Bijan Afshordel

Generic Automorphisms with Prescribed Fixed Fields

Dissertation zur Erlangung des Doktorgrades
der Fakultät für Mathematik und Physik der
Albert-Ludwigs-Universität Freiburg im Breisgau

Mai 2009

Dekan: Prof. Dr. Kay Kay Königsmann

1. Gutachter: Prof. Dr. Martin Ziegler

2. Gutachter: Prof. Dr. Zoé Chatzidakis

Datum der mündlichen Prüfung: 21. September 2009

Für meine Familie

Contents

Introduction

Model Theory of Fields is a rich and exciting area of mathematical research, manifesting a fruitful interplay between Model Theory and other branches of mathematics such as Number Theory, Algebra and Algebraic Geometry.

Pseudo-finite fields, perfect pseudo-algebraically closed fields with absolute Galois group $\widehat{\mathbb{Z}}$, occur already in the investigation of Ax and Kochen [**3**], [**4**] and [**5**] of diophantine problems over local fields in form of non-principal ultraproducts of finite prime fields. Their systematic study was begun by Ax in [**1**] and [**2**] in the late 1960's. Among other results, Ax proves that a field is pseudo-finite if and only if it is elementarily equivalent to a non-principal ultraproduct of finite fields. Together with the failure of Zil'ber's conjecture, Ax's work motivated the investigation of the model theory of difference fields, i.e. fields with a distinguished automorphism. It turned out that the existentially closed difference fields, also called generic difference fields, form an elementary class, a set of axioms being the theory $ACFA$. Hrushovski [**28**] succeeded in generalising the result of Ax, showing that a difference field is existentially closed if and only if it is elementarily equivalent to a non-principal ultraproduct of difference fields $(\mathbb{F}_p^{\mathrm{alg}}, \phi_p^n)$, where ϕ_p denotes the Frobenius automorphism in characteristic p. It is worthwhile noticing that Hrushovski [**27**] used the model theory of difference fields to give a new proof of the Manin-Mumford conjecture.

The fixed field of a generic difference field is a pure pseudo-finite field. Although one does not need to rely on the aforementioned deep results on ultraproducts, it follows therefrom that any pseudo-finite field is elementarily equivalent to the fixed field of a model of $ACFA$. So given a pseudo-finite field it is natural to ask: is there a model of $ACFA$ having that particular field as fixed field? It is this question which motivates the largest part of the present thesis.

We succeed to give an affirmative answer in theorem (4.24) showing

Theorem A. *Any difference field whose fixed field k is pseudo-finite embeds into a model of $ACFA$ whose fixed field is k.*

More interesting theories of fields have proven to admit a generic automorphism. For example the theory of differentially closed fields of characteristic zero, as shown by Hrushovski (in unpublished work), or that of separably closed fields with a finite named p-basis, proved by Chatzidakis in [**12**]. Actually the same method we use in our proof of Theorem A can

be applied, suitably modified, to show the analogues of Theorem A in the differential field case and the separably closed field case. Though interesting in their own, we do not carry out the proofs in the respective setting, but pass to the following far more general context.

What do the above theories have in common? First, all theories, the (completions of the) theory of algebraically closed fields, the theory of differentially closed fields of characteristic zero, and the theory separably closed fields with finite named p-basis, are stable. All are model complete. All eliminate imaginaries. All of them admit generic automorphisms, by which we mean that the class of existentially closed difference fields, respectively of existentially closed difference-differential fields, respectively of existentially closed difference fields with finite fixed p-basis, forms an elementary class. We call TA the common theory of the respective class and say that TA exists for short. In all the above cases, TA eliminates imaginaries. Also, in all the cases considered above, the fixed field of the generic automorphism (pure, differential or with finite fixed p-basis) is "conservatively embedded over elementary substructures". The notion of conservative embedding was isolated by us in the course of our investigation. Roughly speaking, the fixed field is conservatively embedded over some of its subsets if the automorphism does not induce more structure on the fixed field than there is without the automorphism, if we allow both to use parameters from the specified set.

We succeed in generalising Theorem A to this context and show

Theorem B. *Let T be a countable stable theory with quantifier elimination and elimination of imaginaries. Assume that TA exists and eliminates imaginaries. Let (M, σ) be a model of TA and $K \preccurlyeq_L \mathrm{Fix}(M, \sigma)$ be an L-elementary substructure. If $\mathrm{Fix}(M, \sigma)$ is conservatively embedded over K in (M, σ), then there is some model $(N, \sigma) \equiv (M, \sigma)$ with $\mathrm{Fix}(N, \sigma) = K$.*

On the way we prove some results on generic automorphisms that were known so far only in special cases. As an application we obtain the following extension of Theorem A. It forms our motivation behind Theorem B and answers the above extended question positively.

Theorem A'.

(1) *Any difference field whose fixed field k is pseudo-finite embeds into a model of $ACFA$ whose fixed field is k.*
(2) *Any difference-differential field of characteristic zero whose fixed differential field (k, d) is one-free pseudo-differentially closed embeds into some model of $DCFA$ having (k, d) as fixed differential field.*
(3) *Any difference field whose fixed field k is one-free PAC of Ershov invariant e embeds into some model of $SCFA$ having fixed field k.*

From the model theoretic view point, pseudo-finite fields and generic difference fields form the archetypes of supersimple unstable fields, pure and

with extra structure. The notions of simplicity and supersimplicity were introduced by Shelah and generalise stability and superstability. Algebraically closed fields are superstable. By the famous theorem of Macintyre, Cherlin and Shelah, the converse is also true: an (infinite) superstable field is algebraically closed. At present one seeks for an algebraic characterisation of supersimple fields. Hrushovski [**26**] shows that a field is supersimple if it is a perfect pseudo-algebraically closed field with bounded absolute Galois group. Pillay and Poizat in turn show that a supersimple field is perfect and has bounded absolute Galois group in [**54**]. In 1995, Pillay conjectured that supersimple fields are pseudo-algebraically closed. Needless to say that a proof of this conjecture would establish the desired algebraic characterisation of supersimple fields.

The theorem of Prestel-Frey states that a pseudo-algebraically closed field is never henselian unless it is separably closed. We prove this theorem for fields without the strict order property and obtain the following result on simple fields (corollary 2.3).

Theorem C. *Let K be a simple field. If K is henselian, then K is separably closed.*

Hence the Prestel-Frey Theorem is another property that supersimple fields have in common with perfect bounded pseudo-algebraically closed fields. Theorem C can be seen supporting Pillay's Supersimple-implies-PAC conjecture.

Methods from Galois Cohomology Theory have been used to show that certain varieties over a supersimple field K have K-rational points ([**55**], [**44**], [**41**]). One aspect of the non-commutative theory is the following. To a variety V over a field k one assigns the set of k-isomorphism classes of k^{alg}-isomorphic images of V. This set is called the Weil-Chatelet-set of V over k. It is in bijection to the first Galois Cohomology set of the absolute Galois group of k with values in the group of k^{alg}-automorphisms of V. We generalise this fact to types in an arbitrary first-order theory which have a unique extension to the algebraic closure of their domain. The ambient theory is required only to eliminate imaginaries. After introducing the Weil-Chatelet set of a type p with domain A and the extension property just mentioned, we prove

Theorem D. *For each type p over the parameter set A which has a unique extension to* $\mathrm{acl}(A)$ *there is a bijection*

$$WC\big(p/A\big) \xrightarrow{\Phi} H^1\big(G_A, \mathrm{Aut}(p/\mathrm{acl}(A))\big) \ .$$

Galois Cohomology has already been introduced in Model Theory by Pillay [**51**]. He developed the theory for definable sets in atomic homogeneous models. Our approach is different in that we consider types instead of formulas, and we have only the assumption of elimination of imaginaries.

This thesis is organised as follows. A more detailed description of the chapters is included at the beginning of each chapter.

Chapter one provides preliminaries from Model Theory, Algebra, Algebraic Geometry and Galois Cohomology and in course introduces notation and terminology.

We prove Theorem C in **chapter two**. The right framework to do so, that of V-topological fields, is briefly recalled from the literature. Using a definability result of Koenigsmann on t-henselian fields, we show that a field without the strict order property is not henselian unless it is separably closed. This implies Theorem C.

Chapter three deals with Galois Cohomology of types. We introduce the necessary concepts, such as the Weil-Chatelet set of types, and prove Theorem D.

The greater part of the present thesis begins with **chapter four**, which deals with generic difference fields. We give a brief overview of the basic theory of pseudo-finite fields and generic difference fields in sections 4.1 and 4.2. A proof of Hrushovski's theorem on ultraproducts of Frobenii is included, modulo his analogue of the Lang-Weil estimates for difference fields. The proofs of Theorem A and some variants is carried out in sections 4.3 and 4.4.

Chapter five deals with stable theories with a generic automorphism, and forms the very heart of this thesis. We first discuss the basic model theory of a stable theory with a generic automorphism in section 5.1. We deal with the fixed structure in section 5.2, where we also give a new definition of the PAC property that does not require the surrounding theory be stable. We analyse the relation of our definition to those existing in the literature. Section 5.3 provides the aforementioned field theories and is designed to illustrate the general theory with examples. We prove an analogue for one-free PAC structures of a stable theory of the Elementary Equivalence Theorem for PAC fields in section 5.4. In section 5.5 we introduce the notion of conservative embedding. It will play a key role in our proof of Theorem B. We show that the fixed structure is conservatively embedded over an elementary substructure under a certain condition on the algebraic and definable closures of the involved structures. This condition is always satisfied in the cases of fields and, as will turn out, any substructure of the fixed structure that is itself the fixed structure of some generic automorphism satisfies this condition. Proving conservative embedding of the fixed structure requires us to generalise some results on generic automorphism that have so far not been available in that generality. Using conservative embedding we prove Theorem B and some variants in section 5.6. We obtain a complete characterisation of those structures that occur as fixed structures of a generic automorphism. Theorem A' is then deduced in section 5.7.

Acknowledgements

I would like to thank my advisor Martin Ziegler for giving me the possibility to work in this beautiful area of mathematics, as well as for sharing his mathematical insight.

Zoé Chatzidakis has influenced my work on generic automorphisms with her encouragement as well as her invaluable questions and remarks. For this I feel deeply indebted to her.

I feel grateful to Richard Elwes and Olivier A. Roche for helpful discussions on generic automorphisms, and especially to Olivier for helping me learn Stability Theory.

Jörg Flum and Bernd Siebert have supported me in the academic year 2007/2008, for which I want to express my honest gratitude.

I cannot miss to thank all the mathematics department in Freiburg for providing an open and fertile atmosphere.

Chapter 2 arose from a seminar talk of Jochen Koenigsmann on definability of valuations in henselian fields. I thank him and Markus Junker for their comments.

I am happy to thank the organisers of the Workshop "Model Theory of Fields" at the C.I.R.M. at Luminy in November 2007, Zoé Chatzidakis, Anand Pillay and Francois Loeser, for giving me the opportunity to present parts of the results of Chapter 5 at that conference. The discussions with other participants of proved stimulating and invaluable. In particular I thank Ludomir Newelski for drawing my attention to his articles [**48**] and [**49**].

Allen voran jedoch danke ich meiner Familie und meinen Freunden. Für Euer offenes Ohr, für Eure Unterstützung, und für so vieles mehr.

Parts of the results of Chapter 5 have been submitted for publication to The Journal of Symbolic Logic.

CHAPTER 1

Preliminaries

This chapter collects preliminary results that we will use in the thesis. It serves also to fix terminology as well as notation.

1.1. Model Theory

Our main reference for Model Theory are the books of Hodges [**30**], Poizat [**56**] and Tent and Ziegler [**70**]. We will use the following notation for Model Theory. L denotes a first order language and T a complete L-theory with infinite models. They might be many-sorted, and we pass to T^{eq} whenever necessary. We are not going to distinguish between language and vocabulary, that is to say we choose formulas φ from L, or let L be a certain set of predicate, function and constant symbols, depending on the context. Also we make no notational distinction between L-structures and their base sets, so M will stand for a model of T as well as for the underlying universe. $\bar{x}$, $\bar{y}$ and $\bar{z}$ denote possibly infinite tuples of variables. We write $\bar{a}$, $\bar{b}$ etc. and simply AB and $A\bar{a}$ for $A \cup B$ and $A \cup \{a_1, \ldots, a_n\}$ respectively. $\mathrm{acl_T}$ and $\mathrm{dcl_T}$ denote algebraic and definable closure in models of T. We sometimes write acl and dcl if no confusion can arise. Types are called $p, q, \ldots$ and will be complete, unless we say partial type. The type of the tuple $\bar{a}$ over the parameter set A in the model M is denoted by $\mathrm{tp}_M(\bar{a}/A)$ or $\mathrm{tp}_T(\bar{a}/A)$ or just $\mathrm{tp}(\bar{a}/A)$ if reference to the model M is dispensable. If Δ is a finite set of L-formulae $\varphi_i(\bar{x}; \bar{y}_i)$, we write $\mathrm{tp}_\Delta(\bar{a}/A)$ for the Δ-type of $\bar{a}$ over A. The space of types over a parameter set A is denoted by $S(A)$, so that $S(A) = \bigcup_{n\geq 1} S_n(A)$. $\bar{a} \equiv_A \bar{a}'$ abbreviates that $\bar{a}$ and $\bar{a}'$ have the same type over A. By a definable set we mean a set that is definable with parameters. If we want to specify that a definable set X is definable using parameters from A we say that X is A-definable, or definable over A. A type-definable set (subset of some model) is the set of realizations of some partial type. If M is a model and $A \subset B$ are parameter sets contained in M, we write $\mathrm{Aut}_T(B/A)$ or simply $\mathrm{Aut}(B/A)$ for the group of automorphisms of M that fix A pointwise. $\mathrm{Gal}(A)$ denotes the group of elementary permutations of the algebraic closure $\mathrm{acl}(A)$ of A fixing A pointwise. We sometimes call it the Galois group of A.

Only for convenience we assume the existence and uniqueness of a "very big" saturated model of T, the monster model $\mathfrak{C}$. Its universe is not a set but a proper class (so $\mathfrak{C}$ is not a structure in the usual sense) where all types over all subsets are realized. We are aware that there are some difficulties with this assumption, but one never really needs the monster, and to say it with the words of Angus Macintyre [**40**]: "I remark that, unlike ..., I

disregard set-theoretic issues ... in complete confidence that I can, if need be, employ basic metamathematical hygiene to cope with any irritations."

The monster model can be characterised by

(1) Every model of T is elementarily embeddable into $\mathfrak{C}$.
(2) Every partial elementary isomorphism between two subsets can be extended to an automorphism of $\mathfrak{C}$.

Consequently we assume that all parameter sets are subsets of $\mathfrak{C}$ and all models of T, usually denoted by M and N, are elementary substructures of $\mathfrak{C}$ (by which we mean that for any L-formula with parameters in M that is satisfied in $\mathfrak{C}$ is satisfied in M).

Classically, simplicity of a theory is defined via dividing and forking of formulas. However we take the equivalent characterisation of Kim and Pillay from [**31**] as definition. Needless to say that the latter generalises the notion of algebraic independence in algebraically closed fields.

DEFINITION 1.1. *Let T be a first order theory and $\mathfrak{C}$ be its monster model. T is said to be simple if and only if there is some ternary relation $\downarrow$ on subsets of $\mathbb{C}$ which satisfies the following properties.*

(1) *(Invariance) $\downarrow$ is invariant under automorphisms of $\mathbb{C}$.*
(2) *(Symmetry) $\bar{a} \underset{A}{\downarrow} \bar{b}$ if and only if $\bar{b} \underset{A}{\downarrow} \bar{a}$ for any (finite) tuples $\bar{a}$ and $\bar{b}$ and any parameter set A.*
(3) *(Transitivity) Suppose that $A \subseteq B \subseteq C$. Then $\bar{a} \underset{A}{\downarrow} C$ if and only if $\bar{a} \underset{A}{\downarrow} B$ and $\bar{a} \underset{B}{\downarrow} C$.*
(4) *(Local Character) For any finite tuple $\bar{a}$ and any parameter set A there is $A_0 \subseteq A$ of cardinality at most that of T such that $\bar{a} \underset{A_0}{\downarrow} A$.*
(5) *(Finite Character) $\bar{a} \underset{A}{\downarrow} B$ if and only if $\bar{a} \underset{A}{\downarrow} \bar{b}$ for any finite tuple $\bar{b}$ from B.*
(6) *(Extension) For any $\bar{a}, A$ and $B \supseteq A$ there is some $\bar{a}' \equiv_A \bar{a}$ such that $\bar{a}' \underset{A}{\downarrow} B$.*
(7) *(The Independence Theorem over Models) Let M be a model of T and A and B parameter sets containing M with $A \underset{M}{\downarrow} B$. Assume that $\bar{a}_1 \equiv_M \bar{a}_2$ and that $\bar{a}_1 \underset{M}{\downarrow} A$ and $\bar{a}_2 \underset{M}{\downarrow} B$. Then there is $\bar{a}_3$ realizing $\mathrm{tp}(\bar{a}_1/A) \cup \mathrm{tp}(\bar{a}_2/B)$ such that $\bar{a}_3 \underset{M}{\downarrow} AB$.*

If $A \underset{B}{\downarrow} C$ we say that A is independent from C over B, and call $\downarrow$ the non-forking independence relation of T. A simple theory is said to be supersimple if in property (4) A_0 is finite. A structure is called simple (supersimple) if its theory is simple (supersimple).

Our standard reference for simple theories is Wagner's book [**71**]. Archetypical examples of simple (unstable) structures are pseudo-finite fields and

generic difference fields, where independence is coming from algebraic independence in algebraically closed fields (see chapter 4), as well as the random graph. Simple theories do not have the strict order property:

DEFINITION 1.2. *A formula $\varphi(x, y)$ is said to have the strict order property (in some model) if it defines a partial order with arbitrarily long chains (in that model). A theory T is said to have the strict order property if some formula has it in some model of T.*

Stable theories are examples of simple theories, though historically preceded them. A simple theory is stable if any type over an algebraically closed set (in T^{eq}) is stationary. This stationarity property strengthens the Independence Theorem over Models. We are not going to recall stability theory but use freely the results about stable theories. Our main reference for stability theory are Ziegler's lecture notes [**74**], the classical reference being of course Shelah's book [**67**]. Only the two following points desire special mention.

First let T be a complete theory. T is said to be quantifier-free stable if for all cardinals λ with $\lambda^{|T|} = \lambda$ and any parameter set A of size λ there are at most λ quantifier-free types over A. Equivalently, every quantifier-free formula has finite Δ-rank for all finite sets Δ of quantifier-free formulas. If T is countable, then for any quantifier-free formula φ there is some quantifier-free type π in φ that is locally isolated. All this is proved by standard arguments.

Second we would like to mention the following theorem due to Lachlan. We have come to know it after the proof of our main theorem (theorem (5.65)) was completed. Let T be an L-theory. If $P(x)$ is a (unary) predicate of L and A is a set of parameters, the pair (P, A) is said to have the Tarski-Vaught-property if for any consistent $L(A)$-formula $\varphi(x)$ implying $P(x)$ there is $a \in A$ satisfying φ.

THEOREM 1.3 (Lachlan). *Let T be a countable stable theory. Let P be a predicate and A be a set such that (P, A) has the Tarski-Vaught-property. Then there is some model M of T such that $P(M) = P(A)$.*

Proof. Lachlan proved this in [**33**] (compare [**48**]). For the convenience of the reader we give a possible proof here.

As T is countable, we may choose some model M of T that is locally atomic over A. We claim that $P(M) = P(A)$. To see this, choose $m \in P(M)$ and consider the type $p = \mathrm{tp}(m/A)$. As p is locally isolated there is some formula $\delta \in p$ that isolates $p|_\Delta$, where $\Delta = \{P(x), x = y\}$. Then $\delta \models P(x)$, so by the Tarski-Vaught-property there is $a \in A$ realizing δ. Thus $x = a \in p$ and finally $m = a \in A$. □

Galois Theory. We recall Poizat's Galois Theory for imaginaries from his book [**56**] and his original article [**57**], with particular emphasis on procyclic profinite Galois groups. These results are well-known, we state them mainly for future reference.

Recall that a profinite group is a compact, Hausdorff and totally disconnected topological group. Any projective limit of finite groups is a profinite group, and conversely any profinite group can be written as a projective limit of finite groups. We denote by $\widehat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$, which is the projective limit of the groups $\mathbb{Z}/n\mathbb{Z}$, $n \geq 1$, with respect to the canonical projection $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ for $m|n$. A profinite group G is called procyclic if it is the projective limit of finite cyclic groups, or equivalently, if there is some epimorphism (of profinite groups) $\widehat{\mathbb{Z}} \longrightarrow G$.

We note that the term procyclic group is used only for profinite groups in the present thesis.

The following well-known facts on procyclic groups, which we state for future reference, can be found in [**61**] and [**62**].

LEMMA 1.4. *Let G be a profinite group.*

(1) *G is procyclic if and only if for any $n \in \mathbb{N}$ there is at most one closed subgroup H of G of index n.*
(2) *$G \cong \widehat{\mathbb{Z}}$ if and only if for all $n \in \mathbb{N}$ there is exactly one closed subgroup H of G of index n.*
(3) *An epimorphism $\widehat{\mathbb{Z}} \longrightarrow G$ is an isomorphism if and only if $G \cong \widehat{\mathbb{Z}}$.*
(4) *Let G be procyclic and $f : G \longrightarrow H$ be an epimorphism. Then the following are equivalent:*
   (a) *f is an isomorphism.*
   (b) *For all $n \in \mathbb{N}$, if G has a closed normal subgroup of index n, then so does H.*

Needless to say that in (1) and (2) the subgroup H is normal.

REMARK 1.5. *If $G \longrightarrow H$ is an epimorphism of procyclic profinite groups, then any topological generator of H lifts to a topological generator of G.*

The profinite group G is said to be bounded, or small, if for any $n \in \mathbb{N}$ there are only finitely many open normal subgroups of G of index n.

REMARK 1.6. *If G is a bounded profinite group, then any epimorphism $G \longrightarrow G$ is an isomorphism. See [**62**].*

Let T be a complete L-theory, possibly many-sorted, with elimination of imaginaries. Recall that for two parameter sets $A \subseteq B$, B is said to be normal over A if B is setwise invariant under $\mathrm{Aut}_T(\mathfrak{C}/A)$, or equivalently if for all $b \in B$, whenever $c \models \mathrm{tp}_T(b/A)$, then $c \in B$.

As mentioned before we let $\mathrm{Gal}(A)$ denote the group of elementary permutations of $\mathrm{acl_T}(A)$ leaving A pointwise fixed. $\mathrm{Gal}(A)$ is a profinite group with respect to the topology of pointwise convergence. For a subgroup H of $\mathrm{Gal}(A)$ we let

$$\mathrm{Fix}(\mathrm{acl_T}(A), H)$$

be the set of elements of $\mathrm{acl_T}(A)$ which are fixed by any element of H. Clearly $\mathrm{Fix}(\mathrm{acl_T}(A), H) = \mathrm{Fix}(\mathrm{acl_T}(A), \bar{H})$ and $\mathrm{Fix}(\mathrm{acl_T}(A), H)$ is a $\mathrm{dcl_T}$-closed subset of $\mathrm{acl_T}(A)$. If H is (topologically) generated by a single element σ, we also write $\mathrm{Fix}(\mathrm{acl_T}(A), \sigma)$ instead of $\mathrm{Fix}(\mathrm{acl_T}(A), < \sigma >)$.

For a subset B of $\mathrm{acl_T}(A)$ containing A we write $\mathrm{Gal}(\mathrm{acl_T}(A)/B)$ for the subgroup of $\mathrm{Gal}(A)$ of elements that leave B pointwise fixed. The following theorem is known as the Main Theorem of Galois Theory:

THEOREM 1.7 (Poizat). *Let T be a complete L-theory, possibly many-sorted, with elimination of imaginaries, and let A be a parameter set.*

$\mathrm{Fix}(\mathrm{acl_T}(A), -)$ *and* $\mathrm{Gal}(\mathrm{acl_T}(A), -)$ *are antitone lattice isomorphisms between closed subgroups of* $\mathrm{Gal}(A)$ *and* $\mathrm{dcl_T}$*-closed subsets of* $\mathrm{acl_T}(A)$ *that contain A. Under this isomorphism, closed normal subgroups correspond to* $\mathrm{dcl_T}$*-closed B which are normal over A. One has*

$$\mathrm{Fix}\big(\mathrm{acl_T}(A), \mathrm{Gal}(\mathrm{acl_T}(A)/B)\big) = \mathrm{dcl_T}(B)$$

for any $A \subseteq B \subseteq \mathrm{acl_T}(A)$ and

$$\mathrm{Gal}\big(\mathrm{acl_T}(A)/\mathrm{Fix}(\mathrm{acl_T}(A), H\big) = \bar{H}$$

for any subgroup H of $\mathrm{Gal}(A)$.

The following is known as the Primitive Element Theorem.

THEOREM 1.8 (Poizat). *Let T be a complete L-theory, possibly many-sorted, with elimination of imaginaries, and let A be a parameter set. Then for any open subgroup H of* $\mathrm{Gal}(A)$ *there is some finite tuple $\bar{b} \in \mathrm{acl_T}(A)$ such that*

$$\mathrm{Fix}(\mathrm{acl_T}(A), H) = \mathrm{dcl_T}(A\bar{b})\,.$$

Recall that a tuple $\bar{b}$ is said to have degree $n \in \mathbb{N}$ over A if $\bar{b}$ has exactly n A-conjugates. $\bar{b}$ has degree n over A if and only if $\mathrm{tp}_T(\bar{b}/A)$ has degree n, if and only if any $L(A)$-formula isolating $\bar{b}$ over A has exactly n solutions (in any model of T containing A).

COROLLARY 1.9. *Let T be a complete L-theory, possibly many-sorted, with elimination of imaginaries, and let A be a* $\mathrm{dcl_T}$*-closed parameter set. Assume that* $\mathrm{Gal}(A)$ *is procyclic. Then the tuple $\bar{b} \in \mathrm{acl_T}(A)$ has degree $n \in \mathbb{N}$ over A if and only if* $\mathrm{Gal}(\mathrm{dcl_T}(\bar{b}A)/A)$ *is cyclic of order n if and only if* $\mathrm{Gal}(\mathrm{dcl_T}(\bar{b}A)/A)$ *is the unique quotient of* $\mathrm{Gal}(A)$ *of order n.*

Furthermore the following are equivalent:

1. $\mathrm{Gal}(A) \cong \widehat{\mathbb{Z}}$.
2. *for all $n \in \mathbb{N}$ there is a* $\mathrm{dcl_T}$*-closed set $D \subset \mathrm{acl_T}(A)$ that is normal over A and such that $H = \mathrm{Gal}(\mathrm{acl_T}(A)/D)$ has index n in* $\mathrm{Gal}(A)$.
3. *For all $n \in \mathbb{N}$ there is $\bar{a} \in \mathrm{acl_T}(A)$ whose type over A has degree n.*
4. *For all $n \in \mathbb{N}$ there is $\bar{a} \in \mathrm{acl_T}(A)$ with exactly n conjugates over A.*
5. *For all $n \in \mathbb{N}$ there is a complete (algebraic) $L(A)$-formula $\varphi(\bar{x})$ with exactly n realizations (in a model of T containing A).*

As for fields, we call a parameter set A one-free if $\mathrm{Gal}(A) \cong \widehat{\mathbb{Z}}$.

1.2. Field Theory and Algebraic Geometry

All fields are assumed to live inside a fixed universal domain which is an algebraically closed field of characteristic p (a prime number or 0) of very large transcendence degree. $\mathbb{F}_p$ denotes the prime field of characteristic p, setting $\mathbb{F}_0 = \mathbb{Q}$. For a field K, we write K^{alg}, K^{sep} and K^{1/p^∞} for the algebraic, separable and inseparable closure of K (inside the universal domain), respectively. K^{1/p^∞} is also called the perfect closure or perfect hull of K. $\text{abs}(K)$ denotes the absolute part of K, which is $K \cap \mathbb{F}_p^{\text{alg}}$ if $\text{char}(K) = p$. If R is any ring we denote by ϕ_p the Frobenius endomorphism of R sending x to x^p if the characteristic p is positive (and the identity if the characteristic is zero). Similarly ϕ_q denotes the endomorphism sending x to x^q for any power $q = p^n$ of p. For a field extension L/K, not necessarily finite, $\text{Aut}(L/K)$ denotes the group of automorphisms of L over K. If L/K is Galois, we write $\text{Gal}(L/K)$ instead of $\text{Aut}(L/K)$, the Galois group of L/K. $\text{Gal}(K)$ denotes the absolute Galois group $\text{Gal}(K^{\text{sep}}/K)$ of K. It is a profinite group in a natural way, which we sometimes identify with $\text{Aut}(K^{\text{alg}}/K)$. For a finite field extension L/K we denote the degree of the extension by $[L : K]$. For a ring R and a possibly infinite tuple of variables $\bar{X}$ we write $R[\bar{X}]$ for the polynomial ring over R in $\bar{X}$. All we present in this section is well-known and can be found in at least one of the following books: [**34**], [**35**], [**22**], [**45**], [**64**], [**65**] [**24**], [**47**], [**46**] (of course we give references below).

Linear Disjointness. Let F_1 and F_2 be two field extensions of a field K (all contained in a common overfield). F_1 is called called linearly disjoint from F_2 over K if any $a_1, \ldots, a_n \in F_1$ that are linearly independent over K are linearly independent over F_2. Equivalently, the canonical morphisms of K-vector spaces $F_1 \otimes_K F_2 \longrightarrow F_1[F_2]$ is an isomorphism. If F_1 are linearly disjoint from F_2 over K, then F_2 is linearly disjoint from F_1 over K. So we may (and will) say that two field extensions F_1 and F_2 are linearly disjoint over K. Let $K \subseteq L \subseteq F_1$ and F_2/K be field extensions. Then F_1 and F_2 are linearly disjoint over K iff F_2 and L are linearly disjoint over K and F_2L and F_1 are linearly disjoint over L. If the fields F_1 and F_2 are linearly disjoint over K, then they are algebraically independent over K. The converse is true if the field K is algebraically closed (page 57, corollary 3 and theorem 3 of chapter 3 in [**34**]). We will need the following well-known criterion, which we state as a lemma for future reference.

LEMMA 1.10. *If F_1/K is Galois, then $F_1 \cap F_2 = K$ if and only if F_1 and F_2 are linearly disjoint over K.*

Regular and Separable Field Extensions. Let F be a finitely generated field extension of K. F is said to be separably generated over K if there is a transcendence basis $\bar{t} = t_1, \ldots, t_d$ of F over K such that F is separably algebraic over $K(\bar{t})$. Such a transcendence basis is called a separating transcendence basis of F over K. A subset B of the field K is said to be p-independent if for any $b_1, \ldots, b_n \in B$ the family of p-monomials $b_1^{i_1} \ldots b_n^{i_n}$ with $0 \leq i_\nu \leq p-1$ are linearly independent over K^p. A maximal

p-independent subset of K is called a p-basis. $[K : K^p] = p^e$ for any field K, where $e \in \mathbb{N} \cup \{\infty\}$ is the size of a (equivalently every) p-basis of K. It is called the Ershov invariant or the degree of imperfection of K. We denote it as $er(K)$.

A field extension F/K is said to be separable if F is linearly disjoint from K^{1/p^∞} over K. One has the following characterisation of separability.

THEOREM 1.11. *For a field extension F/K, the following are equivalent:*

1. *F/K is separable.*
2. *Any finitely generated subextension $F \supseteq L \supseteq K$ has a separating transcendence basis over K.*
3. *F is linearly disjoint from K^{1/p^n} over K, for some $n \geq 1$.*
4. *Any p-independent subset of K is p-independent in F.*

Proof. For the equivalence of (1), (2), and (3) see page 53, theorem 1 of chapter 3 in [**34**]. The equivalence of (4) and (1) is the content of theorem (26.9) of [**45**] (with theorem (26.5) ibid). □

Note that if K is a perfect field, then any field extension of K is separable. It follows from (4) of the previous theorem that if L/K is a separable extension, then $er(L) \geq er(K)$. If either is finite, then $er(L) = er(K)$ if and only if L/K is separably algebraic (see [**22**], lemma (2.7.3)).

A field extension F/K is said to be regular if F is linearly disjoint from K^{alg} over K. One has the following characterisation of regular field extensions.

THEOREM 1.12. *For a field extension F/K, the following are equivalent:*

1. *F/K is regular.*
2. *F/K is separable and K is relatively algebraically closed in F.*
3. *F/K is separable and the restriction map*

$$\text{res} : \text{Gal}(F) \longrightarrow \text{Gal}(K)$$

of absolute Galois groups is surjective.

Proof. For the equivalence of (1) and (2) see page 56, theorem 2 of chapter 3 in [**34**]. Let us show the equivalence of (1) and (3). If F/K is regular, then by definition F/K is separable. As F and K^{alg} are linearly disjoint over K, any $\sigma \in \text{Gal}(K)$ lifts to an automorphism α of FK^{sep} which is the identity on F, by the universal property of tensor products. α in turn lifts to an automorphism of F^{sep} over F.
For the converse, assume that F/K is separable and the restriction map of absolute Galois groups is surjective. We will show that K is algebraically closed in F. So let $\alpha \in K^{\text{alg}}$. As F/K is separable, we may assume that α is separably algebraic over K. If $\alpha \notin K$, there is some automorphism $\sigma \in \text{Gal}(K)$ moving α. But σ lifts to some $\tilde{\sigma} \in \text{Gal}(F)$, so $\alpha \notin F$. □

F/K is primary if F is linearly disjoint from K^{sep} over K. As K^{sep} and K^{1/p^∞} are linearly disjoint over K and $K^{\text{alg}} = K^{\text{sep}}K^{1/p^\infty}$, F/K is regular if and only if it is separable and primary.

THEOREM 1.13. *Let $K \subseteq L \subseteq F$ be a tower of field extensions. If F/K is regular resp. separable resp. primary, then so is L/K. If L/K and F/L are separable resp. regular, then so is F/K.*

Proof. The first assertion follows immediately from the definition. For the second, see corollaries 1 and 2 on page 54 of chapter 3 in [**34**] for the separability, and use this and the previous theorem for regularity. □

Finally we mention absolutely prime ideals and affine K-algebras, where K is a field. K is still a field. An affine K-algebra is by definition a finitely generated K-algebra which is an integral domain whose quotient field is a regular extension of K. The K-algebra A is an affine K-algebra if and only if $A \otimes_K K^{\mathrm{alg}}$ is an integral domain. In the terminology of Ax in [**2**], affine K-algebras are finitely generated absolutely entire K-algebras. An ideal I in a K-algebra A is called absolutely prime if $I \otimes_K K^{\mathrm{alg}}$ is prime in $A \otimes_K K^{\mathrm{alg}}$. Any affine K-algebras is the quotient of some polynomial ring by an absolutely prime ideal.

