose generics are non-orthogonal to the original type. Then use a result of [H91] to deduce that such a field has the desired form.

(4.4) Semi-minimal analysis. Let $E = acl_\sigma(E)$, and a a tuple with $SU(a/E) < \omega$. There are $a_1, \ldots, a_n \in acl_\sigma(Ea)$, such that $a \in acl_\sigma(Ea_1, \ldots, a_n)$, and for every i, either $tp(a_{i+1}/E(a_i)_\sigma)$ has modular class and SU-rank 1, or there is some finite set B, such that the set of realisations of $tp(a_{i+1}/E(a_i)_\sigma)$ is contained in the difference field generated by $E(a_i) \cup B \cup F$, where F is the set of solutions of $\sigma^m(x) = x^{p^n}$ for some $m, n \in \mathbb{Z}$.

References.

[CH] Z.Chatzidakis, E. Hrushovski, The model theory of difference fields, preprint 1996.

[CHP] Z.Chatzidakis, E. Hrushovski, Y. Peterzil, in preparation.

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

[D] J. -L. Duret, Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance, in: Model theory of Algebra and Arithmetic, Pacholski et al. ed., Springer Lecture Notes 834 (1980), 135 –157.

[H91] E. Hrushovski, Pseudo-finite fields and related structures, manuscript 1991.

[H95] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, preprint 1995.

[H96] E. Hrushovski, The first-order theory of the Frobenius, preprint 1996.

[HP85] E. Hrushovski, A. Pillay, Weakly normal groups, in: Logic Colloquium 85, North Holland 1987, 233 – 244.

[HP94] E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. of Math. 85 (1994), 203 –262.

[HZ] E. Hrushovski, B. Zilber, Zariski Geometries, J. of AMS 9 Nr 1 (1996), 1 – 56.

[KP] B. Kim, A. Pillay, Simple theories, to appear in APAL.

[M95] A. Macintyre, Generic automorphisms of fields, to appear in: Proc. AILA-KGS conference (Florence, 1995), A. Lachlan, D. Mundici editors, APAL.

[M97] A. Macintyre, Nonstandard Frobenius, in preparation.