Varieties and PAC Fields. A variety V over a field K is an integral separated scheme of finite type over K which remains integral after extending scalars to K^{alg}. Affine varieties over K correspond to affine K-algebras. To be more precise, the category of affine K-algebras is equivalent to the category of affine varieties over K (see for example [**47**], proposition 4 of Chapter II, §4). If L is a field containing K, then V_L denotes the variety obtained by base extension to L. Notice that our varieties are called absolutely irreducible or geometrically irreducible by some authors. For a K-algebra R and a variety V over K, an R-valued point of V is a morphism $\mathrm{Spec}(R) \longrightarrow V$ of schemes over K. If $R = L$ is an algebraic field extension of K, an L-valued point will be called an L-rational point. We write $V(R)$ for the set of R-valued points of V.

DEFINITION 1.14. *A field K is called pseudo-algebraically closed, PAC for short, if any variety over K has a K-rational point.*

We take a moment to translate this condition to the solvability of systems of polynomial equations with coefficients in K. Certainly the field K is PAC if and only if any affine variety over K has a K-rational point, as any variety is covered by open affines. Consider the affine variety V over K, say embedded in $\mathbb{A}^n$, for some $n \in \mathbb{N}$, given by the equations

$$f_1(\bar{X}) = \cdots = f_r(\bar{X}) = 0$$

with coefficients in K. As the category of affine varieties over K is equivalent to the category of affine K-algebras, to give a K-rational point on V is the same as to give a morphism of K-algebras

$$K[\bar{X}]/I \longrightarrow K \ ,$$

where I denotes the ideal generated by the polynomials $f_1, \ldots, f_r$. This is in turn the same as to give a maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$ in $K[\bar{X}]$. Note that the a_i lie in K. Thus we see that to give a K-rational point on V is nothing but giving a tuple $\bar{a} \in K$ which solves the polynomial system of equations $f_1(\bar{X}) = \cdots = f_r(\bar{X}) = 0$.

Conversely, if a field K has the property that any system of polynomial equations

$$f_1(\bar{X}) = \cdots = f_r(\bar{X}) = 0$$

has a solution $\bar{a}$ in K whenever $(f_1, \ldots, f_r) \subseteq K[\bar{X}]$ is an absolutely prime ideal, then K is PAC. This is seen by the same arguments as above.

Note that the system of equations

$$f_1(\bar{X}) = \cdots = f_r(\bar{X}) = 0$$

defines a unique n-type in the theory ACF (of Morley-rank equal to the dimension of the variety defined by these equations) by quantifier elimination of ACF. Regarding however the theory of K, we have just seen that K is PAC if and only if whenever I is an absolutely prime ideal, the set of formulas

$$\Sigma_I = \{f(\bar{x}) = 0 \mid f \in I\}$$

with coefficients in K is finitely satisfiable in K. Of course, the set of variables need not be finite.

We have proved the equivalence of (1), (2), (3) and (7) of the following theorem:

THEOREM 1.15. *Let K be a field. Then the following are equivalent:*

(1) *K is a PAC field.*
(2) *Any affine variety over K has a K-rational point.*
(3) *For any affine K-algebra A there is a homomorphism of K-algebras $A \longrightarrow K$.*
(4) *Any curve over K has a K-rational point.*
(5) *Any affine plane curve over K has a K-rational point.*
(6) *For any absolutely irreducible polynomial $f(X, Y) \in K[X, Y]$ there are $a_1, a_2 \in K$ such that $f(a_1, a_2) = 0$.*
(7) *For any cardinal κ, the set Σ_I is finitely satisfiable in K for any absolutely prime ideal in $K[X_\nu \mid \nu < \kappa]$, the polynomial ring over K in κ-many variables.*
(8) *K is existentially closed in regular field extensions.*

Moreover, it is an elementary property for a field to be PAC.

Proof. The equivalence of (1), (2), (3) and (7) have been shown above. (6) is just a reformulation of (5) because $K[\bar{X}]$ is catenary for any field K. The equivalence of (1) and (5) is the content of theorem (11.2.5) in [**22**]. To see that (4) is equivalent to (5), one uses theorem (11.1.1) of [**22**], which states that a field K is PAC if and only if for any variety V over K the set of K-rational points is dense in V (with respect to the K-Zariski topology), as well as the well-known fact that any curve C over a field K is birational over K to a plane curve over K. To see that (1) is equivalent to (8), note that we may restrict attention to finitely generated regular extensions. So because affine varieties over K correspond to affine K-algebras, this equivalence reduces to the equivalence of (1), (2) and (3), which we have proved above.

For the moreover part, we refer to [**22**], proposition (11.3.2). □

Note that by compactness, we get that a κ-saturated field K is PAC if and only if any absolutely entire K-algebra A of size less than κ admits a K-algebra homomorphism $A \longrightarrow K$.

We finally mention the famous theorem of Lang-Weil estimating the number of rational points on varieties over finite fields.

THEOREM 1.16 (Lang-Weil). *For any positive integers n and d there is a constant C such that for any finite field $\mathbb{F}_q$ and any variety V defined by polynomials of degree at most d in the variables $X_1, \ldots, X_n$ with coefficients from $\mathbb{F}_q$*

$$\left| \; |V(\mathbb{F}_q)| - q^{dim(V)} \; \right| \leq C \, q^{dim(V)-1/2} \; .$$

1.3. Galois Cohomology

In this section we will briefly recall some of the basics from non-abelian Galois Cohomology, such as can be found in Serre's book [**68**].

Let G be a profinite group. A G-set A is a discrete topological space on which G acts continuously, which amounts to $(\sigma\tau).x = \sigma.(\tau.x)$ and $1.x = x$ for all $\sigma, \tau \in G$ and $x \in A$, and

$$A = \bigcup_{U \leq G \text{ open}} A^U \; .$$

Here A^U denotes the set of elements in A fixed by all $\sigma \in U$. The action of G on A is often called μ.

A G-set A is called a G-group, or a G-module, if A is a group and if μ is compatible with the group operation $\circ$ of A. Explicitly this means that $\sigma.(x \circ y) = \sigma.x \circ \sigma.y$ all $x, y \in A$ and all $\sigma \in G$. To give A the structure of a G-group μ (i.e. to give an action of G on A which is compatible with the group structure of A) is the same thing as to give a continuous homomorphism of groups

$$\varphi_\mu : G \longrightarrow \mathrm{Aut}(A) \; ,$$

where $\mathrm{Aut}(A)$ is the group of group automorphisms of A endowed with the topology of pointwise convergence.

For a G-set A, we let

$$H^0(G, A) := A^G$$

be the set of elements of A that are invariant under the action of G. If A is a G-group, then of course $H^0(G, A)$ is a group.

If A is a G-group, one calls a continuous 1-cocycle, or simply a continuous cocycle, of G in A a continuous map

$$f : G \longrightarrow A$$

such that $f(\sigma\tau) = f(\sigma) \circ \sigma.f(\tau)$ for all $\sigma, \tau \in G$. $Z^1(G, A)$ denotes the set of continuous cocycles of G in A. For example, one calculates easily that if $a \in A$ then $f : G \longrightarrow A : \sigma \mapsto a^{-1} \circ \sigma.a$ defines a continuous cocycle. We remark that all cocycles that we consider in this thesis will be continuous,

and we will sometimes just say cocycle instead of continuous cocycle. Two continuous cocycles f and g are called cohomologuous if there is some $b \in A$ such that

$$f(\sigma) = b^{-1} \circ g(\sigma) \circ \sigma.b$$

for all $\sigma \in G$. One calculates that this defines an equivalence relation on the set of continuous cocycles $Z^1(G, A)$. Its set of equivalence classes

$$H^1(G, A) := Z^1(G, A)/\sim$$

is called the first cohomology set of G in A. It possesses a distinguished element, namely the class of the unit cocycle (which sends every element of G to $1 \in A$), which turns $H^1(G, A)$ into a pointed set.

Let us note that for any continuous cocycle $f : G \longrightarrow A$, the set $f^{-1}(1)$ is an open subgroup of G. Indeed, using the cocycle condition and $1 \circ 1 = 1$ one verifies that $f(1) = f(1) \circ f(1)$, so that $f(1) = 1$. For arbitrary $\tau \in G$, it follows, using $\tau \circ \tau^{-1} = 1$, that $f(\tau^{-1}) = \tau^{-1}.f(\tau)^{-1}$. So if $\sigma, \tau \in f^{-1}(1)$, then $f(\sigma\tau^{-1}) = 1$ as $\tau.1 = 1$ for any $\tau \in G$. Thus $f^{-1}(1)$ is a subgroup of G. It is open because A carries the discrete topology.

Note that to give a continuous cocycle $f : G \longrightarrow A$ is the same as to give a continuous lift of the identity

$$\begin{array}{ccc} G & \xrightarrow{f'} & A \rtimes_\varphi G \\ & \searrow^{=} & \downarrow \mathrm{pr} \\ & & G \end{array}$$

where the semi-direct product is taken with respect to the action of G on A. Indeed, if f is a continuous cocycle, then $f'(\sigma) := f(\sigma)\sigma$ defines a continuous lift, and if f' is such, then $f(\sigma) := \mathrm{pr}_A(f'(\sigma)\sigma^{-1})$ is a continuous cocycle of G in A. Here pr_A denotes of course the projection of $A \rtimes_\varphi G$ onto A.

EXAMPLE 1.17. *We are particularly interested in the following example. Let k be a perfect field and V a variety over k. A k^{alg}-form of V is a variety W over k that is isomorphic to V over k^{alg}. If k is not algebraically closed, two k^{alg}-forms of V may or may not be isomorphic over k. The set of k-isomorphism classes of k^{alg}-forms of V is called the Weil-Chatelet set of V over k, noted $WC(V/k)$.*

*Now let $G = \mathrm{Gal}(k)$ be the absolute Galois group of k and consider the group $A = \mathrm{Aut}_{k^{\mathrm{alg}}}(V_{k^{\mathrm{alg}}})$ of rational automorphisms of $V_{k^{\mathrm{alg}}}$ over k^{alg}. Endowed with the discrete topology, it is a G-module in a natural way. G acts naturally on $W(k^{\mathrm{alg}})$ for any variety W over k. Therefore, if $\varphi : V \longrightarrow W$ is a k^{alg}-isomorphism of V onto a k^{alg}-form W of V, we obtain a continuous cocycle of G with values in A by mapping σ to $\varphi^{-1}\sigma\varphi\sigma^{-1}$. If V is quasi-projective, this yields a bijection between $WC(V/k)$ and $H^1(k, \mathrm{Aut}_{k^{\mathrm{alg}}}(V_{k^{\mathrm{alg}}}))$ (see for example [**68**], proposition 5 in Chapter III, § 1). Our aim in chapter 3 is to establish this correspondence for types having only one extension to the algebraic closure of their domain.*

1.4. Difference Algebra

The proof of theorem (4.24) given in chapter 4 uses difference algebra/geometry. We introduce the relevant material from the literature, mainly from Cohn's book [**17**].

Difference Rings and Difference Fields. A difference ring is a pair (R, σ) consisting of a (commutative unitary) ring R and an endomorphism σ of R. We follow the convention made by several authors and require the endomorphism σ to be injective. If R is a field we call (R, σ) a difference field. For $f \in R$ the element $\sigma^n(f)$ is called the n^{th} transform of f. Homomorphisms of difference rings are ring homomorphisms compatible with the endomorphisms, as one expects, as well as extensions and substructures of difference rings and fields. All attributes of the underlying rings and ring homomorphisms are used for difference rings and homomorphisms of difference rings as well. For example, if the underlying field of a difference field (K, σ) is algebraically closed, we call (K, σ) an algebraically closed difference field, or if the underlying field extension L/K of the difference field extension $(L, \tau)/(K, \sigma)$ is algebraic, we call $(L, \tau)/(K, \sigma)$ an algebraic difference field extension.

We will often abuse notation and write (L, σ) for an extension of (K, σ), or even omit the endomorphism from the notation and just write R instead of (R, σ).

If S/R is an extension of difference rings and A is a subset of S, we denote by $R[A]_\sigma$ the difference ring generated by A over R, which is the smallest difference subring of S containing A and R. If A is just a finite tuple of elements $\bar{a}$, we write $R[\bar{a}]_\sigma$. In case both S and R are fields, we write $R(A)_\sigma$ and $R(\bar{a})_\sigma$ for the difference field generated by A and $\bar{a}$ over R respectively. Difference fields of the form $k(\bar{a})_\sigma$, with $\bar{a}$ a finite tuple, are called finitely generated over k. They need not be finitely generated over k as pure fields. Take for example a sequence $(t_\nu)_{\nu \in \mathbb{N}}$ of elements of $\mathbb{C}$ that are algebraically independent over $\mathbb{Q}$, and set $\sigma(t_\nu) = t_{\nu+1}$. Lift σ to an automorphism of $\mathbb{C}$. Then $\mathbb{Q}(t_0)_\sigma$ is not finitely generated over $\mathbb{Q}$ as a field.

Note that the underlying endomorphism σ of a difference field (K, σ) need not be surjective. Take for example any non-perfect field and endow it with the Frobenius endomorphism. However, if the endomorphism is surjective we call (K, σ) an inversive difference field. Any difference field (K, σ) has an inversive closure, which is by definition an inversive difference field $(K^{\text{inv}}, \sigma^{\text{inv}})$ together with a homomorphism of difference fields $\iota : K \longrightarrow K^{\text{inv}}$ satisfying the following universal property: to any inversive difference field (L, τ) and homomorphism of difference fields $\varphi : K \longrightarrow L$ there is a homomorphism of difference fields $\psi : K^{\text{inv}} \longrightarrow L$ such that $\varphi = \psi \circ \iota$. The existence of the inversive closure of a difference field is shown the same way as the existence of the perfect hull of a field (the latter in fact being a particular example of inversive closure considering the Frobenius endomorphism). All difference fields considered in this thesis will be inversive unless otherwise stated. Let us just note at this place that we will generalise this

concept in chapter 5 to the notion of inversive L_σ-structures (see section 5.1).

If (K, σ) is a difference field, not necessarily inversive, we let

$$\mathrm{Fix}(K, \sigma) = \{\, a \in K \mid \sigma(a) = a \,\}$$

and call it the fixed field of (K, σ). Note that $\mathrm{Fix}(K^{\mathrm{inv}}, \sigma^{\mathrm{inv}}) = \mathrm{Fix}(K, \sigma)$. This is so because if $a \in K^{\mathrm{inv}}$, then $(\sigma^{\mathrm{inv}})^n(a) \in K$ for some $n \in \mathbb{N}$, so $\mathrm{Fix}(K^{\mathrm{inv}}, \sigma^{\mathrm{inv}}) \subseteq \mathrm{Fix}(K, \sigma)$

Consider a difference ring (R, σ) whose underlying ring is an integral domain. As σ is injective by convention, it extends canonically to the quotient field $\mathrm{Quot}(R)$ of R by setting $\sigma(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)}$. $\big(\mathrm{Quot}(R), \sigma\big)$ is called the quotient difference field of (R, σ), and satisfies the obvious universal property. Note that $\big(\mathrm{Quot}(R), \sigma\big)$ may not be inversive.

Examples. We have already mentioned that the Frobenius endomorphism yields examples of difference fields. Consider now the field $\mathbb{C}(z)$ of meromorphic functions of the Riemannian sphere $\mathbb{P}^1(\mathbb{C})$ and a rational transformation $\tau(z) = \frac{az+b}{cz+d}$ (with $ad - bc \neq 0$). Then $(\mathbb{C}(z), \tau)$ is a difference field. In fact, the name difference field originated from this type of example; an equation of the form

$$p\,(\, f(z), f(z+1), \ldots, f(z+n)\,) \;=\; 0$$

where p is a polynomial over K and f is an unknown function is called an algebraic difference equation.
More generally, let V be any variety over an algebraically closed field k, and let φ be a dominant rational endomorphism of V. Then the rational function field $k(V)$ of V over k endowed with the endomorphism corresponding to φ becomes a (non-inversive) difference field, which is the quotient difference field of the coordinate ring $k[V]$ endowed again with the endomorphism corresponding to φ in case φ is everywhere defined on V.

Of particular interest are difference polynomial rings. Let (R, σ) be a difference ring and $\bar{X} = (X_1, \ldots, X_n)$ be a tuple of indeterminates. The difference polynomial ring over (R, σ) in the indeterminates $\bar{X}$ is the ring

$$R[X_1, \ldots, X_n, X_1^\sigma, \ldots, X_n^\sigma, \ldots, X_1^{\sigma^m}, \ldots]$$

endowed with the extension of σ suggested by the notation. We write $R[\bar{X}]_\sigma$ for the difference polynomial ring over (R, σ), the endomorphism being tacit to that symbol. Elements of $R[\bar{X}]_\sigma$ are called difference polynomials over R and equations of the form $f(\bar{X}) = 0$ for $f(\bar{X}) \in R[\bar{X}]_\sigma$ are called difference equatons, or σ-equations for short, with coefficients in R. One evaluates a difference polynomial at an n-tuple R as suggested by the notation.

Compatible Extensions. Two difference field extensions of a difference field (K, σ) are called compatible if there is some difference field extension of (K, σ) in which both embed (over (K, σ)). In contrast to extensions of differential fields (say in characteristic zero), two algebraic extensions of a difference field need not be compatible. Consider for example the difference field $(\mathbb{Q}, id)$. The identity has two possible extensions to $\mathbb{Q}(i)$, namely the identity and the automorphism mapping i to $-i$. Clearly the difference fields

$(\mathbb{Q}(i), id)$ and $(\mathbb{Q}(i), i \mapsto -i)$ are incompatible. This phenomenon will not occur if (K, σ) is algebraically closed, or more generally if the underlying field extensions are linearly disjoint over K. We state this fact in the following lemma for further reference.

LEMMA 1.18. *Let (F_1, σ_1) and (F_2, σ_2) be difference fields with common subdifference field (K, σ). We assume that all fields are contained in some universal domain. If F_1 is linearly disjoint from F_2 over K, then there is a unique automorphism τ on the compositum F_1F_2 extending both σ_1 and σ_2.*

Proof. On the one hand, F_1 and F_2 are K-algebras via the inclusion. On the other, they are K-algebras via σ followed by the inclusion. Thus $\sigma_1 \times \sigma_2$ is a K-bilinear isomorphism, so the assertion follows from the universal property of tensor products. □

So for example if F_1 is a Galois extension of K and $F_1 \cap F_2 = K$, it follows from (1.10) that F_1 and F_2 are linearly disjoint over K and thus we can amalgamate the automorphisms σ_1 and σ_2.

Difference Ideals. Of particular significance are the so-called perfect and prime difference ideals, which form the analogues of radical and prime ideals in commutative algebra.

A difference ideal, or σ-ideal for short, in a difference ring (R, σ) is a ring ideal I of R with $\sigma(I) = I$. Note that our difference ideals are called reflexive difference ideals by Cohn [**17**]. The factor ring R/I of R modulo the σ-ideal I inherits an endomorphism from R by setting $\sigma(a \bmod I) = \sigma(a) \bmod I$ and thus becomes a difference ring in the natural way. R/I endowed with this endomorphism is called the factor difference ring of (R, σ) modulo I.

We say that the difference ideal I is perfect if it is not the unit ideal and if for all $f \in R$, if $f^n\sigma(f)^m \in I$ (with $n, m \in \mathbb{N}$), then $f \in I$. That this definition is equivalent to Cohn's definition (see [**17**]) is the content of the following lemma.

LEMMA 1.19. *Let (R, σ) be a difference ring and $I \subset R$ be a ring ideal. Then the following are equivalent:*

1. *I is a perfect difference ideal.*
2. *$\sigma(I) \subseteq I$ and for any $f \in R$, if a product of powers of transforms of f is in I, then $f \in I$.*

Proof. That (2) implies (1) is trivial. For the converse, let $f \in R$ be an element with

$$\prod_{0 \le i \le N} \sigma^i(f^{m_i}) \in I \ .$$

Because I is an ideal, we may multiply by suitable elements $\sigma^\nu(f^\mu)$ and obtain

$$\prod_{0 \le i \le N-1} \sigma^i(f^m)\ \sigma\Big(\prod_{0 \le i \le N-1} \sigma^i(f^m)\Big) \ \in I$$

for some m. By the hypothesis on I it follows that

$$\prod_{0\leq i\leq N-1} \sigma^i(f^m) \in I \ .$$

Iterating this process, we obtain

$$f^m \sigma(f^m) \in I \ ,$$

which implies that $f \in I$. □

A difference ideal $\wp$ that is a prime[1] ideal is called a prime difference ideal, or σ-prime ideal for short. A σ-prime ideal is called maximal if it is maximal among σ-prime ideals (with respect to inclusion). If $\wp$ is a prime difference ideal in a difference ring (R, σ), a difference specialisation of $\wp$ is a prime difference ideal $\wp'$ in (R, σ) that contains $\wp$.

Note that any prime difference ideal is perfect. Maximal difference prime ideals need not be maximal ideals. Consequently, if m is a maximal difference prime ideal in an integral domain, then R/m need not be a field. To give an example, consider the difference field $(\mathbb{C}, id)$ and the σ-equation $X^\sigma = X+1$. The ring ideal I generated by $X^\sigma - (X+1)$ and all its transforms in the difference polynomial ring $\mathbb{C}[X]_\sigma$ is a maximal difference prime ideal. The quotient difference ring $\mathbb{C}[X]_\sigma/I$ is just the polynomial ring $\mathbb{C}[X]$ together with the endomorphism $X \mapsto X+1$. In particular it is not a field.

If S is a subset of a difference ring (R, σ) we denote by $(S)_{\text{perf}}$ the perfect difference ideal generated by S, which is by definition the intersection of all perfect difference ideals containing S. ($(S)_{\text{perf}}$ is defined to be R in case there is no perfect σ-ideal that contains S, and is then not a perfect difference ideal in our sense.) A perfect difference ideal is called finitely generated if there is some finite set S such that $I = (S)_{\text{perf}}$. Note aside that $(S)_{\text{perf}}$ is in general much bigger than the ring ideal generated by S and all its transforms. It is obtained by the following procedure. First build the set of all $f \in R$ such that $f^m \sigma(f)^n \in S$, for some $n, m \geq 0$. Then take the difference ideal generated by that (i.e. linear combinations of elements of the set and its transforms). Proceed like this. It is known that this process stabilises after finitely many steps (see [**17**]).

Any perfect difference ideal is the (possibly infinite) intersection of σ-prime ideals. This follows immediately from Zorn's lemma and the fact that

$$(S)_{\text{perf}} \cap (T)_{\text{perf}} = (S \cdot T)_{\text{perf}}$$

for any sets S, T (see [**17**]).

In Ritt difference rings any perfect difference ideal is the intersection of a finite number of prime difference ideals ([**17**], chapter 3, theorem 4). A difference ring (R, σ) is called Ritt if any perfect σ-ideal is finitely generated. Equivalently it satisfies the ascending chain condition on perfect σ-ideals ([**17**], theorem 2 of chapter 3). The fact that difference polynomial rings over difference fields are Ritt is the content of the Finite Basis Theorem of Ritt and Raudenbusch, which we cite from [**17**] (ibid, chapter 3, theorem 5).

[1] We require prime ideals to be different from the unit ideal.

THEOREM 1.20 (Finite Basis Theorem). *Let (R,σ) be a difference ring. If (R,σ) is Ritt, then $R[\bar{X}]_\sigma$ is a Ritt difference ring.*

If L/K is a difference field extension then obviously $K[\bar{X}]_\sigma \subset L[\bar{X}]_\sigma$, and if $A \subset L^n$ we write $I_\sigma(A/K)$ for the vanishing difference ideal of A over K , or just the vanishing σ-ideal of A over K, which is the set of difference polynomials in $K[\bar{X}]_\sigma$ that vanish at every element of A. In case A consists of a single tuple $\bar{a}$, we just write $I_\sigma(\bar{a}/K)$. One verifies easily that $I_\sigma(A/K)$ is a perfect difference ideal (or all of $K[\bar{X}]_\sigma$), and that $I_\sigma(\bar{a}/K)$ is always σ-prime. Conversely, if I is a perfect difference ideal in $K[\bar{X}]_\sigma$, then there is some difference field extension L of K in which I has a common zero. Namely, by convention I is not unit ideal, so we may choose some σ-prime $\wp$ that contains I and put $L = \mathrm{Quot}(K[\bar{X}]_\sigma/\wp)$. Note that as $K[\bar{X}]_\sigma$ is a Ritt difference ring, there are finitely many σ-prime ideals in $K[\bar{X}]_\sigma$ such that

$$I = \bigcap_{\wp \supseteq I} \wp$$

(which correspond to the "irreducible components" of $V_\sigma(I)$, see section 4.2).

A difference field (K,σ) is called generic if for any finite system of difference equations

$$f_1(\bar{X}) = \cdots = f_r(\bar{X}) = 0$$

having a solution in some difference field extension of (K,σ) has a solution in K. Using the basic facts on perfect and prime difference ideals above one sees that (K,σ) is generic if and only if the σ-version of Hilbert's Nullstellensatz is true in (K,σ), namely that any σ-prime ideal in $K[\bar{X}]_\sigma$ has a solution in K. It is also equivalent to (K,σ) be existentially closed in difference field extensions. Generic difference fields serve as universal domains for difference algebra and difference algebraic geometry, the same way as do their counterparts, algebraically closed fields, for algebra and algebraic geometry.

CHAPTER 2

A Prestel-Frey Theorem

The well-known theorem of Macintyre, Cherlin and Shelah states that infinite superstable fields are algebraically closed. The converse being true because of quantifier elimination in algebraically closed fields, one has thus an algebraic characterisation of the class of superstable fields.

Shelah's notion of simplicity and supersimplicity, introduced in [**66**], generalises stability and superstability. Prototypical examples of supersimple (pure) fields are pseudo-finite fields (see chapter 4), and the natural question for an algebraic characterisation of supersimple fields arises.

Hrushovski shows in [**26**] that pseudo-finite fields are supersimple. More general, he proves that any perfect pseudo-algebraically closed field with bounded absolute Galois group is supersimple. Pillay and Poizat in turn show that a supersimple field is perfect and has bounded absolute Galois group in [**54**]. In 1995, Pillay conjectured that supersimple fields are pseudo-algebraically closed.

So far a proof (or counterexample) of this conjecture seems to be out of reach for current methods. Only particular types of curves over a supersimple field k have been shown to have a k-rational point. Pillay, Scanlon and Wagner showed in [**55**] that any rational curve over a supersimple field k has a k-rational point, by proving that the Brauer group of k is trivial. Pillay and Martin-Pizarro proved in [**43**] and [**42**] that the set of k-rational points on an elliptic or hyperelliptic curve C over k, is dense in C if the modulus of the curve in a certain moduli space satisfies some genericity assumption. Assuming that k has exactly one quadratic extension (in a fixed algebraic closure), Martin-Pizarro and Wagner showed in [**44**] that the set of k-rational points on any elliptic curve E over k is dense in E.

The theorem of Prestel-Frey states that a pseudo-algebraically closed field is never henselian unless it is separably closed (see [**22**], corollary (11.5.5)). In this chapter we are going to prove this for simple fields: any simple field which is not separably closed is not henselian (corollary (2.3)). Our proof depends on the definability of the valuation topology in henselian fields that are neither separably closed nor real closed proved by Koenigsmann (see below).

Let us recall the notion of a t-henselian field, which is the right frame to formulate the theorem. We refer to the article of Prestel and Ziegler [**60**] for details. Let (K, τ) be a field with ring topology. (K, τ) is called a V-topological field if any subset $S \subseteq K \setminus \{0\}$ is bounded whenever S^{-1} is

bounded away from 0 (which means there is some $U \in \tau$, $0 \in U$, such that $U \cap S^{-1} = \emptyset$). There are basically two classes of examples for V-topological fields. For the first, let $|.|$ be a (non-trivial) absolute value of K. The absolute value induces a ring topology $\tau_{|.|}$ via the sets

$$V_\varepsilon = \{x \in K \mid |x| < \varepsilon\} \ ,$$

turning K into a V-topological field. The second comes from valuations. Let v be a non-trivial valuation on K. v induces a ring topology τ_v via the sets

$$V_\gamma = \{x \in K \mid v(x) > \gamma\} \ ,$$

which makes K a V-topological field. In fact, by a theorem of Kowalsky-Dürbaum and Fleischer, any V-topological field is of one of the above mentioned type (see [**60**], theorem (3.1)).

Note that it follows therefrom that in any V-topological field there is some strictly decreasing chain of neighbourhoods of 0.

The V-topological field (K, τ) is called t-henselian if for any $n \geq 1$ there is $U \in \tau$ with $0 \in U$ such that any polynomial $f \in X^{n+1} + X^n + U[X]_{\leq n-1}$ has a zero in K. Here by $U[X]_{\leq n-1}$ we denote the set of polynomials of degree less or equal to $n-1$ having coefficients from U [1]. We call a (pure) field K t-henselian if there is a ring topology τ on K such that (K, τ) is t-henselian. Real closed fields and henselian fields are examples of t-henselian fields. The following theorem on t-henselian fields was proved by Koenigsmann in [**32**].

THEOREM 2.1 (Koenigsmann). *Let (K, τ) be a t-henselian field. If K is neither separably closed nor real closed, then the topology τ is uniformly definable in the pure field K, i.e. there is a neighbourhood filter of 0 which is given by a definable family of definable sets.*

THEOREM 2.2. *Let K be a field, possibly with extra structure, which has not the strict order property. If K is t-henselian, then it is separably closed. In particular K is never real closed, and henselian only in case it is separably closed.*

Needless to say, it is well-known that real closed fields have the strict order property, the ordering being definable in the field language.

Proof of 2.2. K is not real closed because $Th(K)$ does not have the strict order property. Assume by way of contradiction that K is not separably closed. If K admits a t-henselian topology τ, then by (2.1) there is some formula $\varphi(\bar{x}; \bar{y})$ and a family of tuples $\bar{a}_\nu \in K$, $\nu \in I$, such that the family $\{\varphi(K; \bar{a}_\nu) : \nu \in I\}$ forms a neighbourhood base of 0 refining the topology τ. By the above remarks on V-topological fields we may assume that the family $\{\varphi(K; a_\nu) : \nu \in I\}$ is strictly decreasing (with respect to inclusion). So it follows that K has the strict order property. □

COROLLARY 2.3. *Let K be a simple field. If K is t-henselian, then it is separably closed. In particular K is never real closed, and henselian only in case it is separably closed.*

[1] The reader may note that this is not the original definition of t-henselianity given in [**60**]. It is however equivalent by theorem (7.2) of [**60**].

Proof of 2.3. Simple fields do not have the strict order property. □

Note that the fact that simple fields cannot be real closed is well-known, the argument being that o-minimal theories do have the strict order property.

Corollary 2.3 constitutes another property that simple and supersimple fields share with PAC fields. It thus supports Pillay's conjecture that supersimple fields are PAC.

CHAPTER 3

On a Theorem from Galois Cohomology

In the present chapter we generalise a well-known theorem from Galois Cohomology theory to a purely model theoretic setting. The situation is as follows (see [**68**], Chapter III, §1). To a variety V over some perfect field k one assigns the so-called Weil-Chatelet set of V over k, denoted $WC(V/k)$. It is by definition the pointed set of k-isomorphism classes of k^{alg}-forms of V, the distinguished point being the isomorphism class of V. It can be viewed as a measure of how many "forms" V can take when transformed with coefficients in k^{alg}. The theorem states that for quasi-projective V, $WC(V/k)$ is isomorphic as a pointed set to $H^1(\text{Gal}(k), \text{Aut}_{k^{\text{alg}}}(V))$, the first Galois cohomology set of the absolute Galois group $\text{Gal}(k)$ of k with values in $\text{Aut}_{k^{\text{alg}}}(V)$, the group of rational automorphisms of V over k^{alg} (see [**68**], proposition 5 of Chapter III, §1).

We generalise this theorem to types in a first order theory T with unique extension to the algebraic closure of their domain, see theorem (3.3). The theory T is only required to have elimination of imaginaries. First the relevant notions are introduced for types having the unique extension property just mentioned, such as automorphisms, forms and what we call the Weil-Chatelet sets of types. Also we introduce for such a type p with domain A, the first Galois cohomology set of $\text{Gal}(A)$ with values in the group of automorphisms of p.

To simplify readability, we sometimes write $\widetilde{A}$ instead of $\text{acl}(A)$ and G_A instead of $\text{Gal}(A)$ for a parameter set A in the present chapter.

3.1. Galois Cohomology and Types

We fix a possibly many-sorted first-order L-theory T with elimination of imaginaries. Our objects, replacing varieties in the algebro-geometric context, will be types with a unique extension to the algebraic closure of their domain: we say that a type p over a parameter set A is *acl*-stationary if it has a unique extension to $\text{acl}(A)$. If A is algebraically closed, $B \subseteq A$ with $\text{acl}(B) = A$ and $p|_B$ is *acl*-stationary, we say that p is *acl*-stationary over B. Needless to say that *acl*-stationary types in stable theories are stationary.

Morphisms of Types. Our morphisms will correspond to rational morphisms rather than regular morphisms of varieties. Let A_1 and A_2 be parameter sets with $\text{acl}(A_1) = \text{acl}(A_2) = A$, and let $p_1(\bar{x}_1)$ and $p_2(\bar{x}_2)$ be

types over A. Assume that p_1 is *acl*-stationary over A_1 and that p_2 is *acl*-stationary over A_2. A strong type $\pi(\bar{x}_1, \bar{x}_2) \in S(A)$ is called a morphism from p_1 to p_2, written $p_1 \xrightarrow{\pi} p_2$, if there are realizations $\bar{a}_1 \models p_1$ and $\bar{a}_2 \models p_2$ with $\bar{a}_1\bar{a}_2 \models \pi$ and $\bar{a}_2 \in \mathrm{dcl}(\bar{a}_1, A)$. If $B \subseteq A$ with $\mathrm{acl}(B) = A$ and $\pi|_B$ is *acl*-stationary we say that π is over B if $\bar{a}_2 \in \mathrm{dcl}(\bar{a}_1, B)$. If $\bar{a}$ realizes p_1, we abuse notation and write $\pi(\bar{a})$ for the (unique) realization of p_2 corresponding to $\bar{a}$ under π. Note that by our definition a morphism from p to somewhere must be over the algebraic closure of the domain of p. The set of morphisms from p_1 to p_2 is denoted by $\mathrm{Hom}(p_1, p_2)$. If $p_1 = p_2 = p$, there is a distinguished morphism in $\mathrm{Hom}(p, p)$, given by $\mathrm{tp}(\bar{a}\bar{a}/\widetilde{A})$ for some (any) realization $\bar{a}$ of p. We denote this endomorphism by 1_p and call it the identity morphism on p.

Let us make some easy observations. First, it follows directly from the definition that $\pi(\bar{x}_1, \bar{x}_2) \models p_1(\bar{x}_1) \wedge p_2(\bar{x}_2)$. Also, for any realizations $\bar{a}_1\bar{a}_2$ of the morphism π, $\bar{a}_2 \in \mathrm{dcl}(\bar{a}_1, A)$. If f is an A-definable function that witnesses $\bar{a}_2 \in \mathrm{dcl}(\bar{a}_1, A)$, then $f(\bar{a}) \models p_2$ for any realization $\bar{a} \models p_1$.

LEMMA 3.1. *Let $p, q \in S(A)$ be acl-stationary and let $\pi \in S(\widetilde{A})$ be a morphism from p to q. Let further $\bar{a}\bar{b} \models \pi$ and $\varphi(\bar{x}, \bar{y})$ be an $L(\widetilde{A})$-formula witnessing that $\bar{b} \in \mathrm{dcl}(\bar{a}, \widetilde{A})$. Then π is determined by*

$$\Sigma_\varphi = p(\bar{x}) \cup \{\, \varphi(\bar{x}, \bar{y}) \,\}$$

Proof. Let $\bar{a}$ and $\bar{b}$ be tuples of the right length such that $\bar{a}\bar{b} \models \Sigma_\varphi$ and call f the partial function defined by φ. Note that $p \models \exists^{=1}\bar{y}\ \ \bar{y} = f(\bar{x})$. If $\bar{a}'\bar{b}' \models \pi$ then $\bar{a}' \models p$ so that there is some $\alpha \in \mathrm{Aut}(\mathfrak{C}/\widetilde{A})$ with $\alpha(\bar{a}) = \bar{a}'$. Because $\bar{b} = f(\bar{a})$ and $\bar{b}' = f(\bar{a}')$, and f is definable over $\widetilde{A}$, it follows that $\bar{b}' = \alpha(\bar{b})$. Thus $\bar{a}\bar{b} \equiv_{\widetilde{A}} \bar{a}'\bar{b}'$ □

Note aside that it follows from this characterisation that every morphism π is over $A\bar{a}$ for some finite tuple $\bar{a} \in \widetilde{A}$.

Let for example T be ACF_p, the theory of algebraically closed fields of characteristic $p \geq 0$. Then *acl*-stationary types are stationary , as ACF_p is stable and eliminates imaginaries. Let $A = \mathrm{dcl}(A)$ be a subfield (of the monster model/field $\mathfrak{C}$). For two stationary types $p \in S_n(A)$ and $q \in S_m(A)$, let V and W be the (affine) varieties corresponding to p and q respectively. If the characteristic is zero, a morphism $p \xrightarrow{\pi} q$ "is" nothing but a rational dominant morphism of varieties, defined over $\mathrm{acl}(A)$ in the algebro-geometric sense, from V onto W. If the characteristic is positive, then π "is" a rational dominant morphism of varieties, again defined over $\mathrm{acl}(A)$ in the algebro-geometric sense, up to some power of the Frobenius morphism $x \mapsto x^p$. This is so because for a subfield K of $\mathfrak{C}$, $\mathrm{dcl}(K)$ is K in characteristic zero and K^{1/p^∞} in positive characteristic.

Composition of Morphisms. Let A be an algebraically closed set and p_1, p_2 and p_3 be types over A. The composition $\pi_2 \circ \pi_1$ of two morphisms $p_1 \xrightarrow{\pi_1} p_2$ and $p_2 \xrightarrow{\pi_2} p_3$ is defined as follows. Choose $\bar{a}_1\bar{a}_2 \models \pi_1$ and $\bar{a}_2'\bar{a}_3 \models \pi_2$ and let $\alpha \in \mathrm{Aut}(\mathfrak{C}/A)$ send $\bar{a}_2'$ to $\bar{a}_2$. We define $\pi_2 \circ \pi_1$ to be $\mathrm{tp}(\bar{a}_1\alpha(\bar{a}_3)/A)$. Clearly this defines a morphism, and is independent from

the realizations of π_1 and π_2 and the automorphism α chosen: if $\bar{b}_1\bar{b}_2 \models \pi_1$, $\bar{b}'_2\bar{b}_3 \models \pi_2$ and $\beta \in \mathrm{Aut}(\mathfrak{C}/A)$ with $\beta(\bar{b}'_2) = \bar{b}_2$, then there is $\gamma \in \mathrm{Aut}(\mathfrak{C}/A)$ with $\gamma(\bar{a}_1) = \bar{b}_1$, and one calculates that $\gamma(\pi_2(\pi_1(\bar{a}_1))) = \beta(\bar{b}_3)$, which shows $\gamma(\bar{a}_1\alpha(\bar{a}_3)) = \bar{b}_1\beta(\bar{b}_3)$.

A morphism $p \xrightarrow{\pi} q$ is called invertible, or an isomorphism from p to q, if there is a morphism $q \xrightarrow{\xi} p$ such that both $\pi \circ \xi$ and $\xi \circ \pi$ are the identity on p and q respectively. In this case ξ is uniquely determined: if $ab \models \pi$ then $\xi = \mathrm{tp}(ba/A)$, as one expects. We write π^{-1} for ξ and call it the inverse morphism of π. p and q are called isomorphic if there is an isomorphism from p to q. Needless to say that p and q might have distinct variable tuples. An isomorphism from p to itself is called an automorphism of p. Observe that if p is *acl*-stationary over B, $B \subsetneq \mathrm{acl}(B) = A$, an automorphism of p need not be over B. To give an example, consider algebraically closed fields of characteristic zero. Let p be the generic type over $\emptyset$ of the affine line $\mathbb{A}^1$, and consider the automorphism given by multiplication with $\sqrt{2}$. We write $\mathrm{Aut}(p/A)$ for the set of automorphisms of p over the algebraically closed set A. It is easily seen to be a group with composition of morphisms, the neutral element being the identity on p.

Forms of Types. Let $A = \mathrm{acl}(A)$ and $p, q \in S(A)$ be *acl*-stationary over $B \subsetneq A$. As with automorphisms, an isomorphism $p \to q$ need not be over B. To give an example, consider again algebraically closed fields, say in characteristic zero. Let p_1 be the generic type over $\emptyset$ of the affine plane curve C_1 given by the equation $X^2 + Y^2 + 1 = 0$, and p_2 be the generic type over $\emptyset$ of the affine plane curve C_2 given by the equation $X^2 + Y^2 - 1 = 0$. Both curves are birational over $\mathbb{Q}^{\mathrm{alg}}$. But obviously $C_1(\mathbb{Q}) = \emptyset$, whereas $C_2(\mathbb{Q})$ is infinite, so they cannot be birational over $\mathbb{Q}$ – one needs i to define an isomorphism between the two curves/types. We say that p_1 and p_2 are isomorphic over B if there is some isomorphism $p_1 \to p_2$ over B.

Now let A be any parameter set, not necessarily algebraically closed, and $p \in S(\widetilde{A})$ be *acl*-stationary over A. For a set B with $A \subseteq B \subseteq \widetilde{A}$ we call $q \in S(\widetilde{A})$ a B-form of p if q is *acl*-stationary over A and if there is some isomorphism $p \xrightarrow{\pi} q$ over B. Being isomorphic over A is clearly an equivalence relation on the set of $\widetilde{A}$-forms of p. We call its set of equivalence classes the Weil-Chatelet set of p and denote it by $WC(p/A)$.

The action of G_A. Let A be any parameter set. Recall that G_A is the set of elementary permutations of $\widetilde{A}$ leaving A pointwise fixed and that G_A is a profinite group with the topology of pointwise convergence. For any *acl*-stationary types $p_1, p_2 \in S(A)$, G_A operates on $\mathrm{Hom}(p_1, p_2)$ (on the left) by

$$\sigma.\pi := \{\varphi(x, y; \sigma(\bar{a})) \mid \varphi(x, y; \bar{a}) \in \pi\}.$$

If π is invertible, then so is $\sigma.\pi$, and $(\sigma.\pi)^{-1} = \sigma.(\pi^{-1})$. For if $ab \models \pi$ and $\bar{\sigma}$ is any lift of σ whose domain contains ab, then $\bar{\sigma}(ab) \models \sigma.\pi$ and the inverse is $\mathrm{tp}(\bar{\sigma}(ba)/\widetilde{A})$. Thus for *acl*-stationary $p \in S(A)$ one has that G_A operates

on $\mathrm{Aut}(p/\widetilde{A})$. We denote this action by μ_p and endow $\mathrm{Aut}(p/\widetilde{A})$ with the discrete topology.

LEMMA 3.2. *Let $p, q, r \in S(A)$ be acl-stationary.*

(1) *For any morphisms $p \xrightarrow{\pi} q$, $q \xrightarrow{\xi} r$ and all $\sigma \in G_A$, one has $\sigma.(\xi \circ \pi) = \sigma.\xi \circ \sigma.\pi$.*
(2) *The morphism $p \xrightarrow{\pi} p$ is over A if and only if $\sigma.\pi = \pi$ for all $\sigma \in G_A$.*
(3) *μ_p turns $\mathrm{Aut}(p/\widetilde{A})$ into a discrete G_A-group.*

Proof. (2) is immediate from lemma (3.1). To show (1), let $p \xrightarrow{\pi} q$ and $q \xrightarrow{\xi} r$ be morphisms and $\sigma \in G_A$. By lemma (3.1) we can choose $\widetilde{A}$-definable functions f and g such that π is determined by $p(\bar{x})$ and f and ξ is determined by $q(\bar{y})$ and g. It follows that $\xi \circ \pi$ is determined by the $\widetilde{A}$-definable function $g \circ f$ and $\sigma.(\xi \circ \pi)$ is determined by $\sigma.(g \circ f)$, which is the $\widetilde{A}$-definable function obtained by applying σ to the parameters from $\widetilde{A}$ in some (any) defining formula for $g \circ f$. But $\sigma(g \circ f) = \sigma g \circ \sigma f$, the latter determining the morphism $\sigma.\xi \circ \sigma.\pi$. Thus $\sigma.(\xi \circ \pi) = \sigma.\xi \circ \sigma.\pi$.

Let us finally address (3). By (1) μ_p is a group action. To see that it is continuous, note that by lemma (3.1) any morphism is over $A\bar{c}$ for some finite tuple $\bar{c} \in \widetilde{A}$. So

$$\mathrm{Aut}(p/\widetilde{A}) = \bigcup \mathrm{Aut}(p/\widetilde{A})^U \ ,$$

where U runs over all open normal subgroups of G_A. □

So we can speak of continuous cocycles of G_A with values in $\mathrm{Aut}(p/\widetilde{A})$ and the Galois cohomology set $H^1(G_A, \mathrm{Aut}(p/\widetilde{A}))$. We now come to the main theorem of the present chapter.

THEOREM 3.3. *Let T have elimination of imaginaries and $p \in S(A)$ be acl-stationary. Then there is a natural isomorphism of pointed sets*

$$WC(p/A) \xrightarrow{\Phi} H^1(G_A, \mathrm{Aut}(p/\widetilde{A})) \ .$$

Proof. Define the map Φ as follows. Let $[q]$ be a class in $WC(p/A)$, represented by the $\widetilde{A}$-form q of p, and choose an isomorphism $p \xrightarrow{\pi} q$ over $\widetilde{A}$. Then $[q]$ is mapped to the cohomology class of the continuous cocycle[1]

$$G_A \longrightarrow \mathrm{Aut}(p/\widetilde{A}) : \sigma \mapsto \pi^{-1} \circ \sigma.\pi \ .$$

To see that Φ is well-defined, note first that this cocycle is obviously continuous. Let $r \in [q]$ and $p \xrightarrow{\pi} q$ and $p \xrightarrow{\xi} r$ be isomorphisms over $\widetilde{A}$ and $q \xrightarrow{\eta} r$ be an isomorphism over A. As η is over A, one has $\eta = \sigma.\eta$ for all $\sigma \in G_A$ by lemma (3.2), so that

$$1_r = \eta \circ \pi \circ \pi^{-1} \circ \sigma.\pi \circ \sigma.\pi^{-1} \circ \sigma.\eta^{-1} \ ,$$

and hence

$$\xi^{-1} \circ \sigma.\xi = \xi^{-1} \circ \eta \circ \pi \circ \pi^{-1} \circ \sigma.\pi \circ \sigma.\pi^{-1} \circ \sigma.\eta^{-1} \circ \sigma.\xi \ .$$

[1] one easily verifies that this map indeed defines a continuous cocycle

If we let $\gamma = \pi^{-1} \circ \eta^{-1} \circ \xi \in \mathrm{Aut}(p/\widetilde{A})$, then the above equation reads as

$$\xi^{-1} \circ \sigma.\xi = \gamma^{-1} \circ (\pi^{-1} \circ \sigma.\pi) \circ \sigma.\gamma \ ,$$

so the cocycles $\pi^{-1} \circ \sigma.\pi$ and $\xi^{-1} \circ \sigma.\xi$ are cohomologuous.

As to show injectivity, let $[q]$ and $[r]$ be in $WC(p/A)$ and let $p \xrightarrow{\pi} q$ and $p \xrightarrow{\xi} r$ be $\widetilde{A}$-isomorphisms and $\gamma \in \mathrm{Aut}(p/\widetilde{A})$ such that

$$\pi^{-1} \circ \sigma.\pi = \gamma^{-1} \circ \xi^{-1} \circ \sigma.\xi \circ \sigma.\gamma \ .$$

Then $\xi \circ \gamma \circ \pi^{-1}$ is an isomorphism from q to r, which is over A because the last equation is equivalent to $\xi \circ \gamma \circ \pi^{-1} = \sigma.(\xi \circ \gamma \circ \pi^{-1})$. Hence $[q] = [r]$.

Now for the surjectivity of Φ, let

$$f : G_A \longrightarrow \mathrm{Aut}(p/\widetilde{A})$$

be a continuous cocycle of G_A with values in $\mathrm{Aut}(p/\widetilde{A})$. We fix a realization $a \models p$ and denote $D_a = \mathrm{dcl}(a\widetilde{A})$. f defines a group action of G_A on D_a via automorphisms as follows. For $\sigma \in G_A$ we let $\sigma^f(a) = f(\sigma)^{-1}(a)$ and $\sigma^f(c) = \sigma(c)$ for $c \in \widetilde{A}$. As p is *acl*-stationary and $f(\sigma) \in \mathrm{Aut}(p/\widetilde{A})$ for all $\sigma \in G_A$, σ^f is an elementary map with a and $\sigma^f(a)$ interdefinable over $\widetilde{A}$. So σ^f lifts uniquely to an automorphism of D_a, which we also denote by σ^f. This indeed defines a group action of G_A on D_a, as the following calculation shows:

$$(\sigma\tau)^f(a) = f(\sigma\tau)^{-1}(a) = \sigma.f(\tau)^{-1}(f(\sigma)^{-1}(a)) = \sigma^f(f(\tau)^{-1}(a)) = \sigma^f(\tau^f(a)) \, .$$

The third equality holds because of the very definition of the action of G_A on D_a. Note that we have defined a section of the restriction map $\mathrm{Aut}(D_a/A) \longrightarrow G_A$, or in other words, we gave a lift of every $\sigma \in G_A$ to an automorphism of D_a.

We now aim to find some finite tuple $b \in D_a$ with the properties that

- $\sigma^f(b) = b$ for all $\sigma \in G_A$, and
- $\mathrm{tp}(b/\widetilde{A})$ is an $\widetilde{A}$-form of p.

For then we are done: if we have b with the above properties and if π is an isomorphism over $\widetilde{A}$ with $\pi(a) = b$, then for all $\sigma \in G_A$

$$\begin{array}{rcccccl} f(\sigma)^{-1}(a) & = & \sigma^f(a) & = & \sigma^f(\pi^{-1}(b)) & = & \sigma.\pi^{-1}(\sigma^f(b)) \\ & = & \sigma.\pi^{-1}(b) & = & \sigma.\pi^{-1}\pi(a), & & \end{array}$$

so $f(\sigma)^{-1} = \sigma.\pi^{-1} \circ \pi$, or equivalently $f(\sigma) = \pi^{-1} \circ \sigma.\pi$ and so Φ is surjective.

In order to find $b \in D_a$ with the above properties, let H be the stabiliser of a with respect to the action of G_A on D_a defined above, and note that $H = f^{-1}(1)$ is an open subgroup of G_A by continuity of f (see section 1.3). So G_A/H is finite and we can choose left representatives $1, \sigma_1, \ldots \sigma_n$ of G_A/H. Further, by elimination of imaginaries, Primitive Element Theorem (1.8) implies that there is some finite tuple $\bar{c} \in \widetilde{A}$ such that $\mathrm{dcl}(\bar{c}, A) = \mathrm{Fix}(\widetilde{A}, H)$. We define

$$b := \{a\bar{c}, {\sigma_1}^f(a\bar{c}), \ldots, {\sigma_n}^f(a\bar{c})\}$$

and claim that b is what we have been looking for. Indeed, $b \in D_a$ because $\sigma^f(a) \in D_a$ for all $\sigma \in G_A$. Also, $\sigma^f(b) = b$ for all $\sigma \in G_A$ by the very choice of b. To see that $\mathrm{tp}(b/\widetilde{A})$ is an $\widetilde{A}$-form of p, note first that $b \in \mathrm{dcl}(a\widetilde{A}) = D_a$ because all $\sigma^f(a) \in \mathrm{dcl}(a\widetilde{A})$. Second, $\mathrm{tp}(b/\widetilde{A})$ is *acl*-stationary over A if and only if any $\sigma \in G_A$ admits a lift fixing b. But as we have seen above, this lift is given by the cocycle f, as we chose b to be a fixed point of the group action. Finally we show that $a \in \mathrm{dcl}(b\widetilde{A})$. Choose to that end an automorphism α of $\mathfrak{C}$ over $\widetilde{A}$ which fixes b. α permutes the elements of b, so $\alpha(a\bar{c}) = {\sigma_i}^f(a\bar{c})$ for some i. $\alpha(\bar{c}) = \bar{c}$ as $\bar{c} \in \widetilde{A}$, so because $\sigma_i(\bar{c}) = \bar{c}$ if and only if $\sigma_i \in H$, we conclude that $\alpha(a\bar{c}) = a\bar{c}$. In particular $\alpha(a) = a$, so we are done. □

Remark 3.4. *Following a different approach, Pillay [**51**] has introduced Galois Cohomology for definable sets in homogeneous atomic structures. We briefly recall this for convenience.*

Let M be an arbitrary (possibly many-sorted) structure with elimination of imaginaries containing the parameter set A such that M is atomic over A and for any finite tuples $\bar{a}$ and $\bar{b}$ from M with $\mathrm{tp}(\bar{a}/A) = \mathrm{tp}(\bar{b}/A)$ there is some automorphism $\alpha \in \mathrm{Aut}(M/A)$ such that $\alpha(\bar{a}) = \bar{b}$. $\mathcal{G} = \mathrm{Aut}(M/A)$ is endowed with the topology of pointwise convergence. For an A-definable set $X \subset M^{\mathrm{eq}}$, $\mathrm{Aut}_{def}(X)$ denotes the group of bijections $X \longrightarrow X$ that are definable using parameters from M. Then $\mathcal{G}$ acts naturally on $\mathrm{Aut}_{def}(X)$ and one has the notion of cocycle of $\mathcal{G}$ with values in $\mathrm{Aut}_{def}(X)$. Such a cocycle $f : \mathcal{G} \longrightarrow \mathrm{Aut}_{def}(X)$ is called definable if there is some tuple $\bar{a} \in M$ and an A-definable partial function $h(\bar{w}, \bar{z}, x)$ such that $f(\sigma) = h(\bar{a}, \sigma(\bar{a}), -)$ for any $\sigma \in \mathcal{G}$. $\mathrm{H}^1_{def}(\mathcal{G}, \mathrm{Aut}_{def}(X))$ denotes the first cohomology set of definable cocycles of $\mathcal{G}$ with values in $\mathrm{Aut}_{def}(X)$. An A-form of X is an A-definable subset Y of M which is in definable bijection to X using parameters from M. Two A-forms Y_1 and Y_2 of X are equivalent if and only if there is some A-definable bijection from Y_1 onto Y_2. Clearly this is an equivalence relation, and the class of X is a distinguished element of the set of equivalence classes. The latter has thus the structure of a pointed set.

*As Pillay proves in §3 of [**51**], $H^1_{def}(\mathcal{G}, \mathrm{Aut}_{def}(X))$ is isomorphic as a pointed set to the set of A-forms of X modulo A-definable bijection.*

CHAPTER 4

Pseudo-finite Fields and Generic Difference Fields

Pseudo-finite fields emerge already in the investigation of Ax and Kochen [**3**], [**4**] and [**5**] of diophantine problems over local fields in form of non-principal ultraproducts of finite prime fields, shortly before Ax started their systematic study in [**1**] and [**2**] in the late 1960's. This study was continued among others by Chatzidakis', van den Dries' and Macintyre's [**13**], as well as Hrushovski [**26**], and constitute a fruitful stimulation not only of modern Model Theory. Together with the failure of Zil'ber's conjecture, Ax' results [**2**] motivated the model theoretic investigation of difference fields in the 1990's. The geometric classification of finite rank definable sets in generic difference fields by Chatzidakis and Hrushovski [**14**] in conjunction with Hrushovski's and Pillay's result on stable one-based groups [**29**], have led to another impressive application of Model Theory in "core mathematics": Hrushovski's proof of the Manin-Mumford conjecture.

Pseudo-finite fields and generic difference fields are closely related, not only through historical development. The fixed field of a generic difference field is a pure pseudo-finite field. On the other hand, to any pseudo-finite field k there is some generic difference field whose fixed field is elementarily equivalent to k.

The aim of the present chapter is to show that even more is true: given any pseudo-finite field k there is some generic difference field whose fixed field even equals k. We also intend to discuss with $ACFA$ a particular example of generic automorphisms of a stable theory from chapter 5 in greater detail.

The chapter is organised as follows. We first recall the basic theory of pseudo-finite fields and generic difference fields in sections 4.1 and 4.2. We include a proof of Hrushovski's theorem on ultraproducts of difference fields, modulo his analogue of the Lang-Weil estimates for difference fields. The proof of the main theorems of this chapter, theorems (4.24), (4.32) and (4.33) are presented in section 4.3. In the last section we prove a variant of theorems (4.24) and (4.33) in the context of fractional powers of the Frobenius.

4.1. Pseudo-finite Fields

We recall in this section some facts about pseudo-finite fields from the literature. All of them are well-known. The original references are [**2**], [**13**] and [**26**]. The basic theory can also be found in [**22**]. Our proof of theorem (4.2) is very easy as we use a very weak version of the Embedding Lemma for PAC fields (see 4.4) and has the nice feature that it can be transported

to other theories of fields that "resemble" pseudo-finite fields, see section 5.2. Also our proof applies when the Galois group is bounded rather than $\widehat{\mathbb{Z}}$. The reason for this is that, regarding the Galois group, we use only the fact that epimorphisms of $\widehat{\mathbb{Z}}$ are already automorphisms, which holds more generally for bounded profinite groups (see [**62**]). We work in the pure ring language throughout this section.

DEFINITION 4.1. *A field k is called pseudo-finite if and only if it is perfect PAC with $\mathrm{Gal}(k) = \widehat{\mathbb{Z}}$. The theory*[1] *of pseudo-finite fields is called PSF.*

The following theorem, fundamental for the basic model theory of pseudo-finite fields, is due to Ax (see [**2**]).

THEOREM 4.2 (Ax). *Let F_1 and F_2 be pseudo-finite fields with common subfield E. Then $F_1 \equiv_E F_2$ if and only if $E^{\mathrm{alg}} \cap F_1 \cong_E E^{\mathrm{alg}} \cap F_2$.*

Proof of theorem (4.2). The implication from left to right follows from the following lemma.

LEMMA 4.3 (Ax). *Let F_1 and F_2 be two algebraic extensions of the field E. Then $F_1 \cong_E F_2$ if and only if $\Delta(F_1/E) = \Delta(F_2/E)$, where for a field extension F/E, $\Delta(F/E)$ denotes the set $\{p \in E[X] \mid F \models \exists x\ p(x) = 0\}$.*

Proof. See lemma 5 of [**2**]. □

For the converse direction we use the following weak version of the Embedding Lemma for PAC fields (for the Embedding lemma for PAC fields, see for example [**22**], lemma (20.2.2)).

LEMMA 4.4 (Embedding Lemma). *Let Ω be a sufficiently saturated pseudo-finite field and $E \subset \Omega$ be a subfield with Ω/E regular. Let F/E be a regular field extension. Assume F is perfect and the restriction maps of absolute Galois groups $\mathrm{res}^{\Omega}_{E} : \mathrm{Gal}(\Omega) \longrightarrow \mathrm{Gal}(E)$ and $\mathrm{res}^{F}_{E} : \mathrm{Gal}(F) \longrightarrow \mathrm{Gal}(E)$ are isomorphisms. Then there is an E-embedding $\varphi : F \longrightarrow \Omega$ such that $\Omega/\varphi(F)$ is regular.*

Proof. We write $F = E(\bar{a})$ for an (infinite) tuple $\bar{a} \in F$. As Ω is PAC and sufficiently saturated, there is some tuple $\bar{a}' \in \Omega$ and an E-isomorphism $\varphi : F = E(\bar{a}) \longrightarrow E(\bar{a}') \subset \Omega$. Denote $K = E(\bar{a}')$. Being an isomorphic image of F, K is perfect and hence the extension Ω/K is separable. The restriction maps $\mathrm{res}^{\Omega}_{E}$ and res^{K}_{E} being isomorphisms, it follows that $\mathrm{res}^{\Omega}_{K} = (\mathrm{res}^{K}_{E})^{-1} \circ \mathrm{res}^{\Omega}_{E}$ is surjective. So $\Omega/\varphi(F)$ is regular. □

Now to prove the implication from right to left of theorem (4.2), let $E^{\mathrm{alg}} \cap F_1 \cong_E E^{\mathrm{alg}} \cap F_2$. We may identify $E^{\mathrm{alg}} \cap F_1$ and $E^{\mathrm{alg}} \cap F_2$, and so assume that E is relatively (field-) algebraically closed in F_1 and F_2. So the field extensions F_1/E and F_2/E are regular because E is perfect. It will be enough to prove the next claim and apply back-and-forth.

[1] It is well-known, and modulo (1.15) not hard to see, that these properties are indeed first-order.

Claim: If Ω_2 is a sufficiently saturated elementary extension of F_2, then there is an E-embedding $\varphi : F_1 \longrightarrow \Omega_2$ such that the extension $\Omega_2/\varphi(F_1)$ is regular.

Proof of the claim. Note that $\mathrm{Gal}(E)$ is procyclic but need not be $\widehat{\mathbb{Z}}$, so we have to work a little in order to apply the Embedding Lemma (4.4).

Ω_2/F_2 is a regular extension, because on the one hand F_2 is perfect, so that the extension is separable, on the other hand the extension is elementary, so that F_2 is relatively algebraically closed in Ω_2. So Ω_2/E is regular, too. Therefore, replacing F_1 by an E-isomorphic copy if necessary, we may assume that F_1 and Ω_2 are linearly disjoint over E. Choose topological generators σ_1 and σ_2 of $\mathrm{Gal}(F_1)$ and $\mathrm{Gal}(\Omega_2)$ respectively, which extend the same topological generator of $\mathrm{Gal}(E)$. This is possible because the absolute Galois groups are procyclic and the respective restriction maps are surjective. Then $\sigma_2|_{F_2^{\mathrm{alg}}}$ generates $\mathrm{Gal}(F_2)$. As F_1 and Ω_2 are linearly disjoint over E, F_1 and F_2 are so over E. Thus F_1^{alg} and F_2^{alg} are linearly disjoint over E^{alg}, and there is a unique automorphism τ of $F_1^{\mathrm{alg}}F_2^{\mathrm{alg}}$ (which is over F_1F_2) extending both σ_1 and $\sigma_2|_{F_2^{\mathrm{alg}}}$. Lift τ to an automorphism of $(F_1F_2)^{\mathrm{alg}}$, which we also denote by τ, and let $L = \mathrm{Fix}((F_1F_2)^{\mathrm{alg}}, \tau)$ be the fixed field of τ inside $(F_1F_2)^{\mathrm{alg}}$. Then L is perfect and τ generates $\mathrm{Gal}(L)$. By the choice of τ and and because F_1 and F_2 are perfect, the field extensions L/F_1 and L/F_2 are regular and the respective restriction maps of absolute Galois groups are isomorphisms. So by lemma (4.4) there is an F_2-embedding φ of L into Ω_2 such that $\Omega_2/\varphi(L)$ is regular. L/F_1 being regular it follows that $\Omega_2/\varphi(F_1)$ is a regular extension, too. This proves the claim.

Applying a back-and-forth argument, the proof of the theorem is complete. □

Corollary 4.5 (Ax, Chatzidakis - van den Dries - Macintyre). *Let F_1 and F_2 be pseudo-finite fields.*

1. *$F_1 \equiv F_2$ if and only if $\mathrm{abs}(F_1) \cong \mathrm{abs}(F_2)$.*
2. *Let further E be a common subfield and $\bar{a} \in F_1$ and $\bar{b} \in F_2$ be tuples (of the same length). Then $\mathrm{tp}_{F_1}(\bar{a}/E) = \mathrm{tp}_{F_2}(\bar{b}/E)$ if and only if there is an E-isomorphism*
$$E(\bar{a})^{\mathrm{alg}} \cap F_1 \xrightarrow{\varphi} E(\bar{b})^{\mathrm{alg}} \cap F_2$$
with $\varphi(\bar{a}) = \bar{b}$.
3. *If $E \subseteq F$ are pseudo-finite, then $E \preccurlyeq F$ iff $E^{\mathrm{alg}} \cap F = E$ iff F/E is regular.*
4. *If A is a subset of the pseudo-finite field F, then the model theoretic algebraic closure of A is $\mathrm{acl}(A) = \mathbb{F}_p(A)^{\mathrm{alg}} \cap F$.*

Proof. (1) and (2) are special instances of theorem (4.2). So is (3) in view of the fact that if K is a perfect field and relatively algebraically closed in a field extension F, then F/K is regular. (4) is proved using the following standard argument, which we repeat for convenience. Assume

some saturation of F and denote $K = \mathbb{F}_p(A)^{\mathrm{alg}} \cap F$. If $\bar{x} \in F$ is a finite tuple with $\bar{x} \notin K$, the field $L = K(\bar{x})^{\mathrm{alg}} \cap F$ is a regular extension of K because F/K is. For any $n \in \mathbb{N}$ let $L_1, \ldots, L_n$ be K-isomorphic copies of L that are pairwise linearly disjoint over K, and consider the field compositum $\mathbb{L}_n = L_1 \ldots L_n$ of the L_i. $\mathbb{L}_n$ is a regular extension of K, so as F is PAC and enough saturated, we can assume that $\mathbb{L}_n$ is a subfield of F. The L_i are K-isomorphic to L, so letting $\bar{x}_i$ be the K-isomorphic images of $\bar{x}$ in L_i, we conclude by *2.* that $\mathrm{tp}(\bar{x}/K)$ is not algebraic. □

Note that if $E \preccurlyeq F$ are pseudo-finite fields, then as the absolute Galois groups of both is $\widehat{\mathbb{Z}}$, it follows that $E^{\mathrm{alg}}F = F^{\mathrm{alg}}$.

If K is a pseudo-finite field, then the absolute Galois group of $\mathrm{abs}(K)$ is procyclic because $K/\mathrm{abs}(K)$ is regular (and hence the restriction map $\mathrm{Gal}(K) \longrightarrow \mathrm{Gal}(\mathrm{abs}(K))$ of Galois groups is surjective). Using the Cebotarev Density Theorem and the Lang-Weil Theorem, Ax shows in [**2**] that conversely to any $k \subset \mathbb{F}_p^{\mathrm{alg}}$ with procyclic absolute Galois group there is some pseudo-finite field F with $\mathrm{abs}(F) = k$. (Of course if $p > 0$, then any field $k \subset \mathbb{F}_p^{\mathrm{alg}}$ has this property.) Let us mention that this can be seen using only basic properties of the theory $ACFA$ (see section 4.2): Given $k \subset \mathbb{F}_p^{\mathrm{alg}}$ as above, choose a topological generator τ of $\mathrm{Gal}(k)$. The difference field $(\mathbb{F}_p^{\mathrm{alg}}, \tau)$, whose fixed field is k by choice, embeds into some model (Ω, σ) of $ACFA$. Its fixed field F is pseudo-finite and has absolute part k because $\sigma|_{\mathbb{F}_p^{\mathrm{alg}}} = \tau$. We summarise this in the following proposition.

Proposition 4.6 (Ax). *The completions of PSF are in one-to-one correspondence with the subfields of $\mathbb{F}_p^{\mathrm{alg}}$ (with p varying, and $\mathbb{F}_0 = \mathbb{Q}$) whose absolute Galois group is procyclic.*

The next theorem was proved by Ax in [**2**]. Together with the failure of Zil'ber's conjecture it motivated the model theoretic study of generic difference fields.

Theorem 4.7 (Ax). *A field K is pseudo-finite if and only if it is elementarily equivalent to some non-principal ultraproduct of finite fields. If the characteristic of K is zero one may take a non-principal ultraproduct of the prime fields $\mathbb{F}_p$, where p runs over the prime numbers, if the characteristic of K is $p > 0$ one may take a non-principal ultraproduct of the fields $\mathbb{F}_{p^n}$, where $n \in \mathbb{N}_{>0}$.*

The proof of theorem (4.7) relies on the Cebotarev Density Theorem, as well as on the Theorem of Lang-Weil. Hrushovski succeeded in generalising it to difference fields, a proof of which we have included in section 4.2.1 (modulo Hrushovski's analogue of the Lang-Weil Theorem for difference fields).

Our short exposition on pseudo-finite fields has to stay far from being complete. Among the numerous interesting facts on them we do not mention the dimension- and measure-theoretic properties of definable sets which were discovered in [**13**]. Also, pseudo-finite fields are archetypical examples of supersimple fields. Supersimplicity of pseudo-finite fields has been shown by Hrushovski in [**26**]. We do not include Hrushovski's original proof of this result here, because supersimplicity can also be derived from supersimplicity

of $ACFA$ and the fact that any pseudo-finite field embeds elementarily into the fixed field of some model of $ACFA$ (see proposition (4.16)).

4.2. Generic Difference Fields

Recall that a difference field is a field K with a distinguished endomorphism σ. This section recalls some of the basic theory of existentially closed difference fields from the literature, and fixes notation concerning difference fields. There is numerous literature on $ACFA$. Our exposition owes much the lecture notes on $ACFA$ of Chatzidakis [**10**]. Other references are of course [**39**], [**14**], [**15**] and [**11**], to mention only a few. Also, we have included a proof of Hrushovski's theorem on ultraproducts of difference fields $(\mathbb{F}_p^{\text{alg}}, \phi_q)$, modulo his analogue of the Lang-Weil Theorem for difference fields. As our main goal is the proof of theorems (4.24), (4.32) and (4.33) in the next section, we cannot aim for a complete overview of the known results about the theory of difference fields, but provide the reader with background material in order to appreciate the next section.

A difference field (K, σ) is called generic if it is existentially closed among difference fields. As we are in fields, this is equivalent to any finite system of difference equations

$$f_1(\bar{X}) = \cdots = f_r(\bar{X}) = 0$$

with coefficients from K having a solution in some difference field extension of (K, σ) has a solution in (K, σ). Newly the term difference closed field is used in the literature for what we call generic difference field. There is no particular reason we stick to the term generic, and hope not to cause any irritation by doing so.

We recall in this section some of the basic model theory of (generic) difference fields from [**39**], [**14**] and [**15**]. The language we work in is the natural language L_σ of difference fields, which is the ring language $L = \{+, -, \cdot, 0, 1\}$ augmented by a new unary function symbol σ for the endomorphism. The class of generic difference fields is axiomatisable in the language L_σ by the theory $ACFA$:

Definition 4.8. *$ACFA$ is the theory consisting of the following axiom schemes describing properties of difference fields (K, σ).*

- *(i) σ is an automorphism of K,*
- *(ii) K is an algebraically closed field, and*
- *(iii) for every affine variety U, and any variety $V \subseteq U \times U^\sigma$ projecting generically onto U and U^σ, there is a tuple $\bar{a} \in K$ such that $(a, \sigma(a)) \in V$. Here, as usual, U^σ denotes the variety obtained by applying σ to the defining equations of U.*

Theorem 4.9 (Chatzidakis-Hrushovski). *$ACFA$ is model complete. Any difference field embeds into some model of $ACFA$.*

Proof. See [**14**], theorem (1.1). □

So $ACFA$ is the model companion of the theory of difference fields. We write acl_σ for the model-theoretic algebraic closure in $ACFA$. There is another closure in models of $ACFA$: if A is a subset of some model of $ACFA$, we denote by $\mathrm{cl}_\sigma(A)$ the closure of A under σ and σ^{-1}. One could define cl_σ for arbitrary difference fields, but we use it only in models of $ACFA$.

$ACFA$ is not complete. Its completions are obtained by specifying the characteristic and describing the action of σ on the algebraic closure of the prime field. More generally, one has the following theorem.

THEOREM 4.10 (Chatzidakis-Hrushovski). *If (Ω_1, σ_1) and (Ω_2, σ_2) are models of $ACFA$ with common subdifference field (E, σ), then*

$$(\Omega_1, \sigma_1) \equiv_E (\Omega_2, \sigma_2) \quad \textit{iff} \quad (E^{\mathrm{alg}}, \sigma_1|_{E^{\mathrm{alg}}}) \cong_E (E^{\mathrm{alg}}, \sigma_2|_{E^{\mathrm{alg}}}) \ .$$

Proof. See [**14**], theorem (1.3). □

If $\bar{a}$ is a tuple from a model of $ACFA$ in which (K, σ) is contained as a subdifference field (with K algebraically closed), then (obviously) $I_\sigma(\bar{a}/K)$ describes the quantifier-free type of $\bar{a}$ over K. From the previous theorem, one obtains an algebraic description of the types, as well of the model-theoretic algebraic closure in $ACFA$.

COROLLARY 4.11 (Chatzidakis-Hrushovski). *Let (Ω_1, σ_1) and (Ω_2, σ_2) be models of $ACFA$ with common subdifference field (E, σ). Then*

1. $(\Omega_1, \sigma_1) \equiv (\Omega_2, \sigma_2)$ *iff* $(\mathbb{F}_p^{\mathrm{alg}}, \sigma_1) \cong (\mathbb{F}_p^{\mathrm{alg}}, \sigma_2)$ *iff there is* $\tau \in \mathrm{Gal}(\mathbb{F}_p)$ *with* $\sigma_1 \tau = \tau \sigma_2$ *on* $\mathbb{F}_p^{\mathrm{alg}}$.
2. $\mathrm{tp}_{(\Omega_1,\sigma_1)}(\bar{a}/E) = \mathrm{tp}_{(\Omega_2,\sigma_2)}(\bar{b}/E)$ *iff there is an E-isomorphism of difference fields*
$$(E(\bar{a})_\sigma^{\mathrm{alg}}, \sigma_1) \xrightarrow{\ \varphi\ } (E(\bar{b})_\sigma^{\mathrm{alg}}, \sigma_2)$$
with $\varphi(\bar{a}) = \bar{b}$.
3. *If A is a subfield of (Ω_1, σ_1), then the model-theoretic algebraic closure of A is* $\mathrm{acl}_\sigma(A) = (\mathrm{cl}_\sigma(A))^{\mathrm{alg}}$.

Proof. (1) and (2) are just instances of theorem (4.10). For a proof of (3), we refer to proposition (1.7) of [**14**]. □

Recall that an element a in a model (Ω, σ) of $ACFA$ is called transformally algebraic over some subdifference field K if $I_\sigma(a/K) \neq 0$. A tuple $\bar{a}$ is called transformally algebraic if all its elements are. A finite tuple is transformally algebraic if and only if there is some $n \in \mathbb{N}$ such that $\mathrm{acl}_\sigma(K, \bar{a}) = K(\bar{a}, \ldots, \sigma^n(\bar{a}))^{\mathrm{alg}}$. The following remark was proved in (1.1) of [**14**].

REMARK 4.12 (Chatzidakis-Hrushovski). *For any model (Ω, σ) of $ACFA$ and any subset A of Ω, the elements of Ω that are transformally algebraic over A form an elementary substructure of (Ω, σ).*

Let (Ω, σ) be a generic difference field and $\bar{X} = X_1, \ldots, X_n$. For any $S \subset \Omega[\bar{X}]_\sigma$ we let

$$V_\sigma(S) = \{\, \bar{a} \in \Omega^n \mid f(\bar{a}) = 0 \text{ for all } f \in S \,\}$$

and call sets of this form σ-algebraic or σ-closed subsets of Ω^n. This defines a topology on Ω^n, which is called the σ-topology on Ω^n. If (K,σ) is an algebraically closed subdifference field of (Ω,σ) and $S \subset K[\bar{X}]_\sigma$, we say that $V_\sigma(S)$ is a σ-algebraic set over K. If $V = V_\sigma(S)$ is over K and L is subdifference field of Ω containing K, we write $V(L)$ for the set of solutions of S in L^n.

For any $S,T \subseteq K[\bar{X}]_\sigma$, one has $V_\sigma(S) = V_\sigma((S)_{\text{perf}})$, and $(S)_{\text{perf}} \subseteq (T)_{\text{perf}}$ if and only if $V_\sigma(S) \supseteq V_\sigma(T)$. If S is a perfect difference ideal, then $S = I_\sigma(V_\sigma(S))$. As $\Omega[\bar{X}]_\sigma$ is Ritt, any perfect difference ideal is finitely generated, so that $V_\sigma(S) = V_\sigma(f_1,\ldots,f_r)$ for suitable difference polynomials $f_i \in \Omega[\bar{X}]_\sigma$ (using elimination of imaginaries, discussed below, and (K,σ) being an algebraically closed subdifference field of (Ω,σ), one can find the f_i's in $K[\bar{X}]_\sigma$ even). Hence σ-algebraic sets are definable, and the σ-topology is noetherian. With the above description of types and acl_σ, it follows by compactness that modulo $ACFA$, any formula $\varphi(\bar{x})$ is equivalent to a finite disjunction of formulas of the form $\exists y\, \psi(\bar{x},y)$, where $\psi(\bar{x},y)$ is quantifier-free and has the property that for any tuple $(\bar{a},b)$ realizing ψ in some difference field, b is (field-) algebraic over $\bar{a},\sigma(\bar{a}),\ldots,\sigma^n(\bar{a})$ for some $n \in \mathbb{N}$. In more geometric words, this reads as follows: for any definable set $D \subseteq \Omega^n$ there is a σ-closed set $W \subseteq \Omega^{n+m}$ such that $D = \pi(W)$, where $\pi : \Omega^{n+m} \longrightarrow \Omega^n$ is the projection on the first n coordinates and such that π is finite-to-one on W.

We will use the term difference variety over K for a a non-empty σ-algebraic subset V of some sufficiently saturated model of $ACFA$, if V is over the algebraically closed difference field K and its vanishing ideal $I_\sigma(V/K)$ in $K[\bar{X}]_\sigma$ is prime. In this case, $K[V]_\sigma := K[\bar{X}]_\sigma/I_\sigma(V)$ resp. $K(V)_\sigma := \text{Quot}(K[V]_\sigma)$, both together with their canonical endomorphisms, are called the difference coordinate ring resp. the difference rational function field of V over K. These will be the only non-inversive difference rings considered in this thesis.

Let A,B and C be subsets of some model (Ω,σ) of $ACFA$. A and B are called independent over C if $\text{acl}_\sigma(AC)$ and $\text{acl}_\sigma(BC)$ are linearly disjoint over $\text{acl}_\sigma(C)$. Clearly this notion of independence is invariant under automorphisms, and satisfies Symmetry and Finite Character. It satisfies Transitivity as $\text{acl}_\sigma(A,B) = (\text{acl}_\sigma(A)\text{acl}_\sigma(B))^{\text{alg}}$ for any sets A and B. That it satisfies Extension is seen using the amalgamation property of algebraically closed difference fields and model completeness of $ACFA$ together with theorem (4.10). If $\bar{a}$ is a finite tuple and C some parameter set (without loss a subdifference field), then $I_\sigma(\bar{a}/C)$ is a perfect difference ideal, hence finitely generated because $C[\bar{X}]_\sigma$ is Ritt. If C_0 denotes the set of coefficients of some finite set of generators of $I_\sigma(\bar{a}/C)$, then $\bar{a}$ is independent from C over C_0 by the description of acl_σ and because the isomorphism type of $C(\bar{a})_\sigma$ is given by $I_\sigma(\bar{a}/C)$. So by the following theorem, the notion of independence defined above is the non-forking independence and $ACFA$ is supersimple.

THEOREM 4.13 (Independence Theorem; Chatzidakis-Hrushovski). *Let (Ω,σ) be a model of $ACFA$, enough saturated. Let $E = \text{acl}_\sigma(E)$ be an algebraically closed subdifference field of (Ω,σ) and $\bar{z}_1$ and $\bar{z}_2$ be tuples of*

the same type over E in Ω. Let further $\bar{a}$ and $\bar{b}$ be tuples in Ω, independent over E, such that $\bar{z}_1$ is independent from $\bar{a}$ over E and $\bar{z}_2$ is independent from $\bar{b}$ over E. Then there is some tuple $\bar{z}$ in Ω satisfying $\mathrm{tp}(\bar{z}_1/E\bar{a}) \cup \mathrm{tp}(\bar{z}_2/E\bar{b})$ *which is independent from $\bar{a}\bar{b}$ over E.*

Proof. This is a special case of [**14**], theorem (1.9). □

As a consequence of the Independence Theorem one obtains elimination of imaginaries for every completion of $ACFA$.

Proposition 4.14 (Chatzidakis-Hrushovski). *Any completion of $ACFA$ eliminates imaginaries.*

Proof. See [**14**], theorem (1.10). □

Recall that for any difference field (K, σ) we defined the fixed field of (K, σ) to be

$$\mathrm{Fix}(K, \sigma) = \{\, a \in K \mid \sigma(a) = a \,\}.$$

If m and n are integers with $n \neq 0$ such that $\sigma^n \phi_p^m$ is an endomorphism of K, where ϕ_p denotes the Frobenius automorphism in characteristic $p > 0$ and the identity otherwise, it has become a custom to call the fields $\mathrm{Fix}(K, \sigma^n \phi_p^m)$ also fixed fields of (K, σ), and to refer to $\mathrm{Fix}(K, \sigma)$ as *the* fixed field of (K, σ).

Let for the moment L be an arbitrary first order language. Let M be an L-structure and $n \in \mathbb{N}$. Recall that a $\emptyset$-definable subset P of M^n is called stably embedded in M if for any m and any set $X \subset M^{mn}$ which is definable using parameters, $X \cap P^m$ is definable using parameters from P. We recall the following lemma from [**14**].

Lemma 4.15 (Chatzidakis-Hrushovski). *Let M be sufficiently saturated and $P \subset M^n$ be definable over $\emptyset$. Then P is stably embedded in M if and only if any automorphism of P^{ind} lifts to an automorphism of M. Here P^{ind} denotes P with its induced structure from M, i.e. the $\emptyset$-definable subsets of P^m are those of the form $P^m \cap X$ for $\emptyset$-definable $X \subset M^{mn}$.*

Proof. See lemma 1 of the appendix of [**14**]. □

We now come back to difference fields:

Proposition 4.16 (Chatzidakis-Hrushovski-Peterzil).

(1) *Let (Ω, σ) be a model of $ACFA$. Then for all integers m and n (with $n \neq 0$) the fixed fields $F = \mathrm{Fix}(\Omega, \sigma^n \phi_p^m)$ are pseudo-finite fields, and are stably embedded in (Ω, σ). If $n = 1$, then any subset of F^k that is definable in (Ω, σ) using parameters is definable in the pure field F, maybe with parameters from F.*

(2) *If F is a pseudo-finite field, then there is some model (Ω, σ) of $ACFA$ such that* $\mathrm{Fix}(\Omega, \sigma) \equiv F$.

Proof. (1) is proposition (7.1) of [**15**]. (2) is folklore, but we give a possible proof. Let K be a pseudo-finite field and choose a (topological) generator of its absolute Galois group, say τ. Obviously $K = \mathrm{Fix}(K^{\mathrm{alg}}, \tau)$. By model completeness of $ACFA$ the difference field (K^{alg}, τ) embeds into

some model (Ω, σ) of $ACFA$. Identifying (K^{alg}, τ) with its image, one has $\sigma|_{K^{\text{alg}}} = \tau$ and so $\text{Fix}(\Omega, \sigma)$ is a regular extension of K. Then corollary (4.5.3) (which is proposition (20.10.2) of [**22**]) implies that the extension $\text{Fix}(\Omega, \sigma)/K$ is elementary. □

The following easy remark will prove useful later on, so we state it explicitly. The second reason to do so is that it will be crucial in chapter 5, where it will be suitably generalised.

REMARK 4.17. *Let (Ω, σ) be a sufficiently saturated model of $ACFA$ and $k \preccurlyeq \text{Fix}(\Omega, \sigma)$. Then any field automorphism α of $\text{Fix}(\Omega, \sigma)$ over k lifts to an automorphism of (Ω, σ).*

Proof. Denote $F = \text{Fix}(\Omega, \sigma)$ and let α be a (field-) automorphism of F over k. As F is a regular extension of k, there is a unique automorphism $\bar{\alpha}$ of $k^{\text{alg}}F$ lifting α and the identity on k^{alg} by lemma (1.18). $\bar{\alpha}$ commutes with σ, so as $k^{\text{alg}}F = F^{\text{alg}} = \text{acl}_\sigma(F)$, it is elementary in the sense of $ACFA$ by proposition (4.10). Thus α is an automorphism of F^{ind}. As F is stably embedded in (Ω, σ) by proposition (4.16), lemma (4.15) implies that α lifts to an automorphism of (Ω, σ). □

We briefly recall the induced structure from models of $ACFA$ on the fixed field from [**14**], to which we refer for more details and proofs. Let (Ω, σ) be a model of $ACFA$ and denote $F = \text{Fix}(\Omega, \sigma)$. For $n > 1$, let S_n be the imaginary sort whose elements are the isomorphism types over F of difference fields (L, τ), where L is an extension of F of degree n and $\tau \in \text{Gal}(L/F)$. More precisely, if L is an extension of F of degree n and $\tau \in \text{Gal}(L/F)$, then by a standard argument there is some finite parameter tuple $\bar{c} \in F$ of length $2n$ such that the difference field (L, τ) is interpretable in the pure field F using $\bar{c}$. Each element $e \in S_n$ corresponds to the definable subset of F^{2n} coding the corresponding difference field (L, τ). As $\text{Gal}(L/F)$ is abelian, it follows that S_n has precisely n elements.

PROPOSITION 4.18 (Chatzidakis-Hrushovski). *Let (Ω, σ) be a model of $ACFA$ and $F = \text{Fix}(\Omega, \sigma)$. Then the induced structure on F from (Ω, σ) is precisely the field structure together with distinguished constants $e_{j,n} \in S_n$, for $n > 1$ and $0 \leq j < n$, where $e_{j,n}$ codes the isomorphism type over F of the difference field $(\text{Fix}(\Omega, \sigma^n), \sigma^j_{\text{Fix}(\Omega, \sigma^n)})$.*

Proof. See [**14**], proposition A of (1.13). □

4.2.1. Ultraproducts of Frobenii. Hrushovski proved the generalisation of Ax' theorem (4.7) for difference fields in [**28**], see theorem (4.19). In this paragraph, we present a possible proof of Hrushovski's theorem, modulo his analogue for difference fields of the Lang-Weil theorem (1.16) (see theorem (4.21) below). It is needless to say that the results in this paragraph are not original to the present author. The proof that theorem (4.21) implies that any non-principal ultraproduct of the difference fields $(\mathbb{F}_p^{\text{alg}}, \phi_q)$ is a model of $ACFA$ is taken from [**10**].

THEOREM 4.19 (Hrushovski). *Let (K,σ) be a difference field. Then (K,σ) is a model of $ACFA$ if and only if there is some non-principal ultraproduct $(\mathcal{R},\sigma_{\mathcal{R}})$ of difference fields $(\mathbb{F}_p^{\mathrm{alg}},\phi_q)$ such that $(K,\sigma)\equiv(\mathcal{R},\sigma_{\mathcal{R}})$. If the characteristic of K is zero one may take a non-principal ultraproduct of difference fields $(\mathbb{F}_p^{\mathrm{alg}},\phi_p)$, where p runs over the prime numbers. If the characteristic of K is $p>0$ one may take a non-principal ultraproduct of the fields $(\mathbb{F}_p^{\mathrm{alg}},\phi_{p^n})$, where $n\in\mathbb{N}_{>0}$.*

Note first that this theorem implies Ax' theorem (4.7). Indeed, the fixed field of an ultraproduct $\prod(\mathbb{F}_p^{\mathrm{alg}},\phi_q)/\mathcal{U}$ is isomorphic to the ultraproduct $\prod \mathrm{Fix}(\mathbb{F}_p^{\mathrm{alg}},\phi_q)/\mathcal{U}$. So any non-principal ultraproduct of finite fields is a pseudo-finite field by proposition (4.16). Furthermore, given a pseudo-finite field K, the above theorem and proposition (4.16) imply there is some non-principal ultraproduct of finite fields that is elementarily equivalent to F.

That any non-principal ultraproduct of the difference fields $(\mathbb{F}_p^{\mathrm{alg}},\phi_q)$ is a model of $ACFA$ relies on two ingredients, the first one being the observation that the axioms of $ACFA$ can be weakened as follows.

PROPOSITION 4.20. *Let (K,σ) be an algebraically closed difference field. Then (K,σ) is a model of $ACFA$ if and only if:*

> *For every affine variety U, and any variety $V\subseteq U\times U^{\sigma}$ with $\dim(U)=\dim(V)$ projecting generically onto U and U^{σ}, there is some tuple $\bar{a}\in K$ such that $(\bar{a},\sigma(\bar{a}))\in V$.*

Proof. The proof of the proposition is sketched in [**10**]. For convenience we give it here. The implication from left to right is clear. For the converse let (K,σ) be an algebraically closed difference field with the above property. It is contained in some model (Ω,σ) of $ACFA$, and we are going to show that (K,σ) is a model of $ACFA$, too. So let U and V be varieties over K such that $V\subseteq U\times U^{\sigma}$ and V projects generically onto U and U^{σ} respectively. By remark (4.12) there is some tuple $\bar{a}\in\Omega$ with $(\bar{a},\sigma(\bar{a}))\in V$ and which is transformally algebraic over K. In particular there is some $n\in\mathbb{N}$ such that

$$\sigma^{n+1}(\bar{a})\in K(\bar{a},\sigma(\bar{a}),\ldots,\sigma^n(\bar{a}))^{\mathrm{alg}}\ .$$

Now consider the varieties U' and V' over K whose generic points are

$$(\bar{a},\ldots,\sigma^n(\bar{a}))\text{ and }(\bar{a},\ldots,\sigma^n(\bar{a});\sigma(\bar{a}),\ldots,\sigma^{n+1}(\bar{a})))$$

respectively. U' and V' have the same dimension because $\sigma^{n+1}(\bar{a})$ is (field-) algebraic over $K,\bar{a},\ldots,\sigma^n(\bar{a})$, and clearly $V'\subseteq U'\times U'^{\sigma}$. Furthermore, by the very choice of U' and V', V' projects generically onto U' and U'^{σ} respectively. So by assumption there is some tuple $\bar{b}=\bar{b}_1,\ldots,\bar{b}_n\in K$ such that $(\bar{b},\sigma(\bar{b}))\in V'$. But then $(\bar{b}_1,\sigma(\bar{b}_1))\in V$ because $(\bar{a},\sigma(\bar{a}))\in V$, and we are done. □

The second ingredient for the proof of theorem (4.19) is the famous analogue of the Lang-Weil estimates for difference fields due to Hrushovski, which he proves in [**28**]. Our formulation is taken from [**10**].

THEOREM 4.21 (Hrushovski). *Let $f_1(\bar{X},\bar{Z}),\ldots,f_n(\bar{X},\bar{Z})$ and $g_1(\bar{X},\bar{Y},\bar{Z}),\ldots,g_m(\bar{X},\bar{Y},\bar{Z})$ be polynomials over $\mathbb{Z}$. Then there is some positive constant C such that for all prime number p and power q of p and all tuples $\bar{a}\in\mathbb{F}_p^{\mathrm{alg}}$, if the equations $f_1(\bar{X},\bar{a})=\cdots=f_n(\bar{X},\bar{a})=0$ and $g_1(\bar{X},\bar{Y},\bar{a})=\cdots=g_m(\bar{X},\bar{Y},\bar{a})=0$ define algebraic varieties U and V over $\mathbb{F}_p^{\mathrm{alg}}$ satisfying the requirements of the above proposition (4.20), then*

$$\Big|\ |\{\bar{a}\in\mathbb{F}_p^{\mathrm{alg}}\ :\ (\bar{a},\phi_q(\bar{a}))\in V\}|\ -cq^d\Big|\leq Cq^{d-1/2}\ .$$

Here $d=dim(U)=dim(V)$ and $c=[\mathbb{F}_p^{\mathrm{alg}}(V):\mathbb{F}_p^{\mathrm{alg}}(U)]/[\mathbb{F}_p^{\mathrm{alg}}(V):\mathbb{F}_p^{\mathrm{alg}}(U^\sigma)]_{ins}$.

That this generalises the Lang-Weil theorem (1.16) is seen as follows: if W is a variety over $\mathbb{F}_q$, then one takes $U=W$ and V the diagonal of $U\times U$.

Now let $(\mathcal{K},\sigma)$ be any non-principal ultraproduct of difference fields $(\mathbb{F}_p^{\mathrm{alg}},\phi_q)$. Given any (affine) varieties U and V with $V\subseteq U\times U^\sigma$ and $\dim(U)=\dim(V)$ such that V projects generically onto U and U^σ, it follows from the above theorem that for ultrafilter-many $(\mathbb{F}_p^{\mathrm{alg}},\phi_q)$ there is some $\bar{a}\in\mathbb{F}_p^{\mathrm{alg}}$ such that $(\bar{a},\sigma(\bar{a}))\in V$. So $(\mathcal{K},\sigma)$ is a model of $ACFA$ by proposition (4.20).

For the other direction, we subdivide into two cases, the case of characteristic zero and of positive characteristic. Let us start with the positive characteristic case.

Proof of theorem (4.19) for positive characteristic. Let (K,σ) be a model of $ACFA$ of characteristic $p>0$. We are going to "construct" a non-principal ultrafilter $\mathcal{U}$ on the naturals $\mathbb{N}$ such that

$$\prod_{n\in\mathbb{N}}(\mathbb{F}_p^{\mathrm{alg}},\phi_{p^n})/\mathcal{U}\ \equiv(K,\sigma)\,.$$

Let $(\nu_n)_{n\in\mathbb{N}}$ be a sequence of natural numbers such that $\sigma|_{\mathbb{F}_{p^n}}=\phi_p^{\nu_n}$ for every $n\in\mathbb{N}$. For any $n\in\mathbb{N}$ we let

$$b_n=\{m\in\mathbb{N}\mid m=\nu_n \bmod n\}\ .$$

Then clearly $m\in b_n$ iff $\phi_p^m=\sigma|_{\mathbb{F}_{p^n}}$. We content that

$$\mathcal{V}=\ \{b_n\mid n\in\mathbb{N}\}\cup\mathrm{Cofin}(\mathbb{N})$$

has the finite intersection property. Indeed, any b_n is infinite, and if k denotes the greatest common divisor of the naturals n_1 and n_2, then by the choice of the ν_i we have $b_k\subseteq b_{n_1}\cap b_{n_2}$.

Let $\mathcal{U}$ be an ultrafilter containing $\mathcal{V}$ and $(\mathcal{K},\tau)$ be the difference field $\prod_{n\in\mathbb{N}}(\mathbb{F}_p^{\mathrm{alg}},\phi_{p^n})/\mathcal{U}$. As $(\mathbb{F}_{p^n},\sigma|_{\mathbb{F}_{p^n}})\subset(\mathbb{F}_p^{\mathrm{alg}},\phi_p^\nu)$ for any $\nu\in b_n$, it follows that $(\mathbb{F}_{p^n},\sigma|_{\mathbb{F}_{p^n}})\subset(\mathbb{F}_p^{\mathrm{alg}},\phi_p^\nu)$ for $\mathcal{U}$-many ν. Thus $\sigma|_{\mathbb{F}_p^{\mathrm{alg}}}=\tau|_{\mathbb{F}_p^{\mathrm{alg}}}$, and hence $(K,\sigma)\equiv(\mathcal{K},\tau)$ by corollary (4.11.1). □

The proof in the characteristic zero case will require the Cebotarev Density Theorem, which we briefly recall for convenience from [**22**]. We treat the number field case only, the function field case working alike (consult

[**22**]). In fact for the proof below it would suffice to consider only finite Galois extensions of $\mathbb{Q}$ rather than of number fields.

Cebotarev Density Theorem. Let $\mathfrak{p}$ be a prime ideal of a number field K. We write $\mathcal{O}_\mathfrak{p}$ for the valuation ring and $K(\mathfrak{p})$ for the residue field corresponding to $\mathfrak{p}$. Assume that $\mathfrak{p}$ is unramified in a finite Galois extension L/K. For an extension $\mathfrak{P}$ of $\mathfrak{p}$ to L we denote by $D(L/K,\mathfrak{P})$ the decomposition group of $\mathfrak{P}$, which is the subgroup of $\mathrm{Gal}(L/K)$ of all $\alpha \in \mathrm{Gal}(L/K)$ with $\alpha(\mathfrak{P}) = \mathfrak{P}$. As $\mathfrak{p}$ is unramified in L/K, the canonical endomorphism

$$\Phi_\mathfrak{P} : \ D(L/K,\mathfrak{P}) \ \longrightarrow \ \mathrm{Gal}(L(\mathfrak{P})/K(\mathfrak{p}))$$

defined by $\Phi_\mathfrak{P}(\sigma)(\bar{a}) = \overline{\sigma(a)}$ for $a \in \mathcal{O}_\mathfrak{P}$, is an isomorphism. Now $K(\mathfrak{p})$ is a finite field, say with p^r elements. So ϕ_p^r is a generator $\mathrm{Gal}(L(\mathfrak{P})/K(\mathfrak{p}))$. The preimage in $D(L/K,\mathfrak{P})$ under $\Phi_\mathfrak{P}$ of this generator is called the Frobenius automorphism of $\mathfrak{P}$ in L/K. We denote it by $\mathrm{Fr}_\mathfrak{P}^{L/K}$ or simply $\mathrm{Fr}_\mathfrak{P}$ if there is no danger of ambiguity. As $\mathfrak{P}$ ranges over its conjugates $\tau\mathfrak{P}$ under $\mathrm{Gal}(L/K)$ (so over all extensions of $\mathfrak{p}$ in L/K), $\mathrm{Fr}_\mathfrak{P}$ ranges over all its conjugates $\tau\mathrm{Fr}_\mathfrak{P}\tau^{-1}$ under $\mathrm{Gal}(L/K)$. In this manner $\mathfrak{p}$ determines a conjugacy class in $\mathrm{Gal}(L/K)$, which is written $\left(\frac{L/K}{\mathfrak{p}}\right)$ and called the Artin-symbol of $\mathfrak{p}$ in L/K. It is tacit to this symbol that $\mathfrak{p}$ is unramified in L/K. Finally, the Dirichlet density of a set A of primes in K is defined to be

$$\delta(A) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in A} \mathbb{N}\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}\in\mathcal{P}(K)} \mathbb{N}\mathfrak{p}^{-s}}$$

if this limit exists, where $\mathcal{P}(K)$ denotes the set of primes in K and $\mathbb{N}\mathfrak{p}$ the number of elements of $K(\mathfrak{p})$ (called the absolute norm of $\mathfrak{p}$). The fact we need about the Dirichlet density is that if A is a finite set, then $\delta(A) = 0$.

Theorem 4.22 (Cebotarev). *Let L/K be a finite Galois extension of global fields and $\sigma \in \mathrm{Gal}(L/K)$. Then the Dirichlet density of $P_{L/K}(\sigma)$ exists and equals $|\mathcal{C}|/|\mathrm{Gal}(L/K)|$, where $\mathcal{C}$ is the conjugacy class of σ in $\mathrm{Gal}(L/K)$.*

Here $P_{L/K}(\sigma)$ is the set of primes $\mathfrak{p}$ with $\sigma \in \left(\frac{L/K}{\mathfrak{p}}\right)$. The consequence of the Cebotarev Density Theorem we are after is that under the assumption of the theorem the set $P_{L/K}(\sigma)$ is infinite.

Proof of Theorem 4.19 for characteristic zero. Let (K,σ) be a model of $ACFA$ of characteristic zero. We will "construct" an ultrafilter $\mathcal{U}$ on the set $\mathcal{P}(\mathbb{Q})$ of primes in $\mathbb{Q}$ such that

$$\prod_{p\in\mathcal{P}(\mathbb{Q})} (\mathbb{F}_p^{\mathrm{alg}}, \phi_p)/\mathcal{U} \equiv (K,\sigma)\,.$$

First note that for a finite Galois extension $L/\mathbb{Q}$ and any automorphism $\beta \in \mathrm{Gal}(L/\mathbb{Q})$ it is an elementary property of β (strictly speaking of the difference field (L,β)) to be in a given conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(L/\mathbb{Q})$. Indeed, any two automorphisms of L are conjugate in $\mathrm{Gal}(L/\mathbb{Q})$ if and only

if the corresponding difference fields are isomorphic. Now choose a primitive element α of $L/\mathbb{Q}$ and let n be the degree of $L/\mathbb{Q}$. Then the action of β on L is determined by its action on α, which can be expressed in L_σ. Thus the isomorphism type of the difference field (L, β) is described by the L_σ-sentence

$$\exists\, x \quad p(x) = 0 \ \wedge \ \sigma(x) = \sum_{\nu=0}^{n-1} a_\nu x^\nu \ ,$$

where $p(X)$ is the minimal polynomial of α over $\mathbb{Q}$ and $a_\nu \in \mathbb{Q}$ are chosen appropriately. Note aside that the two above equations generate the vanishing difference ideal of α over $\mathbb{Q}$, which in turn determines the isomorphism type of the difference field structure on L. All parameters are in $\mathbb{Q}$, so multiplying by the common denominator of the parameters, we obtain an L_σ-sentence without parameters, which we denote $\psi_{p,\mathcal{C}}$ or ψ_p if it is clear which conjugacy class is meant.

Now we write $\mathbb{Q}^{\mathrm{alg}}$ as an ascending union $\mathbb{Q}^{\mathrm{alg}} = \bigcup_{\nu\in\mathbb{N}} \mathbb{Q}(\alpha_\nu)$ of finite Galois extensions $\mathbb{Q}(\alpha_\nu)$ of $\mathbb{Q}$ with α_ν algebraic integers. For each ν we fix some $f_\nu(X) \in \mathbb{Z}[X]$ of minimal degree with $f_\nu(\alpha_\nu) = 0$ and let ψ_ν be the L_σ-sentence introduced above for $p = f_\nu$ and $\mathcal{C}$ the conjugacy class of $\sigma|_{\mathbb{Q}(\alpha_\nu)}$ in $\mathrm{Gal}(\mathbb{Q}(\alpha_\nu)/\mathbb{Q})$. We define

$$a(f_\nu) := \Big\{ p \in \mathcal{P}(\mathbb{Q}) \ \Big|\ \sigma|_{\mathbb{Q}(\alpha_\nu)} \in \Big(\frac{\mathbb{Q}(\alpha_\nu)/\mathbb{Q}}{p}\Big) \Big\}$$

and content that

$$\mathcal{V} = \ \big\{ a(f_\nu) \ \big|\ \nu \in \mathbb{N} \big\} \cup \mathrm{Cofin}(\mathcal{P}(\mathbb{Q}))$$

has the finite intersection property, where $\mathrm{Cofin}(\mathcal{P}(\mathbb{Q}))$ denotes the Frechet filter on $\mathcal{P}(\mathbb{Q})$. Indeed, $a(f_\nu) \subseteq a(f_\mu)$ whenever $\mu \leq \nu$ and as $a(f_\nu) = P_{\mathbb{Q}(\alpha_\nu)/\mathbb{Q}}(\sigma|_{\mathbb{Q}(\alpha_\nu)})$ for all ν, each of the $a(f_\nu)$ is infinite by the Cebotarev Density Theorem.

Now choose any ultrafilter $\mathcal{U}$ containing $\mathcal{V}$. We claim that the ultraproduct

$$(\mathcal{K}, \tau) = \prod_{p\in\mathcal{P}(\mathbb{Q})} (\mathbb{F}_p^{\mathrm{alg}}, \phi_p)/\mathcal{U}$$

is elementarily equivalent to (K, σ). To see this, consider one of the extensions $\mathbb{Q}(\alpha_\nu)/\mathbb{Q}$ and let $p \in a(f_\nu)$. Then p is unramified in $\mathbb{Q}(\alpha_\nu)/\mathbb{Q}$, and if $\mathfrak{P}$ extends p to $\mathbb{Q}(\alpha_\nu)$, then $\mathrm{Fr}_\mathfrak{P}$ is conjugate to σ. Thus

$$(\mathbb{Q}(\alpha_\nu), \mathrm{Fr}_\mathfrak{P}) \models \psi_\nu \ ,$$

which implies that in $(\mathbb{Q}(\alpha_\nu), \mathrm{Fr}_\mathfrak{P})$ the equation

$$m\, \mathrm{Fr}_\mathfrak{P}(\alpha_\nu) = \sum a_i \alpha_\nu^i$$

holds, with m and the a_i being the integers given by ψ_ν. As we have chosen α_ν to be an algebraic integer and because $\Phi_\mathfrak{P}(\mathrm{Fr}_\mathfrak{P}) = \phi_p$, we may take residues modulo $\mathfrak{P}$ and conclude that

$$\bar{m}\, \phi_p(\overline{\alpha_\nu}) = \sum \overline{a_i}\ \overline{\alpha_\nu}^i$$

is true in the difference field $\big(\mathbb{Q}(\alpha_\nu)(\mathfrak{P}), \phi_p\big)$, which is of course a sub-difference field of $(\mathbb{F}_p^{\mathrm{alg}}, \phi_p)$. This shows that $(\mathbb{F}_p^{\mathrm{alg}}, \phi_p) \models \psi_\nu$ for $\mathcal{U}$-many $p \in \mathcal{P}(\mathbb{Q})$, so

$$(\mathcal{K}, \tau) \models \psi_\nu \ .$$

We have shown that for all ν there are automorphisms φ of $\mathbb{Q}(\alpha_\nu)$ such that $\sigma|_{\mathbb{Q}(\alpha_\nu)} = \varphi^{-1} \circ \tau|_{\mathbb{Q}(\alpha_\nu)} \circ \varphi$. Of course there are only finitely many because $\mathbb{Q}(\alpha_\nu)$ is a finite extension of $\mathbb{Q}$. Ordering all these automorphisms by inclusion we obtain a countable tree that is finitely branched. So there is an infinite branch by König's lemma. The union over such a branch is an automorphism $\varphi \in \mathrm{Aut}(\mathbb{Q}^{\mathrm{alg}})$ with the property that $\varphi\,\sigma|_{\mathbb{Q}^{\mathrm{alg}}} = \tau|_{\mathbb{Q}^{\mathrm{alg}}}\,\varphi$. Hence $(\mathcal{K}, \tau) \equiv (K, \sigma)$ by corollary (4.11.1). □

We end this section with the following remark from [**28**].

Remark 4.23 (Hrushovski). *Let (Ω, σ) be a model of $ACFA$ of characteristic zero. Then Ω has infinite transcendence degree. In positive characteristic, there are*[2] *$\sigma \in \mathrm{Gal}(\mathbb{F}_p)$ such that $(\mathbb{F}_p^{\mathrm{alg}}, \sigma) \models ACFA$.*

Proof. See section (13.3) of [**28**]. □

4.3. Prescribed Fixed Fields

As we have seen in proposition (4.16) (which is proposition (7.1) of [**15**]), if k is a pseudo-finite field, then there is some model of $ACFA$ whose fixed field is elementarily equivalent to k. The main result of the present chapter is the following theorem, stating that this elementary equivalence can be strengthened to identity.

Theorem 4.24. *Any difference field whose fixed field k is pseudo-finite embeds into a model (Ω, σ) of $ACFA$ such that $\mathrm{Fix}(\Omega, \sigma) = k$.*

Notice that by our convention any difference field is inversive. However, the theorem applies to non-inversive difference fields as well, as passing to the inversive closure does not change the fixed field (see section 1.4).

While in positive characteristic there are automorphisms σ of the algebraic closure $\mathbb{F}_p^{\mathrm{alg}}$ of the prime field such that $(\mathbb{F}_p^{\mathrm{alg}}, \sigma)$ is a model of $ACFA$, any model of $ACFA$ in characteristic zero has infinite transcendence degree, see remark (4.23). However there is an abundance of pseudo-finite subfields of $\mathbb{Q}^{\mathrm{alg}}$ (combine the Free Generators Theorem (18.5.6) from [**22**] and the PAC-Nullstellensatz (18.6.1) from [**22**]), and by our theorem any of them is the fixed field of a model of $ACFA$.

From the algebro-geometric point of view, the main ingredient in the proof of theorem (4.24) is corollary (4.28), stating that over an algebraically closed difference field (F, σ) whose fixed field k is pseudo-finite, every prime difference ideal admits a specialisation whose difference rational function field has fixed field k. In particular every maximal difference ideal over (F, σ) (resp. "closed point" on the difference variety) has this property.

[2] in fact Hrushovski shows in [**28**] that the set of $\sigma \in \mathrm{Gal}(\mathbb{F}_p)$ with $(\mathbb{F}_p^{\mathrm{alg}}, \sigma) \models ACFA$ is co-meager (with respect to the profinite topology on $\mathrm{Gal}(\mathbb{F}_p)$).

Given a difference field (F, σ) as in the statement of the theorem, we will accomplish a standard chain construction to construct an existentially closed difference field extension of (F, σ) having fixed field k. The first step is to reduce to algebraically closed difference fields (corollary (4.26)).

LEMMA 4.25. *Any difference field (F, σ) whose fixed field k has procyclic absolute Galois group admits an extension $(F^{\mathrm{sep}}, \bar{\sigma})$ such that*

$$\mathrm{Fix}(F^{\mathrm{sep}}, \bar{\sigma}) = k \ .$$

Proof. Let $L = F \cap k^{\mathrm{sep}}$ be the elements of F separably algebraic over k. Since k has procyclic absolute Galois group, any element $x \in L$, which generates the unique (in k^{sep}) algebraic extension of k of degree $[k[x] : k]$, is mapped into L by all automorphisms of k^{sep} over k. Therefore L is invariant under $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. As σ transforms algebraic elements into algebraic ones, it restricts to an automorphism of L with fixed field k. Thus L/k is Galois and $\sigma|_L$ generates $\mathrm{Gal}(L/k)$.

Now $\sigma|_L$ extends to a topological generator τ of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ because $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ is procyclic and $\mathrm{res} : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathrm{Gal}(L/k)$ is surjective.

Of course k^{sep}/L is a Galois extension and thus by choice of L, F and k^{sep} are linearly disjoint over L. So as σ and τ agree on L we can find a (unique) automorphism of Fk^{sep} extending σ and τ. We lift it to an automorphism $\bar{\sigma} \in \mathrm{Aut}(F^{\mathrm{sep}})$ and claim that $\mathrm{Fix}(F^{\mathrm{sep}}, \bar{\sigma}) = \mathrm{Fix}(F, \sigma) = k$. To see this, note first that $\mathrm{Fix}(F^{\mathrm{sep}}, \overline{\sigma}) \subset \mathrm{Fix}(F, \sigma)^{\mathrm{sep}}$. Indeed, let $p \in F[X]$ be the minimal polynomial of some $x \in \mathrm{Fix}(F^{\mathrm{sep}}, \bar{\sigma})$. Because $\bar{\sigma}(x) = x$, one calculates that[3] $p^{\sigma}(x) = p^{\sigma}(\bar{\sigma}(x)) = \bar{\sigma}(p(x)) = 0$, which implies $p = p^{\sigma}$ and thus that all coefficients of p are contained in $\mathrm{Fix}(F, \sigma)$. Thus $x \in k^{\mathrm{sep}}$. Finally, as τ is a (topological) generator of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$, it follows that $x \in k$. □

COROLLARY 4.26. *Any difference field (F, σ) whose fixed field k is pseudo-finite admits an extension $(F^{\mathrm{alg}}, \bar{\sigma})$ such that*

$$\mathrm{Fix}(F^{\mathrm{alg}}, \bar{\sigma}) = k \ .$$

Proof. If (F, σ) is separably closed, then σ lifts uniquely to an automorphism $\bar{\sigma}$ of F^{alg}. One has that $\mathrm{Fix}(F^{\mathrm{alg}}, \bar{\sigma}) = \mathrm{Fix}(F, \sigma)^{\mathrm{perf}}$. □

The second step is to find to a given system of difference equations over F (in finitely many variables) a solution in a difference field extension which "does not increase the fixed field" (corollary (4.28)).

LEMMA 4.27. *Let (F, σ) be an algebraically closed difference field with pseudo-finite fixed field k. If V is a difference variety over F and there are $f, g \in F[V]_{\sigma}$, $g \neq 0$, with $\sigma(\frac{f}{g}) = \frac{f}{g}$, then there is $\lambda \in k$ such that*

$$V \ \cap \ V_{\sigma}(\, f(\bar{X}) - \lambda g(\bar{X})\,) \quad \neq \ \emptyset \ .$$

Here $f(\bar{X})$ and $g(\bar{X})$ denote representatives of f and g in $F[\bar{X}]_{\sigma}$.

[3] p^{σ} denotes the polynomial obtained by applying σ to the coefficients of p.

Proof. The difference variety V is a definable subset of some sufficiently saturated model (Ω, σ) of $ACFA$. Let us consider the formula with parameters from F

$$\varphi(z) = \exists \bar{x} \quad \bar{x} \in V \ \wedge \ f(\bar{x}) - z\, g(\bar{x}) = 0 \ \wedge \ \sigma(z) = z\,,$$

which defines a subset X of $\mathrm{Fix}(\Omega, \sigma)$. X is non-empty because we can embed the integral domain $F[V]_\sigma$ over F into (Ω, σ), and denoting the images of f and g under this embedding by a and b, our assumption implies that $\frac{a}{b} \in X$.

As X is a subset of $\mathrm{Fix}(\Omega, \sigma)$ and as F is dcl_σ-closed, the canonical parameter of X is in $k = F \cap \mathrm{Fix}(\Omega, \sigma)$. By proposition (4.16) (which is proposition (7.1) of [**15**]), X is definable in the pure field $\mathrm{Fix}(\Omega, \sigma)$. As any field automorphism of $\mathrm{Fix}(\Omega, \sigma)$ over k lifts to an automorphism of (Ω, σ) (remark (4.17)) it follows that X is definable in $\mathrm{Fix}(\Omega, \sigma)$ using parameters from k.

Now F is algebraically closed by assumption, so $\mathrm{Fix}(\Omega, \sigma)$ is a regular extension of k. Both k and $\mathrm{Fix}(\Omega, \sigma)$ being pseudo-finite, $\mathrm{Fix}(\Omega, \sigma)$ is an elementary extension of k. And because $X \neq \emptyset$, we conclude that there is some element in k satisfying φ. □

Recall that if $\wp$ is a prime difference ideal in a difference ring (R, σ) then a difference specialisation of $\wp$ is a prime difference ideal $\wp'$ in (R, σ) that contains $\wp$. By definition $\wp'$ is not the unit ideal.

Corollary 4.28. *If (F, σ) is an algebraically closed difference field with pseudo-finite fixed field k and $\wp$ is a prime difference ideal over (F, σ), then there is a difference specialisation $\wp'$ of $\wp$ such that k is the fixed field of* $\mathrm{Quot}(F[\bar{X}]_\sigma/\wp')$.

We will use corollary (4.28) in the form that under the above assumptions, $\mathrm{Fix}\big(\mathrm{Quot}(F[\bar{X}]_\sigma/\wp), \sigma\big) = k$ for all maximal prime difference ideals $\wp$ over (F, σ).

Proof. Choose a maximal prime difference ideal m containing $\wp$ and let (F', σ') denote the (non-inversive) difference field $\mathrm{Quot}(F[\bar{X}]_\sigma/m)$, as always endowed with its canonical endomorphism. Then $W := V_\sigma(m)$ is a difference variety over F with difference rational function field (F', σ'). As m is maximal, W is minimal over F: there is no non-empty σ-algebraic set over F that is strictly contained in W.

Now if $\frac{f}{g} \in F'$ is an element with $\sigma'(\frac{f}{g}) = \frac{f}{g}$, it follows by minimality of W and lemma (4.27) that $W \subset V_\sigma(\, f(\bar{X}) - \lambda g(\bar{X})\,)$ for some $\lambda \in k$. So $f(\bar{X}) - \lambda g(\bar{X}) \in m$ and therefore $\frac{f}{g} = \lambda \in k$. □

Stated in other words, the content of corollary (4.28) is that there is some (closed) difference subvariety of $V_\sigma(\wp)$ whose rational function field has fixed field k.

Proposition 4.29. *For any algebraically closed difference field (F, σ) with pseudo-finite fixed field k and any non-empty σ-algebraic set V over F there is an algebraically closed difference field extension $(L, \bar{\sigma})$ of (F, σ) such that $V(L) \neq \emptyset$ and* $\mathrm{Fix}(L, \bar{\sigma}) = k$.

Proof. As the σ-topology is noetherian, we may assume that V is irreducible over F. Also, by (4.28), we may assume that $F(V)_\sigma$ has fixed field k. Let (F', σ') denote the inversive closure of $F(V)_\sigma$. Given any difference field (M, τ) and its inversive closure (M', τ'), one has that $\mathrm{Fix}(M, \tau) = \mathrm{Fix}(M', \tau')$. So we conclude that $\mathrm{Fix}(F', \sigma') = k$.

Choosing any lift $\bar{\sigma}$ of σ to $L = F'^{\mathrm{alg}}$ we see that $\mathrm{Fix}(L, \bar{\sigma}) = k$ as well. Indeed, this was already shown in the proof of lemma (4.25): for any $a \in \mathrm{Fix}(L, \bar{\sigma})$, the minimal polynomial of a over F' is left fixed under σ. After embedding $(L, \bar{\sigma})$ over (F, σ) into a sufficiently saturated model of $ACFA$, we have that $V(L) \neq \emptyset$ and $\mathrm{Fix}(L, \bar{\sigma}) = k$ by construction. □

Proof of 4.24. Let (F, σ) be a difference field with pseudo-finite fixed field k. We are going to construct an existentially closed difference field extension of (F, σ) having k as fixed field. Again by corollary (4.26) we may assume that $F = F^{\mathrm{alg}}$.

By proposition (4.29) any consistent quantifier-free L_σ-formula with parameters from F can be realized in an algebraically closed difference field extension $(L, \bar{\sigma})$ of (F, σ) such that $\mathrm{Fix}(L, \bar{\sigma}) = k$. Now a standard chain argument gives an existentially closed difference field extension of (F, σ) with fixed field k. □

Corollary 4.30. *Every pseudo-finite field k is isomorphic to the fixed field of some model of $ACFA$.*

Proof. Choose any generator σ of the absolute Galois group of k and apply the theorem to the difference field $(k^{\mathrm{alg}}, \sigma)$. □

Remark 4.31. *Note that the proof gives in fact many models of $ACFA$ having k as fixed field. Because* $\mathrm{Gal}(k)$ *is abelian, any two of its generators σ give non-isomorphic difference fields $(k^{\mathrm{alg}}, \sigma)$, which in turn give models of $ACFA$ not elementarily equivalent over k^{alg} and having k as fixed field.*

We end this section by giving some variants of theorem (4.24). In positive characteristic p, we have more fixed fields coming in via the Frobenius automorphism ϕ_p. Let $n \in \mathbb{Z}$ and consider the fixed field $\mathrm{Fix}(\Omega, \sigma\phi_p^n)$ of the model (Ω, σ) of $ACFA$. Then all definable subsets of $\mathrm{Fix}(\Omega, \sigma\phi_p^n)$ are definable in the pure field $\mathrm{Fix}(\Omega, \sigma\phi_p^n)$ (see (4.16), which is proposition (7.1) from [**15**]). Our proof actually shows the following.

Theorem 4.32. *Let (F, σ) be a difference field of characteristic $p > 0$ and $n \in \mathbb{Z}$. Assume that $\sigma\phi_p^n$ is an endomorphism of F such that the fixed field $k = \mathrm{Fix}(F, \sigma\phi_p^n)$ is pseudo-finite. Then (F, σ) embeds into some model (Ω, σ) of $ACFA$ such that* $\mathrm{Fix}(\Omega, \sigma\phi_p^n) = k$.

Note that if $n < 0$, the condition that $\sigma\phi_p^n$ is an endomorphism of F forces F to be perfect, as our difference fields are inversive.

Proof. We denote $\tau = \sigma\phi_p^n$. First we may assume that (F, τ) is inversive. Then by theorem (4.24), (F, τ) extends to some model (Ω, τ) of $ACFA$

whose fixed field is k. Putting $\bar{\sigma} = \tau\phi_p^{-n}$ we obtain a model $(\Omega, \bar{\sigma})$ of $ACFA$ containing (F, σ) as a subdifference field, and with $\mathrm{Fix}(\Omega, \bar{\sigma}\phi_p^n) = k$. □

We also obtain the following variant of Theorem (4.24), which has been pointed out to us and proved independently by Zoé Chatzidakis (unpublished).

THEOREM 4.33. *Let (F, σ) be an algebraically closed difference field of positive characteristic p and $\Sigma \subseteq \mathbb{Z}$ be a set of integers such that for all $n \in \Sigma$ the fixed field $\mathrm{Fix}(F, \sigma\phi_p^n)$ is pseudo-finite. Then there is some model (Ω, σ) of $ACFA$ such that for all $n \in \Sigma$,*

$$\mathrm{Fix}(\Omega, \sigma\phi_p^n) = \mathrm{Fix}(F, \sigma\phi_p^n) \ .$$

Sketch of Proof of Theorem (4.33). Giving a strict proof would mean repeating the above arguments almost literally. Instead we indicate how to adjust the proof of theorem (4.24) to show the following statement. It is the analogue of proposition (4.29) and so ensures that we can construct the desired model of $ACFA$ by the same chain argument as in (4.24):

For any algebraically closed difference field (F, σ) with $k_n = \mathrm{Fix}(F, \sigma\phi_p^n)$ pseudo-finite for $n \in \Sigma$ and any non-empty σ-algebraic set V over F there is an algebraically closed difference field extension $(L, \bar{\sigma})$ of (F, σ) such that $V(L) \neq \emptyset$ and $\mathrm{Fix}(L, \bar{\sigma}\phi_p^n) = k_n$ for all $n \in \Sigma$.

First we choose a maximal prime difference ideal m over (F, σ) containing $I_\sigma(V)$ and let $W = V_\sigma(m)$. $F(W)_\sigma$ might be non-perfect. But if we show that $f \in k_n$ for all $f \in F(W)_\sigma$ with $\sigma\phi_p^n(f) = f$, then the same is true for the elements of $F(W)_\sigma^{\mathrm{perf}}$ because k_n is perfect (and $\sigma\phi_p^n$ is a field automorphism of $F(W)_\sigma^{\mathrm{perf}}$). So let $f, g \in F[W]_\sigma$ with $g \neq 0$ and $\sigma\phi_p^n(\frac{f}{g}) = \frac{f}{g}$. If we consider in lemma (4.27) the formula

$$\varphi_n(z) = \exists \bar{x} \quad \bar{x} \in V \ \wedge \ f(\bar{x}) - z\, g(\bar{x}) = 0 \ \wedge \ \sigma\phi_p^n(z) = z \,,$$

then the proof of lemma (4.27) shows that

$$W \ \cap \ V_\sigma(\, f(\bar{X}) - \lambda g(\bar{X})\,) \quad \neq \ \emptyset$$

for some $\lambda \in k_n$. So by minimality of W it follows that $\mathrm{Fix}(F', \sigma\phi_p^n) = k_n$ for all $n \in \Sigma$, where F' denotes the perfect closure of $F(W)_\sigma$. Finally, for any lift $\bar{\sigma}$ of σ to $L := F'^{\mathrm{alg}}$ one has that $V(L) \neq \emptyset$, and that $\bar{\sigma}\phi_p^n$ lifts $\sigma\phi_p^n$. So as in the proof of proposition (4.29) we conclude that $\mathrm{Fix}(L, \sigma\phi_p^n) = k_n$ for all $n \in \Sigma$. □

4.4. Fractional Powers of the Frobenius

Let $n, m \in \mathbb{Z}$ with $n \neq 0$ and recall that ϕ_p denotes the Frobenius map in positive characteristic p and the identity in characteristic zero. For a difference field (K, σ), we write $\mathcal{F}_{n,m}(K) = \mathrm{Fix}(K, \sigma^n\phi_p^m)$ and denote by

$$(\mathcal{F}_{n,m}(K), \sigma)$$

the difference field consisting of $\mathcal{F}_{n,m}(K)$ together with the restriction of the automorphism of (K, σ). If (Ω, σ) is a model of $ACFA$ then $(\mathcal{F}_{n,m}(\Omega), \sigma)$ is a subdifference field of (Ω, σ) whose underlying field is pseudo-finite (see

proposition (4.16), which is proposition (7.1) from [**15**])). In view of theorem (4.24) it is natural to ask whether given a difference field (k,σ) which is elementarily equivalent to a difference field $(\mathcal{F}_{n,m}(\Omega),\sigma)$, for some model (Ω,σ) of $ACFA$, is there some model (K,σ) of $ACFA$ such that $(k,\sigma) = (\mathcal{F}_{n,m}(K),\sigma)$?

The next theorem answers this question positively.

THEOREM 4.34. *Let (k,σ) be a difference field and $n,m \in \mathbb{Z}$ with $n \neq 0$. If (k,σ) is elementarily equivalent to the difference field $(\mathcal{F}_{n,m}(\Omega),\sigma)$, for some model (Ω,σ) of $ACFA$, then there is some $(K,\sigma) \models ACFA$ such that*

$$(k,\sigma) = (\mathcal{F}_{n,m}(K),\sigma)\ .$$

Note that if the characteristic is zero, then theorem (4.34) is already covered by theorem (4.24), as the field $\mathrm{Fix}(k,\sigma)$ is definable in (k,σ) and k is a finite extension of $\mathrm{Fix}(k,\sigma)$ of degree n (see also below).

The proof of theorem (4.34) will use the theory $PSF_{(n,m,p)}$, which Ryten introduces in [**63**]. For coprime positive integers n,m with $n>1$ and a prime number p, $PSF_{(n,m,p)}$ axiomatises the class of those difference fields (F,σ) for which there is some model (Ω,σ) of $ACFA$ such that the difference subfield $\mathrm{Fix}(\Omega,\sigma^n\phi_p^m)$ is elementarily equivalent to (F,σ). Actually we will only need the results on $PSF_{(n,m,p)}$ stated below in fact (4.36), which we cite from [**63**].

DEFINITION 4.35. *Let n,m be positive coprime integers with $n>1$ and p be a prime number. Then $PSF_{(n,m,p)}$ is the theory of difference fields (F,σ) given by the following axioms:*

1. *F is a pseudo-finite field of characteristic p.*
2. *σ is an automorphism of F with $\sigma^n\phi_p^m = id$.*
3. *Let $U = U(\bar{x})$ be a variety over F and $U^\sigma = U(\bar{y})$, with $\bar{x} = (x_{ij} \mid 1 \leq i \leq n, 1 \leq j \leq N)$ and $\bar{y} = (y_{ij} \mid 1 \leq i \leq n, 1 \leq j \leq N)$. Suppose $V \subseteq U \times U^\sigma$ is a variety over F containing the algebraic sets $V(y_{ij} - x_{i+1\,j})$ and $V(y_{nj}^{p^m} - x_{1j})$. Further suppose that V projects generically onto U and U^σ and suppose W is a proper F-algebraic subset of V. Then there is some $a \in V(F) \setminus W(F)$ such that $a = bc$ with $b \in U$, $b = (b_{ij} \mid 1 \leq i \leq n, 1 \leq j \leq N)$ and $c \in U^\sigma$, $c = (c_{ij} \mid 1 \leq i \leq n, 1 \leq j \leq N)$ and $b_{ij} = \sigma(c_{ij})$ for all i,j.*
4. *For any tower of finite extensions $F \subseteq K \subseteq L$ with (K,σ) an extension of (F,σ) such that $(F,\sigma) = (\mathcal{F}_{n,m}(K),\sigma)$ there is some extension of σ to L such that $(F,\sigma) = (\mathcal{F}_{n,m}(L),\sigma)$.*

FACT 4.36 (Ryten). *Let n,m be positive coprime integers with $n>1$ and p be a prime number.*

1. *If (Ω,σ) is a model of $ACFA$ of characteristic p, then $(\mathcal{F}_{n,m}(\Omega),\sigma)$ is a model of $PSF_{(n,m,p)}$.*
2. *Let $(F,\sigma) \models PSF_{(n,m,p)}$. Then there is some model (Ω,σ) of $ACFA$ such that $(F,\sigma) \equiv (\mathcal{F}_{n,m}(\Omega),\sigma)$.*

(3) *Let (Ω, σ) be a model of $ACFA$. Then any subset X of a cartesian power of $\mathcal{F}_{n,m}(\Omega)$ which is definable in (Ω, σ) using parameters is definable in the difference field $(\mathcal{F}_{n,m}(\Omega), \sigma)$ using parameters from $\mathcal{F}_{n,m}(\Omega)$.*
(4) *Let $(F, \sigma) \models PSF_{(n,m,p)}$. Then there is some $\bar{\sigma} \in \mathrm{Aut}(F^{\mathrm{alg}})$ such that $(F, \sigma) \subset (F^{\mathrm{alg}}, \bar{\sigma})$ and $(\mathcal{F}_{n,m}(F^{\mathrm{alg}}), \bar{\sigma}) = (F, \sigma)$.*

Proof. For a proof of (1) see lemma (3.3.5) of [**63**], for (2) see theorem (3.3.15) of [**63**], (3) is lemma (3.3.22) of [**63**] and (4) is lemma (3.3.6) of [**63**]. □

Now in order to prove theorem (4.34), we will first prove the following variant. Theorem (4.34) follows therefrom by fact (4.36.4).

THEOREM 4.37. *Let (F, σ) be an algebraically closed difference field of positive characteristic p and $D \subset \mathbb{N}_{>1} \times \mathbb{N}_{\geq 1}$ such that $(n, m) = 1$ for all $(n, m) \in D$. Assume that the difference field $(\mathcal{F}_{n,m}(F), \sigma)$ is a model of $PSF_{(n,m,p)}$ for all $(n, m) \in D$. Then (F, σ) extends to a model (Ω, σ) of $ACFA$ such that*

$$(\mathcal{F}_{n,m}(\Omega), \sigma) = (\mathcal{F}_{n,m}(F), \sigma)$$

for all $(n, m) \in D$.

Proof of theorem (4.37). The idea of proof of theorem (4.24) works in the present situation, and the precise proofs are (almost) literally the same. However, for the convenience of the reader, we sketch the proofs most of the times.

First, given a model (F, σ) of $PSF_{(n,m,p)}$, fact (4.36.4) allows us to pass to some difference field extension $(F^{\mathrm{alg}}, \bar{\sigma})$ without enlarging the difference field $(\mathcal{F}_{n,m}(F), \sigma)$. Second, we want to find a solution to a finite system of difference equations over $(F^{\mathrm{alg}}, \bar{\sigma})$ without increasing $(\mathcal{F}_{n,m}(F^{\mathrm{alg}}), \bar{\sigma})$. This is done in the next two lemmata.

LEMMA 4.38. *Let (Ω, σ) be a model of $ACFA$ and $(k, \sigma) \preccurlyeq (\mathcal{F}_{n,m}(\Omega), \sigma)$. Let X be a subset of some cartesian power of $\mathcal{F}_{n,m}(\Omega)$. If X is k-definable in (Ω, σ) then it is k-definable in the difference field $(\mathcal{F}_{n,m}(\Omega), \sigma)$.*

Proof. We may assume that (Ω, σ) is sufficiently saturated. By fact (4.36.3) X is definable in the difference field $(\mathcal{F}_{n,m}(\Omega), \sigma)$ using parameters.

Let α be an automorphism of $(\mathcal{F}_{n,m}(\Omega), \sigma)$ leaving k pointwise fixed. As $(k, \sigma) \preccurlyeq (\mathcal{F}_{n,m}(\Omega), \sigma)$, the underlying field extension $\mathcal{F}_{n,m}(\Omega)/k$ is elementary, and hence regular by corollary (4.5.3). So by lemma (1.18) we find an automorphism $\tilde{\alpha}$ of $\mathcal{F}_{n,m}(\Omega)^{\mathrm{alg}} = \mathcal{F}_{n,m}(\Omega) \cdot k^{\mathrm{alg}}$ extending both α and the identity on k^{alg}. Note that $\tilde{\alpha}|_{\mathcal{F}_{n,m}(\Omega)}$ commutes with σ because of the choice of α and $\tilde{\alpha}|_{k^{\mathrm{alg}}}$ commutes with σ because $\tilde{\alpha}$ is the identity on k^{alg}. Thus $\tilde{\alpha}$ commutes with σ on $\mathcal{F}_{n,m}(\Omega)^{\mathrm{alg}}$. As $\mathcal{F}_{n,m}(\Omega)^{\mathrm{alg}}$ is algebraically closed in the sense of $ACFA$, it follows that $\tilde{\alpha}$ is elementary in the sense of $ACFA$. Hence α lifts to an automorphism of (Ω, σ) because $(\mathcal{F}_{n,m}(\Omega), \sigma)$ is stably embedded. This shows that X is k-definable in $(\mathcal{F}_{n,m}(\Omega), \sigma)$. □

LEMMA 4.39. *Let (F,σ) be an algebraically closed difference field of characteristic $p>0$ and $D\subset \mathbb{N}_{>1}\times\mathbb{N}_{\geq 1}$ such that $(n,m)=1$ for all $(n,m)\in D$. Assume that the difference field $(\mathcal{F}_{n,m}(F),\sigma)$ is a model of $PSF_{(n,m,p)}$ for all $(n,m)\in D$, and that V is a difference variety over F. If there are $(n,m)\in D$ and $f,g\in F[V]_\sigma$, $g\neq 0$, with $\sigma^n\phi_p^m(\frac{f}{g})=\frac{f}{g}$, then there is $\lambda\in\mathcal{F}_{n,m}(F)$ such that*

$$V\ \cap\ V_\sigma(\,f(\bar{X})-\lambda g(\bar{X})\,)\quad\neq\ \emptyset\ .$$

Here $f(\bar{X})$ and $g(\bar{X})$ denote representatives of f and g in $F[\bar{X}]_\sigma$.

Sketch of Proof. As in the proof of lemma (4.27), the difference variety V is a definable subset of some sufficiently saturated model (Ω,σ) of $ACFA$. Assume there are $(n,m)\in D$ and $f,g\in F[V]_\sigma$, $g\neq 0$, with $\sigma^n\phi_p^m(\frac{f}{g})=\frac{f}{g}$, and consider the formula

$$\varphi_{n,m}(z)=\exists\bar{x}\quad \bar{x}\in V\ \wedge\ f(\bar{x})-z\,g(\bar{x})=0\ \wedge\ \sigma^n\phi_p^m(z)=z\ .$$

The subset $X_{n,m}$ of $\mathcal{F}_{n,m}(\Omega)$ defined by $\varphi_{n,m}(z)$ is non-empty as the integral domain $F[V]_\sigma$ can be embedded over (F,σ) into (Ω,σ), and then by our assumption the images a and b of f and g under this embedding satisfy $\frac{a}{b}\in X_{n,m}$. The canonical parameter of $X_{n,m}$ is in $F\cap\mathcal{F}_{n,m}(\Omega)=\mathcal{F}_{n,m}(F)$. So as $(\mathcal{F}_{n,m}(F),\sigma)\models PSF_{(n,m,p)}$, we have $(\mathcal{F}_{n,m}(F),\sigma)\preccurlyeq(\mathcal{F}_{n,m}(\Omega),\sigma)$, and hence lemma (4.38) implies that$X_{n,m}$ is definable in $(\mathcal{F}_{n,m}(\Omega),\sigma)$ using parameters from $\mathcal{F}_{n,m}(F)$. Now as $(\mathcal{F}_{n,m}(F),\sigma)\preccurlyeq(\mathcal{F}_{n,m}(\Omega),\sigma)$ and $X_{n,m}\neq\emptyset$, we conclude there is $\lambda\in\mathcal{F}_{n,m}(F)$ with $\lambda\in X_{n,m}$, which proves the lemma. □

The following corollary is the analogon to corollary (4.28) for the present context.

COROLLARY 4.40. *Let (F,σ) be an algebraically closed difference field of characteristic $p>0$ and $D\subset\mathbb{N}_{>1}\times\mathbb{N}_{\geq 1}$ such that $(n,m)=1$ for all $(n,m)\in D$. Assume that $(\mathcal{F}_{n,m}(F),\sigma)$ is a model of $PSF_{(n,m,p)}$ for all $(n,m)\in D$, and let $\wp\subset F[\bar{X}]_\sigma$ be a prime difference ideal over (F,σ). If $\wp'$ is a maximal prime difference ideal over (F,σ) containing $\wp$, then*

$$(\mathcal{F}_{n,m}(F),\sigma)=(\mathcal{F}_{n,m}(K),\sigma)\,,$$

where (K,σ) denotes the inversive closure of the quotient difference field $\mathrm{Quot}(F[\bar{X}]_\sigma/\wp')$.

Note that $\sigma^n\phi_p^m$ is an endomorphism of $\mathrm{Quot}(F[\bar{X}]_\sigma/\wp')$ by our assumption $m\geq 1$.

Proof. Let $\wp'\subset F[\bar{X}]_\sigma$ be a maximal prime difference ideal containing $\wp$, and consider the difference variety $W:=V_\sigma(\wp')$ over F. Denote (F',σ') the difference rational function field of W over F. As $\wp'$ is maximal, W is minimal over F. If $\frac{f}{g}\in F'$ is an element with $\sigma^n\phi_p^m(\frac{f}{g})=\frac{f}{g}$, it follows by minimality of W and lemma (4.39) that $W\subset V_\sigma(f(\bar{X})-\lambda g(\bar{X}))$ for some $\lambda\in\mathcal{F}_{n,m}(F)$. Hence $f(\bar{X})-\lambda g(\bar{X})\in\wp'$ and thus $\frac{f}{g}=\lambda\in\mathcal{F}_{n,m}(F)$.

The lemma follows now because $\mathcal{F}_{n,m}(L^{\text{inv}}) = \mathcal{F}_{n,m}(L)$ for any (non-inversive) difference field (L, σ). Indeed, if $\lambda \in L^{\text{inv}}$ with $\sigma^n \phi_p^m(\lambda) = \lambda$, then $\sigma^{kn}(\lambda) = a \in L$, for some $k \in \mathbb{N}$. But this shows $\lambda = \phi_p^{km}(a) \in L$. □

Collecting the above we obtain the following analogue of proposition (4.29), which allows us to carry out the same chain construction as before without increasing the fixed field.

PROPOSITION 4.41. *Let (F, σ) be an algebraically closed difference field of characteristic $p > 0$ and $D \subset \mathbb{N}_{>1} \times \mathbb{N}_{\geq 1}$ such that $(n, m) = 1$ for all $(n, m) \in D$. Assume that $(\mathcal{F}_{n,m}(F), \sigma) \models PSF_{(n,m,p)}$ for all $(n, m) \in D$. Then for any non-empty σ-algebraic set V over F there is an algebraically closed difference field extension $(L, \bar{\sigma})$ of (F, σ) such that $V(L) \neq \emptyset$ and*

$$(\mathcal{F}_{n,m}(L), \bar{\sigma}) = (\mathcal{F}_{n,m}(F), \sigma)$$

for all $(n, m) \in D$.

Sketch of Proof. We may assume that V is minimal (and hence also irreducible) over F. Then by corollary (4.40) we have

$$(\mathcal{F}_{n,m}(F(V)_\sigma), \sigma) = (\mathcal{F}_{n,m}(F), \sigma)$$

for all $(n, m) \in D$. As before, we choose any lift $\bar{\sigma}$ of σ to the algebraic closure L of $F(V)_\sigma^{\text{inv}}$. Then $\bar{\sigma}^n \phi_p^m$ lifts $\sigma^n \phi_p^m$, $V(L) \neq \emptyset$ and

$$(\mathcal{F}_{n,m}(L), \bar{\sigma}) = (\mathcal{F}_{n,m}(F), \sigma)$$

for all $(n, m) \in D$. □

The last proposition enables us to carry out the standard chain construction to extend (F, σ) to a model of $ACFA$ without increasing any of the fixed fields $\text{Fix}(F, \sigma^n \phi_p^m)$, for all $(n, m) \in D$ simultaneously. This finishes the proof of theorem (4.37). □

Proof of theorem (4.34). Let (k, σ) be a difference field elementarily equivalent to $(\mathcal{F}_{n,m}(\Omega), \sigma)$, for some model (Ω, σ) of $ACFA$ and some integers n and m with $n \neq 0$. We are going to show that there is some model (K, σ) of $ACFA$ such that $(k, \sigma) = (\mathcal{F}_{n,m}(K), \sigma)$. Clearly we may assume that $n \geq 1$, for otherwise we work in the model (Ω, σ^{-1}) of $ACFA$.

First look at the case $m = 0$. In that case, the theorem follows quite easily from theorem (4.24): because $(k, \sigma) \equiv (\mathcal{F}_{n,0}(\Omega), \sigma)$, we have that $\text{Fix}(k, \sigma)$ is a pseudo-finite field, so (k, σ) extends to some model (K, σ) of $ACFA$ such that $\text{Fix}(k, \sigma) = \text{Fix}(K, \sigma)$ by theorem (4.24). In any model of $ACFA$, the fixed field of σ^n is the unique extension of degree n of the fixed field of σ, and hence k has degree n over $\text{Fix}(k, \sigma)$ again because $(k, \sigma) \equiv (\mathcal{F}_{n,0}(\Omega), \sigma)$. It follows that $(k, \sigma) = (\mathcal{F}_{n,0}(K), \sigma)$.

This proves the theorem for characteristic zero, and for positive characteristic and $m = 0$. So let us now assume that the characteristic p is positive and $m \neq 0$. In that case, the same argument as above will allow us to derive the theorem from theorem (4.37).

We may assume that $m \geq 1$, for if $m \leq -1$, note that $\sigma^n \phi_p^m = (\sigma^{-n}\phi_p^{-m})^{-1}$ and pass to (Ω, σ^{-1}). Theorem (4.32) deals with the case $n = 1$,[4] so we may assume that $m \geq 1$ and $n > 1$.

Now let d be the greatest common divisor of n and m and write $n' = n/d$ and $m' = m/d$. The field $\mathcal{F}_{n',m'}(\Omega)$ is pseudo-finite by proposition (4.16) and $\mathcal{F}_{n,m}(\Omega)$ is a finite extension of $\mathcal{F}_{n',m'}(\Omega)$ of degree d. Clearly the difference field $(\mathcal{F}_{n',m'}(\Omega), \sigma)$ is definable in $(\mathcal{F}_{n,m}(\Omega), \sigma)$ and is a model of $PSF_{n',m',p}$. Because (k, σ) is elementarily equivalent to $(\mathcal{F}_{n,m}(\Omega), \sigma)$ it follows that $\mathcal{F}_{n',m'}(k)$ is pseudo-finite, that k has degree d over $\mathcal{F}_{n',m'}(k)$, and that $(\mathcal{F}_{n',m'}(k), \sigma)$ is a model of $PSF_{n/d,m/d,p}$. As n' and m' are coprime, theorem (4.37) implies that (k, σ) extends to some model (K, σ) of $ACFA$ such that $\mathcal{F}_{n',m'}(K), \sigma) = \mathcal{F}_{n',m'}(k), \sigma)$. As $(\mathcal{F}_{n,m}(K), \sigma)$ is the unique degree d extension of $\mathcal{F}_{n',m'}(K), \sigma)$ inside K, we have $(\mathcal{F}_{n,m}(K), \sigma) = (k, \sigma)$. □

[4]We did not have to take the automorphism to the data because σ is definable in the pure field $\mathrm{Fix}(\Omega, \sigma\phi_p^m)$, as it is a power of the Frobenius there.

CHAPTER 5

Generic Automorphisms of Stable Theories

The question whether any pseudo-finite field is the fixed field of a generic automorphism could be answered positively in the previous chapter. Yet there are more theories of fields which admit generic automorphisms. For example, the theory of differential fields in characteristic zero, where the fixed differential field of a generic automorphism is a pseudo-finite pseudo-differentially closed differential field, as well as the theory of separably closed fields of given Ershov invariant e, where the fixed field is a one-free PAC field of Ershov invariant e. So the same question demands an answer in these contexts, and as turned out, the answer in each case is also positive. More even, roughly the same idea as in theorem (4.24) proves to be successful in the above cases.

The aim of the present chapter is to give a uniform proof of an analogue of theorem (4.24) for all the aforementioned theories of fields. This requires us to generalise the special setting of fields and pass to stable theories with a generic automorphism.

To be more precise, the context we work in is the following. We let T be a countable complete stable theory with quantifier elimination and elimination of imaginaries in the language L and let σ be a new unary function symbol. We denote $L_\sigma = L \cup \{\sigma\}$ and $T_\sigma = T \cup \{\text{“}\sigma \text{ is an } L\text{-automorphism”}\}$. A model (M, σ) of T_σ is called generic, and σ is called a generic automorphism of T, if it is existentially closed among models of T_σ. We assume that the generic automorphisms of T form an elementary class, axiomatised by the theory TA, and assume that TA eliminates imaginaries. $\mathrm{acl_T}$ and $\mathrm{dcl_T}$ denote the algebraic and definable closure in the sense of T. In this setting, we prove

Theorem. *Let (M, σ) be a model of TA and $K \preccurlyeq_L \mathrm{Fix}(M, \sigma)$ be an L-elementary substructure. If*

$$\mathrm{dcl_T}\big(\mathrm{acl_T}(K), \mathrm{Fix}(M, \sigma)\big) = \mathrm{acl_T}\big(\mathrm{Fix}(M, \sigma)\big)\,,$$

then there is some model $(N, \sigma) \equiv (M, \sigma)$ with $\mathrm{Fix}(N, \sigma) = K$.

Therefrom we deduce the aspired results on generic automorphisms of fields mentioned above.

The chapter is organised as follows. Section 5.1 recalls the basic model theory of TA from the literature, mainly from [**16**]. With this occasion, we introduce the concept inversive L_σ-structures, adapted from difference algebra. We develop the general theory of TA for arbitrary cardinalities of L. Also, we prove that TA eliminates imaginaries if it satisfies the Independence Theorem over algebraically closed sets. Section 5.2 deals with the

fixed structure of a generic automorphism and with the PAC property. We define the PAC property without requiring stability of the ambient theory and analyse the relation to the definitions that already exist in the literature. The fixed structure of a generic automorphism is PAC. Section 5.3 provides known examples of stable theories that admit generic automorphisms, whereby our main emphasis is placed on the stable theories of fields. Section 5.4 is concerned again with PAC structures in stable theories. The rest of the chapter does not depend on the main result of this section: We prove an analogue of the Elementary Equivalence Theorem for PAC fields, for one-free PAC substructures of models of a stable theory. In section 5.5 we introduce the notion of conservative embedding, which will play a key rôle in our construction of generic automorphisms with prescribed fixed structures later on. After discussing some examples we prove in proposition (5.63) that the fixed structures F of models (M, σ) of TA are conservatively embedded over any L-elementary substructure K with

$$\mathrm{dcl_T}(\mathrm{acl_T}(K), F) = \mathrm{acl_T}(F) \ .$$

The main results of this chapter are obtained in section 5.6. Given a sufficiently saturated model (M, σ) of TA, we give a complete characterisation of those L-elementary substructures K of the fixed structure of (M, σ) which occur itself as fixed structures of generic automorphisms. This is achieved in theorem (5.68). As turns out, those $K \preccurlyeq \mathrm{Fix}(M, \sigma)$ which occur as fixed structures of some $(N, \sigma) \models TA$ are precisely those over which $\mathrm{Fix}(M, \sigma)$ is conservatively embedded, and precisely those with

$$\mathrm{dcl_T}(\mathrm{acl_T}(K), F) = \mathrm{acl_T}(F) \ .$$

We also discuss some variants and corollaries. Finally we apply the results from the previous sections to various theories of fields with generic automorphism in section 5.7. In particular we prove that any pseudo-finite field is the fixed field of some generic difference field, that any one-free pseudo-differentially closed field of characteristic zero is the fixed differential field of some generic difference-differential field, and that any one-free PAC field of finite Ershov invariant is the fixed field of some generic separably closed difference field.

Notation and Conventions. We have to distinguish carefully between types, definable sets and so on in the sense of T on the one hand, and in the sense of TA on the other. So it is worthwhile setting notation and conventions for the present chapter at this point, even though some is a reminder from chapter 1.

When dealing with generic automorphisms, we let T denote a complete stable theory with infinite models and with quantifier elimination and elimination of imaginaries in the language L and let σ be a new unary function symbol. T might be many-sorted[1], but we talk nevertheless of the home sort of T. We denote $L_\sigma = L \cup \{\sigma\}$ and $T_\sigma = T \cup \{\text{“}\sigma \text{ is an } L\text{-automorphism”}\}$. A model (M, σ) of T_σ is called generic, and σ is called a generic automorphism

[1]In this case we strictly have to consider a tuple $\sigma = (\sigma_i)$ of automorphisms, one for each sort. For the sake of simple notation, we just don't.

of T, if it is existentially closed among models of T_σ. In what follows, we always assume that the class of generic models of T_σ forms an elementary class, or in other words that T_σ has a model companion. We call this model companion TA, and say that TA exists for short, or that T admits generic automorphisms.

$\mathfrak{C}$ denotes the monster model of T. $\mathrm{acl_T}$ and $\mathrm{dcl_T}$ denote algebraic and definable closure, $\mathrm{tp}_T(\bar{a}/A)$ the type of some (possibly infinite) tuple $\bar{a}$ over the parameter set A, all in the sense of T. For parameter sets $A \subset B \subset \mathfrak{C}$, $\mathrm{Aut}_T(B/A)$ is the set of elementary permutations of A in the sense of T and $\mathrm{Gal}(A)$ denotes $\mathrm{Aut}_T(\mathrm{acl_T}(A)/A)$, the absolute Galois group of A.

TA may not be complete. If (M, σ) is a model of TA and $A \subset M$, we denote by $\mathrm{acl}_\sigma(A)$ and $\mathrm{dcl}_\sigma(A)$ the algebraic and definable closure of A in (M, σ). We write $\mathrm{cl}_\sigma(A)$ for the closure of A under σ and σ^{-1}. For a possibly infinite tuple $\bar{a} \in M$, $\mathrm{tp}_\sigma(\bar{a}/A)$ denotes the (complete) type of a over A in (M, σ). All these depend on the model or the completion of TA chosen, however we use this simpler notation if it is clear from the context which model we are working in. Otherwise we will use the more precise though illegible notation $\mathrm{acl}_{(M,\sigma)}(A)$, $\mathrm{tp}_{(M,\sigma)}(a/A)$ and the like. Also, if (M, σ) is a model of T_σ, we abuse language and write (N, σ) for an extension of (M, σ).

In either case, if we say definable we always mean definable with parameters, unless we state to the contrary. Sets and parameter sets will be subsets of the monster model $\mathfrak{C}$ of T and parameter sets in the sense of T, unless stated otherwise. By saturation of $\mathfrak{C}$ it is clear that for any completion of TA there is some $\sigma \in \mathrm{Aut}(\mathfrak{C})$ such that $(\mathfrak{C}, \sigma)$ is a monster model of that completion of TA. So we sometimes say "we choose $\sigma \in \mathrm{Aut}_T(\mathfrak{C})$ such that $(\mathfrak{C}, \sigma) \models TA$" instead of saying "we choose a monster model $(\mathfrak{C}, \sigma)$ of TA".[2]

5.1. General Model Theory of TA

In this section we describe the general model theory of TA, for which [**16**] is our main reference. Before we do so we discuss the amalgamation property for partial automorphisms in stable theories and introduce inversive L_σ-structures. The language L need not be countable in this section, except at the end where we briefly discuss the question of existence of TA.

Amalgamation of Automorphisms (la PAPA). We first discuss la proprieté d'amalgamation des paires d'automorphismes, PAPA for short. It was introduced by Lascar in [**37**] and plays a particular rôle in the general model theory of TA. We use his modification from [**36**].

Definition 5.1. *Let L be an arbitrary language, and denote by L_σ the language obtained from L by adding a new unary function symbol σ. Let T be an L-theory and $\mathfrak{C}$ be the monster model of T. T is said to have the PAPA if the class of of L_σ-structures (A, σ), where A is an $\mathrm{acl_T}$-closed subset of $\mathfrak{C}$ and $\sigma \in \mathrm{Aut}_T(A)$, has the amalgamation property with respect*

[2] see also our convention concerning the monster model made in section 1.1

to L_σ-homomorphisms that are elementary in the sense of T. Explicitly: if A_0, A_1 and A_2 be $\mathrm{acl_T}$-closed subsets of $\mathfrak{C}$ and $\sigma_i \in \mathrm{Aut}_T(A_i)$ for $i = 0, 1, 2$, and if $f_1 : A_0 \longrightarrow A_1$ and $f_2 : A_0 \longrightarrow A_2$ are elementary maps such that $f_1\sigma_0 = \sigma_1 f_1$ and $f_2\sigma_0 = \sigma_2 f_2$, then there are $\mathrm{acl_T}$-closed $A_3 \subset \mathfrak{C}$ and $\sigma_3 \in \mathrm{Aut}_T(A_3)$, and elementary maps $g_1 : A_1 \longrightarrow A_3$ and $g_2 : A_2 \longrightarrow A_3$ with $g_1\sigma_1 = \sigma_3 g_1$ and $g_2\sigma_2 = \sigma_3 g_2$, such that $g_1 f_1 = g_2 f_2$.

LEMMA 5.2. *Let T be a stable L-theory. Let A be any parameter set and p and q be types over A at least one of which is stationary. Then for every partial elementary map σ whose domain contains A,*

$$\sigma(p \otimes_A q) = \sigma(p) \otimes_{\sigma(A)} \sigma(q) \ .$$

A word on the notation: the left hand side product of types $p \otimes_A q$ is taken in the type space over the parameter set A, the right hand side product $\sigma(p) \otimes_{\sigma(A)} \sigma(q)$ in the type space over the parameter set $\sigma(A)$.

Proof. Say p is stationary. Then $\sigma(p)$ is stationary, too, hence both products $p \otimes q$ and $\sigma(p) \otimes \sigma(q)$ are well-defined. If $(\bar{z}_1, \bar{z}_2)$ realises $\sigma(p \otimes q)$, then $(\sigma^{-1}(\bar{z}_1), \sigma^{-1}(\bar{z}_2))$ realises $p \otimes q$, which implies that $\sigma^{-1}(\bar{z}_1)$ realises p and $\sigma^{-1}(\bar{z}_2)$ realises q. So $\bar{z}_1 \models p$ and $\bar{z}_2 \models q$, hence $(\bar{z}_1, \bar{z}_2) \models \sigma(p) \otimes \sigma(q)$, which proves the claim. □

PROPOSITION 5.3 (Lascar). *Let T be a stable theory with elimination of imaginaries and quantifier elimination*[3]*. Let A_1, A_2 and A_3 be $\mathrm{acl_T}$-closed subsets of $\mathfrak{C}$ with $A_1 \subset A_2$ and $A_1 \subset A_3$, and let $\sigma_i \in \mathrm{Aut}_T(A_i)$ for $i = 1, 2, 3$ with $\sigma_2|_{A_1} = \sigma_1 = \sigma_3|_{A_1}$. If A_2 is independent from A_3 over A_1, then $\sigma_2 \cup \sigma_3$ is elementary (in the sense of T).*

Proof. This was proved by Lascar in [**36**]. As T is stable and A_1 is algebraically closed, both $p_2 := \mathrm{tp}(A_2/A_1)$ and $p_3 := \mathrm{tp}(A_3/A_1)$ are stationary by elimination of imaginaries. So using the previous lemma (5.2) we compute

$$\begin{aligned} \sigma_1(p_2 \otimes_{A_1} p_3) &= \sigma_1(p_2) \otimes_{\sigma_1(A_1)} \sigma_1(p_3) \\ &= \mathrm{tp}(\sigma_2(A_2)/\sigma_1(A_1)) \otimes_{\sigma_1(A_1)} \mathrm{tp}(\sigma_3(A_3)/\sigma(A_1)) \\ &= \mathrm{tp}(\sigma_2(A_2)\sigma_3(A_3)/\sigma_1(A_1)) \end{aligned}$$

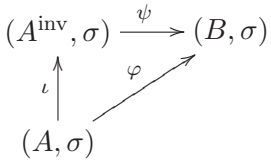
Hence $\sigma_2 \cup \sigma_3$ is elementary. □

COROLLARY 5.4 (Lascar). *"Stable theories have the $PAPA$"*
Let T be a stable L-theory with elimination of imaginaries and quantifier elimination. Then T has the $PAPA$.

Proof. We just have to note that if A_0, A_1, A_2 and $\sigma_0, \sigma_1, \sigma_2$ are as in definition (5.1), then as T is stable we can replace A_1 by an A_0-isomorphic copy A_1' such that $A_1' \underset{A_0}{\downarrow} A_2$ in the sense of T and, if $\psi : A_1 \longrightarrow A_1'$ is a (local) isomorphism over A_0, replace σ_1 by $\sigma_1' = \psi\sigma_1\psi^{-1}$. □

[3] if T does not eliminate quantifiers, one requires the inclusion maps $A_1 \subset A_2$ and $A_1 \subset A_3$ to be elementary.

We now introduce the concept of inversive L_σ-structure, which generalises the notion of inversive difference field in difference algebra. Consider an arbitrary language L, without fixing a specific theory T. We call an L_σ-structure (A, σ) inversive if σ is an automorphism of the L-structure A. Let (A, σ) be an L_σ-structure with σ an L-embedding of A into itself. We define the inversive closure of (A, σ) to be an inversive L_σ-structure (A^{inv}, σ) together with an L_σ-embedding $\iota : (A, \sigma) \longrightarrow (A^{\text{inv}}, \sigma)$ satisfying the following universal property: For any L_σ-homomorphism $\varphi : (A, \sigma) \longrightarrow (B, \sigma)$ with (B, σ) inversive there is a unique L_σ-morphism $\psi : (A^{\text{inv}}, \sigma) \longrightarrow (B, \sigma)$ such that $\varphi = \psi \circ \iota$.



LEMMA 5.5. *Any L_σ-structure (A, σ) with σ an L-embedding has an inversive closure (A^{inv}, σ). Moreover, $(A^{\text{inv}}, \sigma^{\text{inv}})$ is unique up to (unique) L_σ-isomorphism.*

Proof. The lemma is proved using an easy chain argument and the well-known fact that if $f : B \longrightarrow C$ is an L-embedding of L-structures, then there is an L-overstructure B^* of B and an L-isomorphism $f^* : B^* \longrightarrow C$ extending f. □

REMARK 5.6. *Note that if the L_σ-morphism $\varphi : (A, \sigma) \longrightarrow (B, \sigma)$ is an embedding, then so is $\psi : (A^{\text{inv}}, \sigma^{\text{inv}}) \longrightarrow (B, \sigma)$. In that case, we will often consider the inversive closure be embedded in (B, σ). For example if (B, σ) is a model of TA, then $A^{\text{inv}} = \text{cl}_\sigma(A)$ and σ^{inv} is the restriction of σ to A^{inv}.*

In this terminology, proposition (5.3) implies that if T is a stable L-theory with elimination of imaginaries and quantifier-elimination, then the class of inversive L_σ-structures (A, σ), with A an acl_{T}-closed L-substructure of the monster model $\mathfrak{C}$ of T, has the strong amalgamation property[4] with respect to L_σ-homomorphisms that are elementary in the sense of T. Note that we can also amalgamate infinitely many (A_i, σ_i). To be more precise, if $(A_i, \sigma_i)_{i<\lambda}$ is a family of algebraically closed inversive L_σ-structures, all containing (A, σ) and with the A_i pairwise independent over A, then $\bigcup_{i<\lambda} \sigma_i$ is elementary. We summarise this in the following corollary.

COROLLARY 5.7. *Let T be a stable L-theory with elimination of imaginaries and quantifier elimination[5] and monster model $\mathfrak{C}$. Let λ be any cardinal and $(A_i, \sigma_i)_{i<\lambda}$ be a sequence of inversive L_σ-structures, with each A_i an acl_{T}-closed subset of $\mathfrak{C}$. Assume for $i > 0$ we have L_σ-embeddings $f_i : (A_0, \sigma_0) \longrightarrow (A_i, \sigma_i)$. Then there is some inversive $(A_\lambda, \sigma_\lambda)$ with $A_\lambda \subset \mathfrak{C}$ acl_{T}-closed and L_σ-embeddings $g_i : (A_i, \sigma_i) \longrightarrow (A_\lambda, \sigma_\lambda)$ for all $i > 0$ such*

[4] recall that strong means that in definition (5.1), one requires additionally that $g_1(A_1) \cap g_2(A_2) = g_1 f_1(A_0)$.

[5] again, if we do not have quantifier elimination, we have to require all maps to be elementary in the sense of T.

that for any $i \neq j$: $g_i f_i(A_i) \cap g_j f_j(A_j) = g_i f_i(A_0)$ and $g_i f_i(A_i)$ is independent from $g_j f_j(A_j)$ over $g_i f_i(A_0)$ in the sense of T.

Proof. Reasoning similar as in the proof of the last corollary, we may assume that the A_i are pairwise independent over A_0 in the sense of T. □

Basic Model Theory of TA. We now start our discussion of the model theory of TA. We let L be an arbitrary first-order language, possibly many-sorted, and T be a complete stable L-theory with infinite models. We assume that T has quantifier elimination and elimination of imaginaries in L. σ be a new unary function symbol[6]. We denote $L_\sigma = L \cup \{\sigma\}$ and $T_\sigma = T \cup \{\text{“}\sigma \text{ is an } L\text{-automorphism”}\}$. In general, a model of an arbitrary (not necessarily complete) theory is called generic if it is existentially closed among models of that theory. So a model (M, σ) of T_σ is called generic, and σ is called a generic automorphism of T, if it is existentially closed among models of T_σ. Clearly generic models of T_σ exist, because T_σ is an $\forall\exists$-theory due to quantifier elimination of T. We assume that the class of generic models of T_σ forms an elementary class, in other words that T_σ has a model companion. This model companion is called TA. To abbreviate we say that TA exists, or that T admits generic automorphisms.

Recall our convention that if (M, σ) is a model of TA and $A \subset M$, then $\mathrm{acl_T}$ and $\mathrm{dcl_T}$ denote the algebraic and definable closure of A in the L-structure M, whereas $\mathrm{acl}_\sigma(A)$ and $\mathrm{dcl}_\sigma(A)$ denote the algebraic and definable closure of A in the L_σ-structure (M, σ), respectively. Further, we write $\mathrm{cl}_\sigma(A)$ for the closure of A under σ and σ^{-1}.

Let (M, σ) be a model of TA (or of T_σ even). If $A \subset M$ is an $\mathrm{acl_T}$-closed subset with $\sigma(A) \subseteq A$, then A is obviously an L_σ-substructure of (M, σ) in a natural way. In particular, if we start with an L_σ-substructure (A, σ) then $\mathrm{acl_T}(A)$ will naturally be an L_σ-structure, because σ is an L-automorphism.

Theorem 5.8 (Chatzidakis-Pillay). *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries such that TA exists.*

If (M_1, σ_1) and (M_2, σ_2) are models of TA containing a common L_σ-substructure (A, σ) then putting $\sigma_i' = \sigma_i|_{\mathrm{acl_T}(A)}$ we have

$$(M_1, \sigma_1) \equiv_A (M_2, \sigma_2) \quad \textit{iff} \quad (\mathrm{acl_T}(A), \sigma_1') \cong_A (\mathrm{acl_T}(A), \sigma_2').$$

Note that the $(\mathrm{acl_T}(A), \sigma_i')$ are not necessarily inversive.

Proof. This was proved by Chatzidakis and Pillay in [**16**], proposition (3.5).

If $(M_1, \sigma_1) \equiv_A (M_2, \sigma_2)$ we can choose a common elementary extension (M_3, σ_3). Then clearly $(\mathrm{acl_T}(A), \sigma_1) \cong (\mathrm{acl_T}(A), \sigma_3) \cong (\mathrm{acl_T}(A), \sigma_2)$, the isomorphisms being over A.

For the converse, let $\varphi_1 : (\mathrm{acl_T}(A), \sigma_1') \longrightarrow (\mathrm{acl_T}(A), \sigma_2')$ be an L_σ-isomorphism over A. σ_1' and σ_2' are elementary maps in the sense of T, so

[6]We note again that strictly speaking we have to consider a tuple $\sigma = (\sigma_i)$ of automorphisms, one for each sort of L. For the sake of simple notation, we just don't.

by quantifier elimination of T they are L-embeddings of $\mathrm{acl_T}(A)$ into itself. Hence by lemma (5.5) φ_1 lifts to an L_σ-isomorphism

$$\varphi_2 : \mathrm{cl}_{\sigma_1}(\mathrm{acl_T}(A)), \sigma_1'') \longrightarrow \mathrm{cl}_{\sigma_2}(\mathrm{acl_T}(A)), \sigma_2'')$$

of the inversive closures (here we write σ_i'' for $\sigma_i|_{\mathrm{cl}_{\sigma_i}(\mathrm{acl_T}(A))}$). As $\sigma(A) \subseteq A$ and the σ_i are L-automorphisms it follows that

$$\mathrm{cl}_{\sigma_i}(\mathrm{acl_T}(A)) = \mathrm{acl_T}(\mathrm{cl}_{\sigma_i}(A)) \ (i = 1, 2) \ .$$

Thus $A_i := \mathrm{cl}_{\sigma_i}(\mathrm{acl_T}(A))$ are $\mathrm{acl_T}$-closed and (A_i, σ_i) are inversive. We identify them and apply proposition (5.3) to see that $\sigma_1 \cup \sigma_2$ is elementary. It extends to some $(M, \sigma) \models T_\sigma$, which in turn extends to some model (M_3, σ_3) of TA, the model companion of T_σ. Model completeness of TA implies that (M_3, σ_3) is an elementary extension of both (M_1, σ_1) and (M_2, σ_2). The embeddings are the identity on A, so $(M_1, \sigma_1) \equiv_A (M_2, \sigma_2)$. □

The following immediate consequence will prove useful later on, so we state it in a remark for future reference.

Remark 5.9. *Under the assumptions as in theorem (5.8), any bijection between* acl_σ*-closed sets that is elementary in the sense of* T *and commutes with* σ *is elementary in the sense of* TA*.*

Corollary 5.10 (Chatzidakis-Pillay). *Let* T *be a stable* L*-theory with quantifier elimination and elimination of imaginaries such that* TA *exists. Then* $TA \cup \mathrm{qfdiag}((A, \sigma))$ *is complete for any* $A = \mathrm{acl_T}(A)$ *and* $\sigma \in \mathrm{Aut}_T(A)$*. In particular the completions of* TA *are classified by the isomorphism type of the* L_σ*-structure* $(\mathrm{acl_T}(\emptyset), \sigma)$*.*

Proof. Immediate from theorem (5.8). □

Let us note aside that one does not have to use parameters to describe the isomorphism type of $(\mathrm{acl_T}(\emptyset), \sigma|_{\mathrm{acl_T}(\emptyset)})$. See remark (5.17) for an explanation.

Corollary 5.11 (Chatzidakis-Pillay). *Let* T *be a stable* L*-theory with quantifier elimination and elimination of imaginaries such that* TA *exists. Let* A *be an* L_σ*-substructure of the two models* (M_1, σ_1) *and* (M_2, σ_2) *of* TA*. If* $\bar{a} \in M_1$ *and* $\bar{b} \in M_2$*, then*

$$\mathrm{tp}_{(M_1, \sigma_1)}(\bar{a}/A) = \mathrm{tp}_{(M_2, \sigma_2)}(\bar{b}/A)$$

if and only if there is an isomorphism of L_σ*-structures*

$$\mathrm{acl}_{(M_1, \sigma_1)}(A\bar{a}) \longrightarrow \mathrm{acl}_{(M_2, \sigma_2)}(A\bar{b})$$

over A *which maps* $\bar{a}$ *to* $\bar{b}$*. Here* $\mathrm{acl}_{(M_1, \sigma_1)}(A\bar{a})$ *is endowed with the restriction of* σ_1 *and* $\mathrm{acl}_{(M_2, \sigma_2)}(A\bar{a})$ *with the restriction of* σ_2*.*

Proof. This is just a special instance of theorem (5.8). □

Corollary 5.12 (Chatzidakis-Pillay). *Let* T *be a stable* L*-theory with quantifier elimination and elimination of imaginaries such that* TA *exists. Let* A *be a subset of some model of* TA*. Then*

$$\mathrm{acl}_\sigma(A) = \mathrm{acl_T}(\mathrm{cl}_\sigma(A)) \ .$$

Proof. The corollary was proved by Chatzidakis and Pillay in [**16**]. The proof we give here is motivated by a standard argument for fields (see for example the proof of (4.5.4)).

Let $\sigma \in \mathrm{Aut}_T(\mathfrak{C})$ such that $(\mathfrak{C}, \sigma) \models TA$. Let $A = \mathrm{acl_T}(\mathrm{cl}_\sigma(A))$ and assume $a \notin A$. We are going to show that $a \notin \mathrm{acl}_\sigma(A)$.

Note that σ restricts to an automorphism of A, because it restricts to an automorphism of $\mathrm{cl}_\sigma(A)$ and hence of $\mathrm{acl_T}(\mathrm{cl}_\sigma(A))$, since σ is an L-automorphism. So $(A, \sigma|_A)$ is an inversive $\mathrm{acl_T}$-closed L_σ-structure and $TA \cup \mathrm{qfdiag}(A, \sigma|_A)$ is complete by (5.10).

Put $A_1 = \mathrm{acl}_\sigma(A, a)$ and $\sigma_1 = \sigma|_{A_0}$. Note that because A_1 is acl_σ-closed, it is $\mathrm{acl_T}$-closed and (A_1, σ_1) is inversive. Consider now the sequence $(A_i, \sigma_i)_{i<\omega}$ with $(A_0, \sigma_0) = (A, \sigma|_A)$ and $(A_i, \sigma_i) = (A_1, \sigma_1)$ for $i > 0$. By corollary (5.7) we find an inversive $(A_\omega, \sigma_\omega)$ with $A_\omega = \mathrm{acl_T}(A_\omega) \subset \mathfrak{C}$ and L_σ-embeddings $g_i : (A_i, \sigma_i) \longrightarrow (A_\omega, \sigma_\omega)$ such that $g_i(A_i) \cap g_j(A_j) = A$ whenever $i \neq j$. In particular, if a_i denotes the image of a under g_i, the a_i are pairwise distinct. As in the proof of (5.8), $(A_\omega, \sigma_\omega)$ extends to some model (M, σ) of TA, which contains $(A, \sigma|_A)$ as a substructure by construction. So as $TA \cup \mathrm{qfdiag}(A, \sigma|_A)$ is complete, we can embed (M, σ) over A into $(\mathfrak{C}, \sigma)$. The images of the a_i under this embedding are then pairwise distinct realisations of $\mathrm{tp}_\sigma(a/A)$ by theorem (5.8), so $a \notin \mathrm{acl}_\sigma(A)$. □

The following remark will prove useful later on.

Remark 5.13. *With the same assumptions as in theorem (5.8), let (A, σ) be an L_σ-substructure of some model (M, σ) of TA. If A is* $\mathrm{acl_T}$*-closed, then A^{inv} is* acl_σ*-closed.*

Proof. The (underlying set of the) inversive closure of A in (M, σ) is $\mathrm{cl}_\sigma(A)$. As σ is an L-automorphism, we have as in the proof of theorem (5.8) that $\mathrm{cl}_\sigma(\mathrm{acl_T}(A)) = \mathrm{acl_T}(\mathrm{cl}_\sigma(A))$. So $A^{\mathrm{inv}} = \mathrm{acl}_\sigma(A)$ by corollary (5.12). □

By model completeness every L_σ-formula is modulo TA equivalent to an existential formula. The description of types in TA allows us to do even better. We aim to show a weak quantifier elimination result for TA, namely that modulo TA, any formula $\varphi(\bar{x})$ is equivalent to a finite disjunction of formulas of the form $\exists \bar{y}\ \theta(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^n(\bar{x}); \bar{y}, \sigma(\bar{y}), \ldots, \sigma^m(\bar{y}))$, where θ is a quantifier-free L-formula which implies that $(\bar{y}, \sigma(\bar{y}), \ldots, \sigma^m(\bar{y}))$ is algebraic over $\bar{x}, \sigma(\bar{x}), \ldots, \sigma^n(\bar{x})$ in the sense of T, see corollary (5.16).

Let A be a set of parameters (in the sense of T) and $\bar{x}$ be a (possibly infinite) tuple of variables. We let $\Sigma(\bar{x}/A)$ be the set of $L_\sigma(A)$-formulas of the form

$$\exists \bar{y}\ \theta\big(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^n(\bar{x}); \bar{y}, \sigma(\bar{y}), \ldots, \sigma^m(\bar{y}); \bar{a}, \sigma(\bar{a}), \ldots, \sigma^l(\bar{a})\big)$$

where $\bar{a} \in A$ and $\theta\big(\bar{x}_0, \ldots, \bar{x}_n; \bar{y}_0, \ldots, \bar{y}_m; \bar{z}_0, \ldots, \bar{z}_l\big)$ is a quantifier-free L-formula with the property that for all realisations

$$(\bar{d}_0, \ldots, \bar{d}_n; \bar{b}_0, \ldots, \bar{b}_m; \bar{c}_0, \ldots, \bar{c}_l)$$

of θ in models of T, $\bar{b}_0, \ldots, \bar{b}_m$ is algebraic over $\bar{d}_0, \ldots, \bar{d}_n, \bar{c}_0, \ldots, \bar{c}_l$ (in the sense of T). For a tuple $\bar{a}$ in some model $(M, \sigma) \models TA$ with $A \subset M$ let $\Sigma(\bar{a}/A)$ be the set of $\varphi \in \Sigma(\bar{x}/A)$ true of $\bar{a}$ in (M, σ). Note that we allow $\bar{a}$ to be the empty tuple. The information in $\Sigma(\bar{a}/A)$ is enough to determine the isomorphism type over A of $(\mathrm{acl}_\sigma(A, \bar{a}), \sigma)$, as we will see in the next lemma.

LEMMA 5.14. *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries such that TA exists.*

Let A be a common subset of the models (M_1, σ_1) and (M_2, σ_2) of TA. Let $\bar{a}$ and $\bar{b}$ be tuples in M_1 and M_2 respectively of the same length. If $\Sigma(\bar{a}/A) = \Sigma(\bar{b}/A)$, then $\mathrm{tp}_{(M_1,\sigma_1)}(\bar{a}/A) = \mathrm{tp}_{(M_2,\sigma_2)}(\bar{b}/A)$.

Note that since the language L as well as the set A might be uncountable, we cannot use König's lemma.

Proof. By corollary (5.11) we have to construct an L_σ-isomorphism over A from $\mathrm{acl}_\sigma(A\bar{a})$ onto $\mathrm{acl}_\sigma(A\bar{b})$ mapping $\bar{a}$ to $\bar{b}$.

Let A_1 and A_2 denote the L_σ-substructures generated by $A\bar{a}$ and $A\bar{b}$ in (M_1, σ_1) and (M_2, σ_2) respectively. The quantifier-free diagrams of A_1 and A_2 are contained in $\Sigma(\bar{a}/A) = \Sigma(\bar{b}/A)$, and coincide. So there is an L_σ-isomorphism $f : A_1 \longrightarrow A_2$ over A taking $\bar{a}$ to $\bar{b}$. Note that f is elementary in the sense of T by quantifier elimination.

Claim: f lifts to an elementary bijection $\bar{f}$ (in the sense of T) from $\mathrm{acl}_\mathrm{T}(A_1)$ onto $\mathrm{acl}_\mathrm{T}(A_2)$ such that $\bar{f}\sigma_1 = \sigma_2\bar{f}$.

Let us postpone for short the proof of the claim and assume it is true. Then we know that f extends to an L_σ-isomorphism between $\mathrm{acl}_\mathrm{T}(A_1)$ and $\mathrm{acl}_\mathrm{T}(A_2)$, the former endowed with the restriction of σ_1, the latter with the restriction of σ_2. By lemma (5.5) this isomorphism lifts to an isomorphism of the inversive closures, which are $\mathrm{acl}_\sigma(A\bar{a})$ and $\mathrm{acl}_\sigma(A\bar{b})$ respectively by remark (5.13) (of course both endowed with the corresponding restriction of σ_1 and σ_2). So when we have proved the claim we have also proved the lemma by corollary (5.11).

Proof of the Claim. To prove the claim we work entirely in T. Let M be a model of T containing the parameter sets A_1 and A_2. σ_1 and σ_2 are partial elementary selfmaps of $\mathrm{acl}_\mathrm{T}(A_1)$ and $\mathrm{acl}_\mathrm{T}(A_2)$ respectively (strictly speaking we replace σ_1 and σ_2 by their restrictions).

To get $\bar{f}$ we first define a (directed) inverse system $(M_S)_{S \in I}$ of partial elementary maps

$$\mathrm{acl}_\mathrm{T}(A_1) \xrightarrow{g} \mathrm{acl}_\mathrm{T}(A_2)$$

such that $g\sigma_1 = \sigma_2 g$. The index set I is the set of dcl_T-closed subsets $S \subset \mathrm{acl}_\mathrm{T}(A_1)$ of the form $S = \mathrm{dcl}_\mathrm{T}(A_1, \bar{s})$ for some finite tuple $\bar{s} \in \mathrm{acl}_\mathrm{T}(A_1)$. Putting $S_1 \leq S_2$ if and only if $S_1 \subseteq S_2$ we obtain a pre-ordering on I (by which we mean that $\leq$ is reflexive and transitive). Clearly $(I, \leq)$ is a directed pre-ordering: for $S_1, S_2 \in I$, choose finite tuples $\bar{s}_1$ and $\bar{s}_2$ such that $S_i = \mathrm{dcl}_\mathrm{T}(A_1, \bar{s}_i)$, and let $S_3 = \mathrm{dcl}_\mathrm{T}(A_1, \bar{s}_1, \bar{s}_2)$. Then $S_3 \in I$ with $S_1 \leq S_3$ and $S_2 \leq S_3$.

For $S \in I$ we define M_S to be the set of elementary maps

$$S \cup \sigma_1(S) \xrightarrow{g_S} \mathrm{acl_T}(A_2)$$

with the property that $g_S(\sigma_1(c)) = \sigma_2(g_S(c))$ for all $a \in S$. By our assumption that $\Sigma(\bar{a}/A) = \Sigma(\bar{b}/A)$, each M_S is non-empty. Further, any M_S is finite: choose a finite tuple $\bar{s} \in \mathrm{acl_T}(A_1)$ with $\mathrm{dcl_T}(A_1, \bar{s}) = S$, and let $\varphi(\bar{x}) \in L(A_1)$ isolate $\mathrm{tp}_T(\bar{s}/A_1)$. Then, as g_S is elementary, $g_S(\bar{s})$ realises $f\varphi(\bar{x})$ and $g_S(\sigma_1(\bar{s}))$ realises $f\sigma_1\varphi(\bar{x})$, and in fact g_S is determined by these realisations. As φ is algebraic and f and σ_1 elementary, there are only finitely many realisations of $f\varphi(\bar{x})$ and $f\sigma_1\varphi(\bar{x})$.

For $S_1 \leq S_2$ we let $\pi^{S_2}_{S_1} : M_{S_2} \longrightarrow M_{S_1}$ be the canonical restriction map. Endowing all M_S with the discrete topology, we obtain an inverse system of non-empty compact spaces, so the inverse limit

$$G = \varprojlim_{S \in I} M_S$$

is non-empty by theorem (3.6) of chapter VIII in [**20**]. We choose any $\bar{f} \in G$ and content that $\bar{f}$ is the promised extension of f.

Clearly $\bar{f}$ extends f as any element of A_1 is definable over A_1. To see that it is elementary (in the sense of T), let $\bar{s} \in \mathrm{acl_T}(A_1)$ be a finite tuple. Then $\bar{f}|_{S \cup \sigma_1(S)} = g_S$ for some $g_S \in M_S$, where $S = \mathrm{dcl_T}(A_1, \bar{s})$. So $\bar{f}$ is elementary. The same argument shows that $\bar{f}(\sigma_1(c)) = \sigma_2(\bar{f}(c))$ for all $c \in \mathrm{acl_T}(A_1)$. Finally, to show that $\bar{f}$ is surjective, let $d \in \mathrm{acl_T}(A_2)$ and $\varphi(x) \in L(A_2)$ isolate $\mathrm{tp}_T(d/A_2)$. Let $\bar{c} = c_0, \ldots, c_n$ be the set of realisations of $f^{-1}\varphi(x)$. Clearly $\bar{c} \in \mathrm{acl_T}(A_1)$, and $\bar{f}|_S = g_S|_S$ for some $g_S \in M_S$, where $S = \mathrm{dcl_T}(A_1, \bar{c})$. As g_S is elementary, there is some i with $g_S(c_i) = d$. Hence $\bar{f}$ is onto.

This proves the claim, and also the lemma. □

Remark 5.15. *Instead of inverse limits and theorem (3.6) of chapter VIII in [**20**] in the above proof we could have applied the following kind of Rado's Selection Lemma: Let $\mathcal{F}$ be a system of finite partial maps $A \longrightarrow B$, closed under restriction, such that for all finite $A_0 \subset A$ the set*

$$\{f \in \mathcal{F} \mid \mathrm{dom}(f) = A_0\}$$

is finite and non-empty. Then there is $F : A \longrightarrow B$ such that for all finite non-empty subsets $A_0 \subset A$ there is $f \in \mathcal{F}$ with $F|_{A_0} = f$.

Corollary 5.16 (Weak Quantifier Elimination). *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries such that TA exists. Then any L_σ-formula $\varphi(\bar{x})$ is modulo TA equivalent to a finite disjunction of formulas in $\Sigma(\bar{x}/\emptyset)$.*

Proof. In view of lemma (5.14), the statement is an example of the following more general principle: If τ is any theory and Δ some set of formulas (in the language of τ) closed under conjunction such that all types in τ are implied by some subset of Δ, then modulo τ every formula is equivalent to some finite disjunction of formulas in Δ. This is a consequence of compactness, and follows immediately from theorem (5.3) in [**56**]. We

just have to note that $\Sigma(\bar{x}/\emptyset)$ is closed under conjunction (up to equivalence, but this does no harm), so the corollary follows from lemma (5.14). □

REMARK 5.17. *We have already remarked that one does not need to use parameters in order to describe the action of σ on $\mathrm{acl_T}(\emptyset)$. This is indeed a special case of lemma (5.14), taking A to be the empty set and $\bar{a}$ to be the empty tuple.*

Independence Theorem and Simplicity.

DEFINITION 5.18. *Let $\sigma \in \mathrm{Aut}_T(\mathfrak{C})$ such that $(\mathfrak{C}, \sigma) \models TA$. For subsets A, B and C of $\mathfrak{C}$ we say that A is independent from C over B if and only if $\mathrm{acl}_\sigma(AB)$ is independent from $\mathrm{acl}_\sigma(CB)$ over $\mathrm{acl}_\sigma(B)$ in the sense of T.*

We will see (within the next few results) that this is non-forking independence, turning TA into a simple theory. We start with the following lemma, which is proved in [**16**], though it is not explicitly stated there.

LEMMA 5.19 (Chatzidakis-Pillay). *Let T be stable with elimination of imaginaries and M be a model of T. Let further A, B and C be $\mathrm{acl_T}$-closed sets containing M that are pairwise independent over M. Then $\mathrm{dcl_T}(BC)$ is $\mathrm{acl_T}$-closed in $\mathrm{dcl_T}(\mathrm{acl_T}(AB), \mathrm{acl_T}(AC))$.*

Proof. For convenience we repeat the proof from [**16**]. If $\lambda \in \mathrm{dcl_T}(\mathrm{acl_T}(AB), \mathrm{acl_T}(AC))$ is algebraic over BC we may choose tuples $\bar{a} \in A$, $\bar{b} \in B$, $\bar{c} \in C$, $\beta \in \mathrm{acl_T}(\bar{a}, \bar{b})$ and $\gamma \in \mathrm{acl_T}(\bar{a}, \bar{c})$ such that λ is definable over $\bar{b}\bar{c}\beta\gamma\bar{a}$, say by the L-formula $\varphi(x, \bar{b}, \bar{c}, \beta, \gamma, \bar{a})$. Further there are L-formulas $\psi_1(y_1, \bar{b}, \bar{a})$ and $\psi_2(y_2, \bar{c}, \bar{a})$ isolating $\mathrm{tp}_T(\beta/\bar{a}, \bar{b})$ and $\mathrm{tp}_T(\gamma/\bar{a}, \bar{c})$ respectively. Consider $p = \mathrm{tp}_T(\lambda, \bar{b}, \bar{c}/A)$. By the above, p represents the L-formula $\delta(x, \bar{x}_1, \bar{x}_2; \bar{z})$, where $\delta(x, \bar{x}_1, \bar{x}_2; \bar{z})$ implies that $\psi_1(y_1, \bar{x}_1, \bar{z})$ and $\psi_2(y_2, \bar{x}_2, \bar{z})$ are consistent formulas algebraic in y_1 and y_2 respectively, for all of whose realisations y_1 and y_2 respectively, the formula $\varphi(x, \bar{x}_1, \bar{x}_2, y_1, y_2, \bar{z})$ has exactly one realisation in x.

As $\mathrm{acl_T}(BC)$ is independent from A over M, p does not fork over M. So because M is a model of T and as T is stable, p is the heir of $p|_M$, so the latter represents the formula $\delta(x, \bar{x}_1, \bar{x}_2, \bar{z})$. In other words there is $\bar{a}' \in M$ such that $p|_M \models \delta(x, \bar{x}_1, \bar{x}_2; \bar{a}')$. It follows that there are $\beta' \models \psi_1(y_1, \bar{b}, \bar{a}')$ and $\gamma' \models \psi_2(y_2, \bar{c}, \bar{a}')$ such that λ is definable over $\bar{b}\bar{c}\beta'\gamma'\bar{a}'$. B and C are algebraically closed, so $\beta' \in B$ and $\gamma' \in C$, and hence $\lambda \in \mathrm{dcl_T}(BC)$. □

The following theorem is due to Chatzidakis and Pillay [**16**].

THEOREM 5.20 (Independence Theorem over models of T_σ). *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries such that TA exists. Let (M, σ) be a model of T_σ and A, $B \supset M$ be independent over M. Assume that $\bar{c}_1$ and $\bar{c}_2$ are tuples realising the same type over M with $\bar{c}_1$ independent from A over M and $\bar{c}_2$ independent from B over M. Then there is a tuple $\bar{c}$ independent from AB over M realising $\mathrm{tp}_\sigma(\bar{c}_1/A) \cup \mathrm{tp}_\sigma(\bar{c}_2/B)$.*

Proof. This theorem was proved by Chatzidakis and Pillay in [**16**]. For convenience we repeat their proof here.

Without loss we may assume that A and B are acl_σ-closed. Choose $\bar{c}$ with $\bar{c} \equiv_A \bar{c}_1$ and, writing $C = \mathrm{acl}_\sigma(M, \bar{c})$, such that C is independent from AB over M.

Fist note that as T is stable, corollary (5.12) shows that $\mathrm{acl}_\sigma(A_1A_2) = \mathrm{acl}_\mathrm{T}(\mathrm{acl}_\sigma(A_1), \mathrm{acl}_\sigma(A_2))$ for any sets $A_1, A_2 \subset \mathfrak{C}$. So because σ restricts to automorphisms of A, B and C respectively, we find that acl_σ and acl_T agree on A, B, C, AB, AC, BC and ACB. Let us call $\sigma_{AB} = \sigma|_{\mathrm{acl}_\mathrm{T}(AB)}$ and $\sigma_{AC} = \sigma|_{\mathrm{acl}_\mathrm{T}(AC)}$. Then proposition (5.3) implies that $\sigma_{AB} \cup \sigma_{AC}$ is elementary in the sense of T. Working in $\mathfrak{C}$, we want to find an automorphism τ on $\mathrm{acl}_\mathrm{T}(ABC)$ extending σ_{AB} and σ_{AC} such that $(\mathrm{acl}_\mathrm{T}(BC), \tau|_{\mathrm{acl}_\mathrm{T}(BC)})$ and $(\mathrm{acl}_\sigma(B, \bar{c}_2), \sigma)$ are L_σ-isomorphic over (B, σ) via an isomorphism sending $\bar{c}$ to $\bar{c}_2$.

To that end we define σ_{BC} on $\mathrm{acl}_\mathrm{T}(BC)$ as follows. Because T is stable, we may use corollary (5.11) to first choose an L_σ-isomorphism φ_1 over M from (C, σ) onto $(\mathrm{acl}_\sigma(M, \bar{c}_2), \sigma)$ sending $\bar{c}$ to $\bar{c}_2$. As C and $\mathrm{acl}_\sigma(M, \bar{c}_2)$ are both independent from B over M, this isomorphism extends to an L_σ-isomorphism over B from $(\mathrm{dcl}_\mathrm{T}(BC), \sigma)$ onto $(\mathrm{dcl}_\mathrm{T}(\mathrm{acl}_\sigma(M, \bar{c}_2), B), \sigma)$. Now we extend the latter to an L-isomorphism φ_2 from $\mathrm{acl}_\sigma(B, \bar{c})$ onto $\mathrm{acl}_\sigma(B, \bar{c}_2)$ and put $\sigma_{BC} = \varphi_2^{-1}\sigma|_{\mathrm{acl}_\sigma(B,\bar{c}_2)}\varphi_2$.

We want to show that $\alpha = \sigma_{AB} \cup \sigma_{AC} \cup \sigma_{BC}$ is elementary in the sense of T. For then α lifts to an automorphism τ of $\mathrm{acl}_\mathrm{T}(ABC)$ and we can, using (5.10), embed $(\mathrm{acl}_\mathrm{T}(ABC), \tau)$ over AB into $(\mathfrak{C}, \sigma)$. The image of $\bar{c}$ under this embedding is the promised realisation of $\mathrm{tp}_\sigma(\bar{c}_1/A) \cup \mathrm{tp}_\sigma(\bar{c}_2/B)$.

We know already that $\sigma_{AB} \cup \sigma_{AC}$ is elementary, so let $\bar{z}_0$ enumerate $\mathrm{dcl}_\mathrm{T}(BC)$, $\bar{z}_1$ enumerate $\mathrm{dcl}_\mathrm{T}\big(\mathrm{acl}_\mathrm{T}(AB), \mathrm{acl}_\mathrm{T}(AC)\big) \setminus \mathrm{dcl}_\mathrm{T}(BC)$ and $\bar{z}_2$ enumerate $\mathrm{acl}_\mathrm{T}(BC) \setminus \mathrm{dcl}_\mathrm{T}(BC)$. Because T is stable, we know by lemma (5.19) that $\mathrm{dcl}_\mathrm{T}(BC)$ is acl_T-closed in $\mathrm{dcl}_\mathrm{T}(\mathrm{acl}_\mathrm{T}(AB), \mathrm{acl}_\mathrm{T}(AC))$. So because σ_{AB}, σ_{AC} and σ_{BC} are automorphisms onto their domains it follows that

$$\mathrm{tp}_\sigma(\bar{z}_2\bar{z}_0) \vdash \mathrm{tp}_\sigma(\bar{z}_2\bar{z}_1\bar{z}_0)$$

and

$$\mathrm{tp}_\sigma(\sigma_{BC}(\bar{z}_2)(\sigma_{AB} \cup \sigma_{AC})(\bar{z}_0)) \ \vdash \ \mathrm{tp}_\sigma(\sigma_{BC}(\bar{z}_2)(\sigma_{AB} \cup \sigma_{AC})(\bar{z}_1\bar{z}_0)) \ .$$

But σ_{BC} and $\sigma_{AB} \cup \sigma_{AC}$ coincide on $\mathrm{dcl}_\mathrm{T}(BC)$ by construction, so

$$\mathrm{tp}_\sigma(\sigma_{BC}(\bar{z}_2)\sigma_{BC}(\bar{z}_0)) \ \vdash \ \mathrm{tp}_\sigma(\sigma_{BC}(\bar{z}_2)(\sigma_{AB} \cup \sigma_{AC})(\bar{z}_1\bar{z}_0)) \ ,$$

which implies that

$$\mathrm{tp}_\sigma(\bar{z}_0\bar{z}_1\bar{z}_2) = \mathrm{tp}_\sigma(\alpha(\bar{z}_0\bar{z}_1\bar{z}_2))$$

because σ_{BC} is elementary. □

Corollary 5.21 (Chatzidakis-Pillay). *Let T be a stable theory and assume TA exists. Then any completion of TA is simple. If T is superstable, then any completion of TA is supersimple.*

Proof. This was shown in [**16**], we repeat their proof for convenience.

We first show simplicity of TA in case T is stable, so let $(\mathfrak{C}, \sigma)$ be a sufficiently saturated model of TA. Clearly the notion of independence

defined above is invariant under automorphisms and satisfies Symmetry and Finite Character. Note that, by corollary (5.12),

$$\mathrm{acl}_\sigma(AB) = \mathrm{acl}_\mathrm{T}(\mathrm{acl}_\sigma(A), \mathrm{acl}_\sigma(B))$$

for all sets A and B, wherefrom Transitivity follows.

To show Extension, let $\bar{a}$ be a tuple and $A \subset B$ be subsets of $\mathfrak{C}$. We may assume that A and B are acl_σ-closed and consider the L_σ-structures $(A, \sigma_0), (\mathrm{acl}_\sigma(A\bar{a}), \sigma_1)$ and (B, σ_2), where σ_i denotes the corresponding restriction of σ to $A, \mathrm{acl}_\sigma(A\bar{a})$ and B. By corollary (5.7) we may assume that $\mathrm{acl}_\sigma(A\bar{a})$ and B are independent over A in the sense of T. By model completeness of TA we can embed (C, σ) over B into $(\mathfrak{C}, \sigma)$. Then the type of image of $\bar{a}$ under this embedding is the desired extension of $\mathrm{tp}_\sigma(\bar{a}/A)$ to B.

To show Local Character, let $\bar{a}$ be a tuple and A be a subset of $(\mathfrak{C}, \sigma)$. We may assume that A is acl_σ-closed. As $\mathrm{cl}_\sigma(\bar{a})$ is countable, it follows that there is some $A_0 \subset A$ with $|A_0| \leq |T| = |TA|$ such that $\mathrm{cl}_\sigma(\bar{a}) \underset{A_0}{\downarrow} A$ in the sense of T. By Transitivity (for T) we may assume that A_0 is acl_σ-closed. Then still $|A_0| \leq |TA|$. It follows that $A_0\mathrm{cl}_\sigma(\bar{a}) \underset{A_0}{\downarrow} A$, which implies $\mathrm{acl}_\mathrm{T}(A_0\mathrm{cl}_\sigma(\bar{a})) \underset{A_0}{\downarrow} A$, both in the sense of T. But $\mathrm{acl}_\mathrm{T}(A_0\mathrm{cl}_\sigma(\bar{a})) = \mathrm{acl}_\sigma(A_0, \bar{a})$ by corollary (5.12), so $\bar{a}$ is independent from A over A_0 in the sense of TA.

We suppose now that T is superstable and aim to show that TA is supersimple. Let $\bar{a} \in M$ and $B = \mathrm{acl}_\sigma(B) \subset M$ for some model (M, σ) of TA. As T is superstable there is $m > 0$ such that $\mathrm{tp}(\bar{a}/B\{\sigma^i(\bar{a})\}_{i\in\mathbb{N}})$ does not fork over $B, \sigma(\bar{a}), \ldots, \sigma^m(\bar{a})$ in the sense of T. Also there is some finite $A_0 \subset B$ such that $\mathrm{tp}(\bar{a}, \sigma(\bar{a}), \ldots, \sigma^m(\bar{a})/B)$ does not fork over A_0, again in the sense of T.

Let $A = \mathrm{acl}_\sigma(A_0)$. We will show by induction that $\bar{a}, \sigma(\bar{a}), \ldots, \sigma^k(\bar{a})$ is independent from B over A in the sense of T for all $k > 0$. Therefrom it follows that $\mathrm{acl}_\sigma(A, \bar{a})$ is independent from B over A, which is equivalent to $\bar{a}$ being independent from B over A_0 in the sense of TA.

If $k \leq m$ there is nothing to show. Assume the statement is true for k. By choice of m and transitivity we know that

$$\bar{a} \underset{B,\sigma(\bar{a}),\ldots,\sigma^m(\bar{a})}{\downarrow} B, \sigma(\bar{a}), \ldots, \sigma^{k+1}(\bar{a}) \ .$$

Also by transitivity it follows from $\bar{a}, \sigma(\bar{a}), \ldots, \sigma^m(\bar{a}) \underset{A}{\downarrow} B$ that

$$\bar{a} \underset{A,\sigma(\bar{a}),\ldots,\sigma^m(\bar{a})}{\downarrow} B, \sigma(\bar{a}), \ldots, \sigma^m(\bar{a}) \ .$$

Again transitivity implies that

$$\bar{a} \underset{A,\sigma(\bar{a}),\ldots,\sigma^m(\bar{a})}{\downarrow} B, \sigma(\bar{a}), \ldots, \sigma^{k+1}(\bar{a})$$

and thus

$$\bar{a} \underset{A,\sigma(\bar{a}),\ldots,\sigma^{k+1}(\bar{a})}{\downarrow} B, \sigma(\bar{a}), \ldots, \sigma^{k+1}(\bar{a}) \ .$$

Together with $\sigma(\bar{a}), \ldots, \sigma^{k+1}(\bar{a}) \underset{A}{\downarrow} B$, which comes from the induction hypothesis, transitivity yields

$$\bar{a}, \sigma(\bar{a}), \ldots, \sigma^{k+1}(\bar{a}) \underset{A}{\downarrow} B \ .$$

□

The following proposition gives a criterion for when TA is even stable. It is a direct consequence of corollary (5.11), so we omit the proof.

PROPOSITION 5.22. *Let A be acl_σ-closed and $\bar{a}$ be a tuple. Then $\mathrm{tp}_\sigma(\bar{a}/A)$ is stationary if and only if for any set B containing A that is acl_σ-closed and independent from $\bar{a}$ over A, $\sigma|_{\mathrm{dcl_T}(B,C)}$ has a unique extension to $\mathrm{acl_T}(B,C)$ up to conjugation in $\mathrm{Aut}_T(\mathrm{acl_T}(B,C)/\mathrm{dcl_T}(B,C))$, where $C = \mathrm{acl}_\sigma(A\bar{a})$.*

We will later be interested fields with a generic automorphism. In that cases, TA is simple unstable. However, the quantifier-free fragment of TA is always stable.

LEMMA 5.23. *Let T be a stable complete L-theory with quantifier elimination and elimination of imaginaries such that TA exists. Then TA is quantifier-free stable (i.e. every completion of TA is quantifier-free stable). Furthermore, if T is totally transcendental then TA is quantifier-free totally transcendental.*

Proof. Let $\sigma \in \mathrm{Aut}_T(\mathfrak{C})$ such that $(\mathfrak{C}, \sigma) \models TA$ and A be a subset of $(\mathfrak{C}, \sigma)$ of size λ with $\lambda^{|T|} = \lambda$. Then $\lambda^\omega = \lambda$. We may assume that A is acl_σ-closed . Then A is also $\mathrm{acl_T}$-closed. Consider a tuple $\bar{a} \in (\bar{M}, \sigma)$. Obviously $qftp_\sigma(\bar{a}/A)$ is uniquely determined by $qftp_L(\sigma^i(\bar{a})_{i\in\mathbb{Z}}/A)$ by quantifier elimination of T. As T is stable there are only λ-many (quantifier-free) types over A of sequences of length ω.

The second part was proved by Bustamante-Medina (see [**7**], the discussion preceding remark (3.32)). Since we are going to use this fact later on, we repeat his argument here. So assume that T is totally transcendental and let $A = \mathrm{acl}_\sigma(A) \subset \mathfrak{C}$ and $\bar{a} \in \mathfrak{C}$ be a tuple. Let $B = \mathrm{dcl_T}(A, \sigma^i(\bar{a}) | i < 0)$ and consider $\mathrm{tp}_T(\bar{a}/B)$. Now our assumption that T is totally transcendental implies that there is some $n \in \mathbb{N}$ such that $\mathrm{tp}_T(\bar{a}/B)$ is the unique non-forking extension of $\mathrm{tp}_T(\bar{a}/A, \sigma^{-n}(\bar{a}), \ldots, \sigma^{-1}(\bar{a}))$ to B. Because σ^i is an L-automorphism, it follows that $\mathrm{tp}_T(\sigma^i(\bar{a})/\sigma^i(B))$ is the unique non-forking extension of the type $\mathrm{tp}_T(\sigma^i(\bar{a})/A, \sigma^{i-n}(\bar{a}), \ldots, \sigma^{i-1}(\bar{a}))$ to $\sigma^i(B)$. This shows that TA is quantifier-free totally transcendental. □

So in particular we have local ranks on quantifier-free formulae in TA. Quantifier-free stability of TA has the following consequence, which will play an important rôle in our proof of theorem (5.65). Recall that for a theory T' and parameter set A in T' the locally isolated quantifier-free types are said to be dense in (the space of) quantifier-free types over A if for any quantifier-free formula $\varphi(\bar{x})$ in the language of T' there is some quantifier-free type π containing φ such that for any finite set Δ of quantifier-free formulae there is some $\delta(\bar{x}) \in \pi$ (in the language of T') such that $\delta(\bar{x}) \vdash \pi|_\Delta$.

PROPOSITION 5.24. *Let T be a countable complete stable L-theory, with quantifier elimination and elimination of imaginaries. Assume that TA exists and eliminates imaginaries. Then for any completion of TA and any parameter set A (in the sense of that completion) the locally isolated quantifier-free types are dense in the space of quantifier-free types over A. If T is totally transcendental, then the isolated quantifier-free types are dense in the quantifier-free types over A.*

Proof. It is well-known that in a countable stable theory the locally isolated types are dense over any parameter set (see for example [**74**], theorem (11.8)). Even if TA might be unstable, its quantifier-free fragment is stable by lemma (5.23). It is countable because T is. From now on the proof follows the same line as for countable stable theories: Let $\varphi(\bar{x})$ be a quantifier-free L_σ-formula and $(\Delta_i)_{i\in\mathbb{N}}$ be an enumeration of all finite sets of quantifier-free L_σ-formulae $\psi(\bar{x},\bar{y})$. One constructs recursively a sequence $\varphi_i(\bar{x})$ of quantifier-free $L_\sigma(A)$-formulae. Starting with $\varphi_0(\bar{x}) = \varphi(\bar{x})$ one lets $\varphi_{n+1}(\bar{x})$ be a quantifier-free $L_\sigma(A)$-formula of minimal Δ_{n+1}-rank and -degree with $\models \varphi_{n+1}(\bar{x}) \to \varphi_n(\bar{x})$. Then $\{\varphi_n(\bar{x}) \mid n \in \mathbb{N}\}$ axiomatises a locally isolated quantifier-free type over A that contains $\varphi(\bar{x})$. □

Finally we want to mention the impact of the Independence Theorem on elimination of imaginaries. We say that TA satisfies the Independence Theorem over algebraically closed sets if it satisfies the Independence Theorem (5.20) with the hypothesis $(M,\sigma) \models T_\sigma$ weakened to (M,σ) be an acl_σ-closed substructure of $(\mathfrak{C},\sigma)$ (of the home sort of $(\mathfrak{C},\sigma)$, not of $(\mathfrak{C},\sigma)^{\mathrm{eq}}$). At first sight this may seem peculiar, so let us point out that if $\mathrm{acl}_{\mathrm{T}}(A)$ is a model of T, as for example when T is ACF or SCF_e ($e \in \mathbb{N}$) or when T is strongly minimal with $\mathrm{acl}_{\mathrm{T}}(\emptyset)$ infinite, then this is nothing but theorem (5.20). When T is DCF, TA exists and also satisfies the Independence Theorem over algebraically closed sets, as proved by Bustamante-Medina [**7**].

PROPOSITION 5.25. *Let T be stable and eliminate imaginaries and let TA satisfy the Independence Theorem over algebraically closed sets. Then TA eliminates imaginaries (i.e. every completion of TA does).*

Note that this was proved for several theories of fields with generic automorphism, for example in the case when T is ACF by Chatzidakis and Hrushovski in [**14**], when T is SCF_e ($e \in \mathbb{N}$) by Chatzidakis in [**12**], when T is DCF by Bustamante-Medina in [**7**], and for strongly minimal T with $\mathrm{acl}_{\mathrm{T}}(\emptyset)$ infinite by Chatzidakis and Pillay in [**16**]. We step here along Pillay's proof line in [**52**] where he did the strongly minimal case.

Proof of proposition (5.25). Let (M,σ) be a model of TA and e be an imaginary element. We may assume that (M,σ) is enough saturated. To distinguish, we write acl_σ and dcl_σ if we compute the respective closure in the home sort (and obtain subsets if M), and $\mathrm{acl}_\sigma^{\mathrm{eq}}$ and $\mathrm{dcl}_\sigma^{\mathrm{eq}}$ if we compute the respective closure in $(M,\sigma)^{\mathrm{eq}}$. Choose a $\emptyset$-definable function f and a tuple $\bar{a} \in M$ such that $e = f(\bar{a})$. Let $\bar{b}$ realise the type of $\bar{a}$ over e and be

independent from $\bar{a}$ over e. Further let $\bar{c} \in M$ realise the type of $\bar{a}$ over e and be independent from $\mathrm{acl}_\sigma(\bar{a}, \bar{b})$ over $\mathrm{acl}^{\mathrm{eq}}_\sigma(e)$.

There is a unique smallest acl_σ-closed subset $A \subset M$ (not M^{eq}) such that $\bar{c}$ is independent from $\mathrm{acl}_\sigma(\bar{a}, \bar{b})$ over A: if $\mathrm{Cb}(p)$ is the canonical basis of the type $p = \mathrm{tp}((\sigma^i(\bar{c}))_{i\in\mathbb{Z}}/\mathrm{acl}_\sigma(\bar{a}, \bar{b}))$, all in the sense of T, then we just take $A = \mathrm{acl}_{\mathrm{T}}(\mathrm{Cb}(p))$. Thereby we may assume that $\mathrm{Cb}(p) \subset M$ by elimination of imaginaries of T. A does the job because clearly $\sigma(p) = p$ and hence $\sigma(\mathrm{Cb}(p)) = \mathrm{Cb}(p)$, which implies that $A = \mathrm{acl}_\sigma(A)$ by corollary (5.12).

At first we want to show that e is algebraic over A. To that end, let us show that $A \subseteq \mathrm{acl}^{\mathrm{eq}}_\sigma(e)$. We have chosen c to be independent from $\mathrm{acl}_\sigma(\bar{a}, \bar{b})$ over $\mathrm{acl}^{\mathrm{eq}}_\sigma(e)$, so c is independent from $\mathrm{acl}^{\mathrm{eq}}_\sigma(\bar{a}, \bar{b})$ over $\mathrm{acl}^{\mathrm{eq}}_\sigma(e)$. By transitivity we obtain that c is independent from $\mathrm{acl}^{\mathrm{eq}}_\sigma(\bar{a}, \bar{b})$ over $\mathrm{acl}^{\mathrm{eq}}_\sigma(a)$ because $e \in \mathrm{acl}^{\mathrm{eq}}_\sigma(\bar{a})$. Hence c is independent from $\mathrm{acl}_\sigma(\bar{a}, \bar{b})$ over $\mathrm{acl}_\sigma(\bar{a})$, as $a, b, c \in M$. By the choice of A, we then have that $A \subseteq \mathrm{acl}_\sigma(\bar{a})$. The same argument shows that $A \subseteq \mathrm{acl}_\sigma(b)$, whence we get $A \subseteq \mathrm{acl}_\sigma(\bar{a}) \cap \mathrm{acl}_\sigma(\bar{b})$. As $\mathrm{acl}^{\mathrm{eq}}_\sigma(\bar{a}) \cap \mathrm{acl}^{\mathrm{eq}}_\sigma(\bar{b}) = \mathrm{acl}^{\mathrm{eq}}_\sigma(e)$ we conclude that $A \subseteq \mathrm{acl}^{\mathrm{eq}}_\sigma(e)$.

So $A \subseteq \mathrm{acl}^{\mathrm{eq}}_\sigma(e)$. c is independent from $\mathrm{acl}_\sigma(\bar{a}, \bar{b})$ over A, so it is independent from $\mathrm{acl}^{\mathrm{eq}}_\sigma(\bar{a}, \bar{b})$ over $\mathrm{acl}^{\mathrm{eq}}_\sigma(A)$. As $\mathrm{acl}^{\mathrm{eq}}_\sigma(A) \subseteq \mathrm{acl}^{\mathrm{eq}}_\sigma(e)\mathrm{acl}^{\mathrm{eq}}_\sigma(a, b)$, transitivity implies that c is independent from e over A. But e is algebraic over c, so it must be algebraic already over A.

We want to show that e is even definable over A. To that end choose any realisation $\bar{a}'$ of $\mathrm{tp}_\sigma(\bar{a}/A)$. There is some $\bar{b}'$ realising $\mathrm{tp}_\sigma(\bar{a}'/A)$ which is independent from $\bar{a}'$ over A, with $f(\bar{b}') = f(\bar{a}')$ and which is independent from $\bar{b}$ over A. As A is acl_σ-closed we can apply the Independence Theorem over algebraically closed sets to find some realisation $\bar{d}$ of $\mathrm{tp}_\sigma(\bar{a}/A\bar{b}) \cup \mathrm{tp}_\sigma(\bar{a}'/A\bar{b}')$. But then $f(\bar{a}) = f(\bar{d}) = f(\bar{a}')$, so it follows that e is definable over A.

What we have shown is that there is some real tuple $\bar{a}'$ with $\bar{a}' \in \mathrm{acl}^{eq}_\sigma(e)$ and $e \in \mathrm{dcl}^{eq}_\sigma(\bar{a}')$. As T eliminates imaginaries, the set of e-conjugates of $\bar{a}'$ is interdefinable with a real tuple, and thus so is e. □

Reducts. The reduct of (M, σ) we will primarily deal with is $(M, \sigma\phi)$, where ϕ is an automorphism of T which is L-definable over $\emptyset$. We have not found the following in the literature in this generality. It is a direct generalisation of [**14**], corollary (1.12).

Proposition 5.26. *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries such that TA exists. Let $(M, \sigma) \models TA$ and ϕ be an automorphism of T that is L-definable over $\emptyset$. Let further $k \in \mathbb{Z} \setminus \{0\}$ and $n \in \mathbb{N}$.*

1. *The reduct $(M, \sigma^k\phi)$ is a model of TA. If (M, σ) is κ-saturated, then so is $(M, \sigma^k\phi)$.*
2. *If there is $\tau \in \mathrm{Aut}_T(\mathrm{acl}_{\mathrm{T}}(\emptyset))$ such that $\tau^n = \sigma|_{\mathrm{acl}_{\mathrm{T}}(\emptyset)}$, then there is some elementary extension (N, σ) of (M, σ) and $\tau' \in \mathrm{Aut}_T(N)$ extending τ such that $(N, \tau') \models TA$ and $\tau'^n = \sigma$.*

Proof. Obviously $(M, \sigma^k\phi) \models T_\sigma$. We show that $(M, \sigma^k\phi)$ is existentially closed in models of T_σ.

First note that if $(M, \sigma) \models TA$, then so is (M, σ^{-1}). Indeed, if (N, τ) is a model of T_σ extending (M, σ^{-1}), then (N, τ^{-1}) is a model of T_σ extending (M, σ). So to prove *1.*, we may assume that $k \geq 1$.

Second, by the assumption made on ϕ, if $(N, \tau) \models T_\sigma$ extends $(M, \sigma\phi)$, then $(N, \tau \circ \phi^{-1}) \models T_\sigma$ extends (M, σ), and $(M, \sigma\phi)$ is existentially closed in (N, τ) if and only if (M, σ) is so in $(N, \sigma \circ \phi^{-1})$. Thus we may assume that $\phi = id$.

Let $(N, \tau) \models T_\sigma$ be an extension of (M, σ^k). To show that (M, σ^k) is existentially closed, it clearly suffices to show that there is some elementary extension M' of M and some automorphism σ' of M' extending σ such that $\sigma^k|_N = \tau$. Choose $N_i \models \sigma^i \mathrm{tp}(N/M)$ for any $i \in [0; k-1]$, starting with $N_0 = N$, such that $N_0, \ldots, N_{k-1}$ are pairwise independent over M in the sense of T. Choose further elementary maps $\sigma_i : N_{i-1} \longrightarrow N_i$ for $i \geq 1$ extending σ and define $\sigma_k := \tau \circ (\sigma_{k-1} \circ \cdots \circ \sigma_1)^{-1}$. Then $\sigma_k : N_{k-1} \longrightarrow N$ is an elementary map extending σ. As T is stable, it follows from lemma (5.2) that $\sigma' = \sigma_1 \cup \cdots \cup \sigma_k$ is elementary (in the sense of T) and thus extends to an automorphism of some elementary extension M' of M that contains N. By abuse of notation we call this automorphism σ', too. By construction, σ' extends σ and $\sigma'^k|_N = \tau$.

It is clear that if (M, σ) is κ-saturated, then so is $(M, \sigma^k\phi)$.

For the second assertion, we may assume that (M, σ) is enough saturated. Then from the above argument it follows that (M, σ^n) is enough saturated, so by the description of the completions of TA we are done. □

Existence of TA. To round up our exposition of the general model theory of TA, we shortly mention the question of existence. T is assumed to be countable in this paragraph.

Given a model complete theory T, neither necessarily complete nor necessarily stable, it is a general (open) problem to find necessary and sufficient conditions on T for the class of existentially closed models of T_σ to be elementary. Baldwin and Shelah gave such a characterisation in [**6**] in the case when T is a countable complete model complete stable theory. We present the translation of Pillay from [**50**].

Recall that an L-theory T has non-fcp[7] if for any L-formula $\theta(\bar{x}, \bar{y}, \bar{z})$, with $\bar{x}$ and $\bar{y}$ variable tuples of the same length, there is an L-formula $\phi(\bar{z})$ such that for any $\bar{a}$ for which $\theta(\bar{x}, \bar{y}, \bar{a})$ defines an equivalence relation E, E has infinitely many classes if and only if $\models \phi(\bar{a})$.

THEOREM 5.27 (Baldwin-Shelah, Pillay). *For a countable stable theory T with quantifier elimination, TA exists if and only if*

(1) *T has non-fcp, and*
(2) *for every finite set Δ_1 of L-formulas there is a finite set of L-formulas $\Delta_2 \supseteq \Delta_1$, such that for any $(M, \sigma) \models T_\sigma$, any complete*

[7] we use Shelah's definition, which is well-known to be equivalent to Keisler's for stable theories T, see [**30**]

Δ_1-type $p(\bar{x}, \bar{y})$ over M, where $\bar{x}$ and $\bar{y}$ have the same length, and for any complete Δ_2-type $q(\bar{x}, \bar{y})$ over M extending $p(\bar{x}, \bar{y})$, if $q(\bar{x}, \bar{y})$ implies that the Δ_2-type of $\bar{y}$ over M equals σ of the Δ_2-type of x over M, then there is a complete type $q'(\bar{x}, \bar{y})$ over M extending $p(\bar{x}, \bar{y})$ such that $q'(\bar{x}, \bar{y})$ implies that $\mathrm{tp}(\bar{y}/M) = \sigma(\mathrm{tp}(\bar{x}/M))$.

Proof. For a proof we refer to [**50**]. □

As outcome of the proof given in [**50**], one obtains the following axioms for TA in case it exists. Let $\varphi(x, y, z)$ be an L-formula and set $\Delta_1 = \{\varphi\}$. Let Δ_2 be a finite set of L-formulas containing Δ_1 as in fact (5.27). Then the axiom scheme contains:

(M, σ) is a model of T_σ, and for all $d \in M$ and all complete Δ_2-types $q(x, y)$ over M such that $\varphi(x, y, d) \in q$ and $q(x, y)$ implies that $\mathrm{tp}_{\Delta_2}(y/M) = \sigma(\mathrm{tp}_{\Delta_2}(x/M))$*, there is some $(a, b) \in M$ realising $\varphi(x, y, d)$ with $\sigma(a) = b$.*

This is first order because T has the non-fcp: As T is stable, a compactness argument shows that for any model M of T and for any formula $\varphi(\bar{x}; \bar{y})$ in L there is a finite set Δ of L-formulae such that any φ-type p over M is definable by a formula $\psi(\bar{y}, \bar{a})$, with $\psi(\bar{y}; \bar{z}) \in \Delta$ and $\bar{a} \in M$. Since T has the non-fcp, given a finite set of formulas Δ and $\delta(x, z) \in L$, there is some L-formula $\psi(z)$ such that for any model M of T and any tuple $a \in M$, $M \models \psi(a)$ if and only if $\delta(x, a)$ defines a complete Δ-type over M.

5.2. Fixed Structures and the PAC-property

We discuss the fixed structure $\mathrm{Fix}(M, \sigma)$ of a generic automorphism $(M, \sigma) \models TA$ and the PAC property. We define the notion of a PAC structure for arbitrary theories, in particular without requiring that the ambient theory be stable, and analyse the relation to the existing definitions: for example if the ambient theory is stable, then our definition coincides with those in the literature. We also include the proof that $\mathrm{Fix}(M, \sigma)$ is a PAC structure.

5.2.1. Fixed Structures. For an L_σ-structure (A, α), we call

$$\mathrm{Fix}(A, \alpha) = \{\, a \in A \,:\, \alpha(a) = a \,\}$$

the fixed set of (A, α). Let us start noting some easy observations. First, if T is an arbitrary L-theory and $(M, \sigma) \models T_\sigma$, then $\mathrm{Fix}(M, \sigma)$ is a $\mathrm{dcl_T}$-closed subset of M because σ is an L-automorphism of M. Hence if $\mathrm{Fix}(M, \sigma)$ is non-empty, it is an L-substructure of M. The same holds for $\mathrm{Fix}(M, \sigma\phi)$ for all automorphisms ϕ of M that are L-definable without parameters. Furthermore, as σ is an L_σ-automorphism, it restricts to an automorphism of the L-structure $\mathrm{Fix}(M, \sigma\phi)$, and by definition we have $\sigma|_{\mathrm{Fix}(M,\sigma\phi)} = \phi^{-1}$. For the same reason ϕ is an L_σ-automorphism, so $\mathrm{Fix}(M, \sigma\phi)$ is definably closed in the L_σ-structure (M, σ). Hence $\mathrm{Fix}(M, \sigma\phi)$ is also an L_σ-substructure of (M, σ).

In the following we will not distinguish between the subset $\mathrm{Fix}(M, \sigma)$ of M and the L-substructure $\mathrm{Fix}(M, \sigma)$ of M, and call $\mathrm{Fix}(M, \sigma)$ the fixed

structure of (M, σ). For an automorphism ϕ of T that is L-definable without parameters, $\mathrm{Fix}(M, \sigma\phi)$ will be called fixed structure also.

REMARK 5.28. *If TA eliminates imaginaries, then $\mathrm{Fix}(M, \sigma\phi)$ is stably embedded in all $(M, \sigma) \models TA$.*

Proof. The canonical parameter of a definable subset X of $\mathrm{Fix}(M, \sigma\phi)$ is fixed by $\sigma\phi$. □

In particular, if (M, σ) is sufficiently saturated, then by lemma (4.15) any automorphism of $\mathrm{Fix}(M, \sigma)^{ind}$ lifts to an automorphism of (M, σ). The structure $\mathrm{Fix}(M, \sigma)^{ind}$ is a priori richer than the L-structure $\mathrm{Fix}(M, \sigma)$ in that there are more definable sets. However we will show in section 5.5 that in some sense $\mathrm{Fix}(M, \sigma)^{ind}$ is not richer than $\mathrm{Fix}(M, \sigma)$, namely we will show that $\mathrm{Fix}(M, \sigma)$ is conservatively embedded over certain L-elementary substructures, see lemma (5.62) and proposition (5.63).

5.2.2. ***PAC*-Structures.** The fixed structure $\mathrm{Fix}(M, \sigma)$ of a model (M, σ) of TA has a particularly interesting property: it is a so-called PAC-substructure of M (see proposition (5.40)). So far this notion was defined only for substructures of a stable theory. We are going to introduce the notion of a PAC structure for an arbitrary first order theory T with quantifier elimination. Below we will analyse the relationship between our definition and the known definitions in the literature for stable theories. But before, let us recall a few observations concerning substructures of models of T, which we use frequently in what follows. All are trivial or follow immediately from quantifier elimination of T.

Let T be an arbitrary first-order L-theory with quantifier elimination. If K is an L-substructure of some model of T, then of course any $K' \equiv_L K$ embeds into some model of T. If K is $\mathrm{dcl_T}$-closed, then so is K', and further, being $\mathrm{dcl_T}$-closed does not depend on the embedding or on the model into which K embeds. This follows from quantifier elimination of T. So by abuse of language we say that K is $\mathrm{dcl_T}$-closed, even if we have not fixed an embedding. Also $\mathrm{Gal}(K)$, the group of permutations of $\mathrm{acl_T}(K)$ over K that are elementary in the sense of T, is independent of the embedding of K into some model of M, up to isomorphism. So we will talk of $\mathrm{Gal}(K)$ even if no embedding into a model of T is specified. Finally if $K' \preccurlyeq_L K$, then $\mathrm{acl_T}(K') \cap K = K'$.

DEFINITION 5.29. *Let T be an arbitrary L-theory with quantifier-elimination and K be an L-structure which embeds into some model of T.*

1. *An extension $F \supseteq K$ of L-structures is called regular for T if F embeds into some model of T such that*
   (a) $\mathrm{acl_T}(K) \cap F = K$ *and*
   (b) *The restriction map* $\mathrm{Gal}(F) \longrightarrow \mathrm{Gal}(K)$ *is surjective.*
2. *K is said to be a pseudo-algebraically closed structure for T, or shortly a PAC-structure for T, or PAC for T, if K is existentially closed in all L-extensions that are regular for T.*

Obviously any model of T is PAC for T. If K is a PAC structure for T and contained in the model M of T, we say that K is a PAC-substructure of M for short. We also say that K is $\mathrm{dcl_T}$-closed PAC for T to abbreviate K is a $\mathrm{dcl_T}$-closed PAC L-substructure of some model of T. If it is clear from the context what theory T is meant, we just say that $F \supseteq K$ is a regular extension. Also, as in field theory, we write F/K for the extension of L-structures $K \subseteq F$.

REMARK 5.30. (1) *The property of the extension F/K to be regular for T does not depend on the embedding into a model of T. For as F embeds into some model,* $\mathrm{qfdiag}(F)$ *is a complete type in the sense of T by quantifier elimination. Hence any two images are conjugate over $\emptyset$ (in the monster model of T). Likewise, for an L-structure K to be PAC for T is independent of the embedding.*

(2) *K is PAC if and only if any regular extension embeds into some elementary extension of K.*

(3) *If F/K is regular for T and $K \subset H \subset F$, then H/K is regular for T.*

The PAC-property originates from Ax's article [**2**], where he introduced the notion of a PAC-field (called regularly closed field there). It has by now run through several steps of generalisation; first by Hrushovski [**26**] and later by Pillay and Polkowska [**53**]. We will analyse the relationship between these generalisations and our definition, but before that we give some examples.

EXAMPLE 5.31. *Let $e \in \mathbb{N}$ and T be $SCF_{e,b}$, the theory of separably closed fields of Ershov invariant e in the language L with constant symbols $b_1, \ldots, b_e$ for the p-basis and the λ-functions. A field K can be expanded to a $\mathrm{dcl_T}$-closed PAC structure for $SCF_{e,b}$ if and only if K is a PAC field of Ershov invariant e.*

Proof. Choosing a p-basis for K we may assume that K is an L-substructure of some (sufficiently saturated) model Ω of $SCF_{e,b}$. Because $\mathrm{acl}_{SCF_{e,b}}(F) = F^{\mathrm{sep}}$ for any subfield F of Ω that contains the p-basis $b_1, \ldots, b_e$, an extension F/K of L-structures is regular for $SCF_{e,b}$ if and only if the field extension $\mathrm{Quot}(F)/K$ is regular. □

EXAMPLE 5.32. *Let L be the ring language with λ-functions and $SCF_{\infty,\lambda}$ be the L-theory of separably closed fields of infinite Ershov invariant. A field K can be expanded to a $\mathrm{dcl_T}$-closed PAC structure for $SCF_{\infty,\lambda}$ if and only if K is a PAC field of infinite Ershov invariant.*

Proof. The proof is the same as in the previous example. Separability of the field extension F/K is ensured by the λ-functions of F extend the λ-functions of K. □

EXAMPLE 5.33. *Let L be the natural language of differential fields and T be DCF_0, the theory of differentially closed fields of characteristic zero. A differential field K is PAC for DCF_0 if and only if K is a pseudo-differentially closed differential field: any differential variety over K has a K-rational point.*

Proof. Similar as in the previous example. □

EXAMPLE 5.34. *Recall from [**59**] that a field K is called pseudo-real closed (PRC for short) if K is existentially closed in all regular field extensions to which any ordering of K extends. Let T be RCF, the theory of real closed fields, in the language L of rings with ordering $<$. If K is a PRC field, then then any expansion of K to an ordered field is PAC for RCF.*

Proof. Let K be a PRC field, and $<$ a field ordering on K. For an L-extension F of $(K,<)$ that is regular for RCF, the underlying field extension is regular. Thus K is existentially closed in F. □

We now analyse the relationship of our definition and those in the literature. Recall (e.g. from chapter 1) that a primary field extension of a perfect field is regular, and that regular field extensions F of a perfect field k correspond to stationary types over k (in ACF). The following lemma can be viewed a generalisation of this observation.

LEMMA 5.35. *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries, and let K and F be $\mathrm{dcl_T}$-closed L-substructures of some model of T. Assume that F extends K. Then the following are equivalent:*

(1) $\mathrm{acl_T}(K) \cap F = K$.
(2) *F/K is regular for T.*
(3) $\mathrm{tp}_T(F/K)$ *is stationary (in the sense of T).*

Proof. By elimination of imaginaries for T and as F is $\mathrm{dcl_T}$-closed, $\mathrm{tp}_T(F/F \cap \mathrm{acl_T}(K))$ is stationary. So (1) implies (3).

To show that (3) implies (2), let $p = \mathrm{tp}_T(F/K)$ be stationary. If $b \in \mathrm{acl_T}(K) \cap F$ has n conjugates over K, then p has at least n extensions to $\mathrm{acl_T}(K)$. As K is $\mathrm{dcl_T}$-closed it follows that $b \in K$.
Furthermore, $\alpha\big(\mathrm{tp}_T(F/\mathrm{acl_T}(K))\big) = \mathrm{tp}_T(F/\mathrm{acl_T}(K))$ for all $\alpha \in \mathrm{Gal}(K)$ by stationarity, so $\alpha \cup \mathrm{id}_F$ is elementary and lifts to an element of $\mathrm{Gal}(F)$. Thus F/K is regular for T.

That (2) implies (1) is trivial. □

COROLLARY 5.36. *Let L be the ring language and T be ACF_p (with p a prime of zero). A field K is a $\mathrm{dcl_T}$-closed PAC structure for T if and only if K is a perfect PAC field of characteristic p.*

Proof. Any field extension of a perfect field is separable, so the assertion follows from lemma (5.35) and theorem (1.12). □

COROLLARY 5.37. *Let T be a totally transcendental L-theory with quantifier elimination and elimination of imaginaries, and let K be an L-substructure of some model of T. Then the following are equivalent:*

(1) *K is a dcl_T-closed PAC structure for T.*
(2) *Any formula of Morley-degree one with parameters in K has a solution in K.*

Hrushovski [**26**] takes property (2) of the above equivalence to define the notion of a PAC-structure in strongly minimal theories.[8]

Let κ be a cardinal. Recall that an L-structure K is quantifier-free κ-saturated if any quantifier-free type in the sense of $Th(K)$ of size at most κ is realised in K.

COROLLARY 5.38. *Let T be a complete stable L-theory with quantifier elimination and elimination of imaginaries. Let K be an L-substructure of some model of T and $\kappa \geq |T|^+$ be a cardinal. Then the following are equivalent:*

1. *K is a quantifier-free κ-saturated L-structure which is dcl_T-closed and PAC L structure for T.*
2. *For any subset $A \subset K$ of size at most κ, any stationary type over A in the sense of T is realised in K.*

Pillay and Polkowska [**53**] defined the notion of a κ-PAC substructure of a model of a stable theory by property (2) of the above equivalence.

Proof of corollary (5.38). We first prove *(1) implies (2)*, so let K be quantifier-free κ-saturated, $\mathrm{dcl_T}$ -closed and PAC for T, A be a subset of K of size at most κ and let p be a stationary type over A in the sense of T. If $\bar{a}$ realises p and is independent from K over A in the sense of T, then the L-extension $F = \mathrm{dcl_T}(\bar{a}, K)$ of K is regular for T by lemma (5.35). Hence the set $\pi = \mathrm{qfdiag}_L(\mathrm{dcl_T}(\bar{a}, A))$ is finitely satisfiable in the L-structure K and can be viewed a partial type in the sense of K with parameters from A. By the saturation assumption on K there is a realisation $\bar{b}$ of π in K. Now by quantifier elimination of T it follows that $\bar{b} \models p$.

For the converse, it is clear that K is $\mathrm{dcl_T}$-closed. To show that K is PAC for T, let F/K be regular for T, and $\bar{a} \in F$ be a finite tuple that satisfies the quantifier-free L-formula $\varphi(\bar{x}, \bar{m})$, with $\bar{m} \in K$. By lemma (5.35) the type $p = \mathrm{tp}_T(\bar{a}/K)$ is stationary, as $\mathrm{dcl_T}(\bar{a}, K)/K$ is regular for T and K is $\mathrm{dcl_T}$-closed. Because T is stable there is some subset $A_0 \subset K$ with $|A_0| \leq |T|$ such that $p|_{A_0,\bar{m}}$ is stationary. Then by assumption $p|_{A_0,\bar{m}}$ is realised in K. In particular there is some $\bar{b} \in K$ with $K \models \varphi(\bar{b}, \bar{m})$.

To see that K is quantifier-free κ-saturated, let $K_1 \preccurlyeq_L K$ and K_2 be an elementary extension of K_1. Assume that K_1 and K_2 have size at most κ. K_1 and K_2 embed into models of T and are $\mathrm{dcl_T}$-closed because K is so. Furthermore $\mathrm{acl_T}(K_1) \cap K_2 = K_1$, so by elimination of imaginaries for T it follows from lemma (5.35) that $\mathrm{tp}_T(K_2/K_1)$ is stationary. Hence K_2 embeds over K_1 into K. This shows that K is quantifier-free κ-saturated. □

REMARK 5.39. *It follows from the above proof that if $Th(K)$ happens to be model complete, then "quantifier-free κ-saturated" can be replaced by "κ-saturated".*

[8] We note that Hrushovski requires $\mathrm{tp}_T(\bar{a}/\mathrm{acl}_T(C) \cap \mathrm{dcl}_T(C\bar{a}))$ to be stationary for any tuple $\bar{a}$ and parameter set C, instead of full elimination of imaginaries. We could have done so, too, but we want to stay coherent with our general assumption of elimination of imaginaries.

PROPOSITION 5.40 (Pillay-Polkowska). *Let T be stable with quantifier elimination and elimination of imaginaries. Assume that TA exists and eliminates imaginaries. Then for any model (M,σ) of TA, $\mathrm{Fix}(M,\sigma)$ is a dcl_T-closed PAC L-structure for T. Furthermore $\mathrm{Gal}(\mathrm{Fix}(M,\sigma)) = \widehat{\mathbb{Z}}$.*

Proof. That $\mathrm{Fix}(M,\sigma)$ is a PAC for T follows from lemma (4.1) of [**53**]. That $\mathrm{Gal}(\mathrm{Fix}(M,\sigma)) = \widehat{\mathbb{Z}}$ follows from a standard argument. We give the proof for convenience.

To begin with, it is clear that $\mathrm{Fix}(M,\sigma)$ is $\mathrm{dcl_T}$-closed, as σ is an L-automorphism.

Denote $F = \mathrm{Fix}(M,\sigma)$. It follows from Galois Theory [**57**] that $\mathrm{Gal}(F)$ is procyclic. Namely, $F = \mathrm{Fix}(\mathrm{acl_T}(F), \sigma|_{\mathrm{acl_T}(F)})$ and so $\sigma|_{\mathrm{acl_T}(F)}$ generates $\mathrm{Gal}(F)$ topologically. Hence we only have to show that for any $n \in \mathbb{N}$ there is an open subgroup of $\mathrm{Gal}(F)$ of index n. Reasoning as in the proof of (5.26) we find an extension $(N,\sigma) \models T_\sigma$ of (M,σ) and pairwise distinct elements $c_0, \ldots, c_{n-1} \in N$ with $\sigma(c_i) = c_{i+1}$ (where $c_n = c_0$). Hence

$$(N,\sigma) \models \exists \bar{x} \;\; \sigma^n(\bar{x}) = \bar{x} \wedge \bigwedge_{i=1}^{n-1} \sigma^i(\bar{x}) \neq \bar{x}$$

and thus so does (M,σ). So we find $a \in M$ with $\sigma^n(a) = a$ and $\sigma^i(a) \neq a$ for all $i \in [1; n-1]$. Using elimination of imaginaries and Galois theory [**57**] we see that the stabiliser of the tuple $a, \sigma(a), \ldots, \sigma^{n-1}(a)$ in $\mathrm{Gal}(F)$ is an open subgroup of $\mathrm{Gal}(F)$ of index n.

To show that F is PAC let H be a regular extension of F. By definition H embeds into some model of T, which we may assume to contain M also. As in the proof of corollary (5.38) we may assume that $H = \mathrm{dcl_T}(\bar{a}K)$ for some finite tuple $\bar{a}$. So $p = \mathrm{tp}_T(H/F)$ is a complete stationary type in the sense of T by lemma (5.35). Further we may assume that H is independent from M over F in the sense of T. It follows from stationarity of p that $\sigma(p) = p$ because σ leaves F pointwise fixed. Hence $\sigma \cup id_H$ is elementary in the sense of T, and so extends to some automorphism τ of some model N of T. As TA is the model companion of T_σ, we may assume that $(N,\tau) \models TA$. Because TA is model complete we have $(M,\sigma) \preccurlyeq (N,\tau)$, whence it follows that that F is existentially closed in H. □

REMARK 5.41. *The notion of regular extension for T serves us mainly to define the PAC property. We could have defined both only for stable theories, by saying that an extension F/K is regular if and only if it is regular in the sense of our definition (5.29), and additionally the canonical basis of $\mathrm{tp}_T(F/K)$ is contained in K (rather than in $\mathrm{dcl_T}(K)$). If we did this, then PAC fields would be exactly the PAC structures for ACF. However, we would loose example (5.34).*

5.3. Generic Automorphisms of Stable Fields

After the general theory in the previous sections, we now discuss some examples. We are particularly interested in the following theories of stable

fields with a generic automorphism, though other theories admit generic automorphisms, too. We give references below.

Algebraically Closed Fields. Maybe the most prominent example is $ACFA$, the theory of algebraically closed fields with a generic automorphism. We have already discussed it in the previous chapter, so we recommemorate only briefly. For references we refer to the previous chapter. Let $L_{ring} = \{ 0, 1, +, -, \cdot \}$ be the ring language and T be ACF, the L_{ring}-theory of algebraically closed fields. T is model complete and admits quantifier elimination. It is strongly minimal and eliminates imaginaries. ACF_σ has a model companion, $ACFA$. $ACFA$ is supersimple unstable. The fixed field of a model of $ACFA$ is a pseudo-finite field, and to any given pseudo-finite field k there is a model of $ACFA$ whose fixed field is elementarily equivalent to k.

Differentially Closed Fields. Recall that a differential field (K, d) consists of a field K together with a derivation $d : K \longrightarrow K$. Let L_d be the natural language of differential fields, namely $L_d = \{ 0, 1, +, -, \cdot, d \}$ with d a unary function symbol for the derivation. (K, d) is called differentially closed if it is existentially closed among differential fields (as L_d-structures). We call DCF_0 the L-theory of differentially closed fields in characteristic zero. DCF_0 is complete and admits quantifier elimination. It is ω-stable of rank ω and eliminates imaginaries. We refer to [**75**] and [**72**] for details on differential algebra and differentially closed fields.

If (K, d) is a differential field and σ is an automorphism of (K, d), that is, a field automorphism commuting with the derivation, we call (K, d, σ) a difference-differential field. We let $L_{d,\sigma}$ be the language of differential fields augmented by a unary function symbol σ.

Fact 5.42 (Hrushovski, unpublished). *DCF_0 admits generic automorphisms. The model companion of the $L_{d,\sigma}$-theory of difference-differential fields of characteristic zero is called $DCFA$.*

Proof. We refer the reader to Bustamante-Medina's thesis [**8**].

Fact 5.43 (Bustamante-Medina). *$DCFA$ satisfies the Independence Theorem over algebraically closed sets and eliminates imaginaries. If (k, d) is a differential field, then $(k, d) \equiv_{L_d} \mathrm{Fix}(\Omega, d, \sigma)$ for some model $\mathrm{Fix}(\Omega, d, \sigma)$ of $DCFA$ if and only if*

1. *k is pseudo-finite of characteristic zero, and*
2. *(k, d) satisfies the geometric axioms of differentially closed fields: For every (absolutely irreducible) affine variety V over k and (abs. irred.) subvariety W of the torsor[9] $\tau(V)$ of V projecting generically onto V, there is $a \in V(k)$ such that $(a, d(a)) \in W$.*

Proof. The Independence Theorem over algebraically closed sets for $DCFA$ is proved in [**7**], theorem (3.31). Elimination of imaginaries was

[9]Recall for an affine variety $V \subseteq \mathbb{A}^n$ defined over the differential field (K, d) the torsor $\tau(V)$ of V is the subvariety of $\mathbb{A}^{2n}$ defined by the equations $f(\bar{X}) = 0$ and $\sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(\bar{X}) Y_j + f^d(\bar{X}) = 0$, for all $f \in I(V)$.

proved in [**7**], proposition (3.36). The last assertion was mentioned in [**7**], theorem (4.4) and the discussion following theorem (4.4). □

It is well-known that a differential field of characteristic zero is pseudo-differentially closed[10] if and only if it satisfies condition (2) of the above equivalence. As Pillay and Polkowska show in [**53**], proposition (5.6), the class of PAC-substructures of models of DCF_0 is axiomatised by the above axiom scheme (2).

Separably Closed Fields. We fix a prime number p and $e \in \mathbb{N}$. We call $SCF_{e,b}$ the theory of separably closed fields of Ershov invariant e in the language $L(\bar{b})$, which denotes the ring language augmented by constant symbols $\bar{b} = b_1, \ldots, b_e$ for the p-basis. $SCF_{e,b}$ is model complete, stable and eliminates imaginaries. We refer to [**18**] for proofs and more details on separably closed fields.

FACT 5.44 (Chatzidakis). *$SCF_{e,b}$ admits generic automorphisms. The model companion of the $L(\bar{b})_\sigma$-theory of difference fields with p-basis $\bar{b}$ is denoted by $SCFA_{e,b}$ (note that the p-basis is fixed by the automorphism). $SCFA_{e,b}$ satisfies the Independence Theorem over algebraically closed sets and eliminates imaginaries. The fixed field of a model of $SCFA_{e,b}$ is a one-free PAC field with p-basis $\bar{b}$, and to any one-free PAC field k with p-basis $\bar{b}$ there is some model of $SCFA_{e,b}$ whose fixed field is elementarily equivalent to k (in the language $L(\bar{b})$).*

Proof. For the proof of this fact we refer to [**12**]. □

Note that though $SCF_{e,b}$ does not eliminate quantifiers, it serves as an example for the theory developed in the previous sections. For if T denotes a model complete theory in the language L and T_σ has a model companion TA, and if T^M denotes the Morleysation of T, then $(T^M)_\sigma \cup TA$ is the model companion of $(T^M)_\sigma$.

Let us mention that the theory $SCF_{\infty,\lambda}$ of separably closed fields of infinite Ershov invariant in the ring language with λ-functions is complete and eliminates quantifiers (see [**18**]). Also, $SCF_{\infty,\lambda}$ admits generic automorphisms (see [**12**]). However it does not eliminate imaginaries, so we cannot apply our theorem (5.65) in that case.

Though our main interest is in fields, we do not keep quiet about some other stable theories which admit generic automorphisms. We will be very brief and refer the reader to the references given below.

Theories of Finite Morley Rank. Recall that an L-theory T of finite Morley rank is said to have the definable multiplicity property, DMP for short, if T has definable Morley rank and if whenever $\phi(\bar{x}, \bar{a})$ has Morley rank n and Morley degree k there is some L-formula $\psi(\bar{y}) \in \mathrm{tp}_T(\bar{a}/\emptyset)$ such that for all $\bar{a}'$ in some model M of T, $M \models \psi(\bar{a}')$ if and only if $\phi(\bar{x}, \bar{a}')$ has Morley rank n and Morley degree k. An argument of Lascar [**36**] shows that if T is a theory of finite Morley rank with DMP, then TA exists (see [**36**],

[10] see the definition in example (5.33)

example 5). Hasson and Hrushovski [**25**] show that if T is strongly minimal, then TA exists if and only if T has the DMP.

The theory ACF is a particular example, but also the theory of an infinite set as well as the theory of infinite K-vector spaces (for a given field K). Note that for the latter two, TA is stable by proposition (5.22), as in both cases $\mathrm{dcl_T}(A) = \mathrm{acl_T}(A)$ for any parameter set A.

Modules. Chatzidakis and Pillay show in [**16**] that if T is a complete ω-stable theory of modules, that TA exists. TA is stable in this case, because any model (M, σ) of T_σ can by viewed again as a module over $R[\sigma, \sigma^{-1}]$ if M is an R-module.

5.4. One-free PAC structures

In this section we wish to generalise theorem (4.2) on pseudo-finite fields to one-free PAC structures of a stable theory. This is done under the assumption that this class is elementary (see theorem (5.47)).

As we have mentioned in section 1.2, the PAC fields form an elementary class. Also, if T is an L-theory of finite Morley rank with the DMP, quantifier elimination and elimination of imaginaries, then the class of $\mathrm{dcl_T}$-closed PAC-substructures K of models of T is elementary. Namely, because of the DMP it is a first order property of the tuple $\bar{m}$ that the formula $\varphi(\bar{x}, \bar{m})$ has multiplicity one, expressed by a quantifier-free formula. So one writes down the L-theory expressing that K is an L-substructure of some model of T and that any degree-one formula (in the sense of T) with parameters in K has a solution in K.

In general however, even if T is stable, the class of PAC-structures is not necessarily elementary (we refer to [**53**] for examples). We fix for the rest of this section a complete stable L-theory T with quantifier elimination and elimination of imaginaries such that TA exists and has also elimination of imaginaries. Our aim is to generalise theorem (4.2) for the class of L-structures that are PAC for T and that are elementarily equivalent (in the language L) to $\mathrm{Fix}(M, \sigma)$ for some $(M, \sigma) \models TA$. We do this under the assumption that this class is elementary, and let Σ denote its common L-theory.

Corollary 5.45. *Let Σ be a consistent L-theory whose models are precisely those L-structures K that are PAC for T and for which there is some model (M, σ) of TA such that $K \equiv_L \mathrm{Fix}(M, \sigma)$. Then Σ is a simple theory. If T is superstable, then Σ is supersimple.*

Proof. By definition of Σ, any model $K \models \Sigma$ is elementarily equivalent as an L-structure to $\mathrm{Fix}(M, \sigma)$ for some model (M, σ) of TA. As simplicity and supersimplicity are preserved under interpretations (see corollary (2.8.11) and remark (2.8.14) of Wagner's book [**71**]), the assertion follows from corollary (5.21). □

Example 5.46. *We have mainly the following examples in mind. As is well-known, in all of them the class of L-structures under consideration is elementary.*

(1) *Let L be the ring language and T be (any completion of) ACF. Then Σ is nothing but the theory of pseudo-finite fields.*
(2) *Let L be the natural language of differential fields and T be DCF_0, the theory of differentially closed fields of characteristic zero. A PAC substructure of some model of T is nothing but a pseudo-differentially closed field of characteristic zero, and the class of one-free pseudo-differentially closed fields of characteristic zero is elementary (see fact (5.43)). Σ is the theory of one-free pseudo-differentially closed differential fields of characteristic zero.*
(3) *Let $e \in \mathbb{N}$ and T be $SCF_{e,b}$, the theory of separably closed fields of Ershov invariant e, in the ring language with constant symbols for the p-basis and λ-functions. As we have seen in example (5.31) a PAC structure for T is nothing but a PAC field of Ershov invariant e. Σ is the theory of one-free PAC fields of Ershov invariant e.*

Generalising (4.2) we wish to prove the following theorem.

THEOREM 5.47. *Let T be a complete stable L-theory with quantifier elimination and elimination of imaginaries. Assume that TA exists and eliminates imaginaries. Further, we assume that Σ is a (consistent) L-theory whose models are precisely the PAC substructures of models of T that are elementarily equivalent to the L-structure $\mathrm{Fix}(M,\sigma)$ for some model (M,σ) of TA.*

Let F_1 and F_2 be models of Σ containing a common L-substructure E. Then $F_1 \equiv_E F_2$ if and only if there is some model M of T and an L-embedding φ of E into M and L-embeddings of F_1 and F_2 into M extending φ such that $\mathrm{acl_T}(E) \cap F_1 \cong_E \mathrm{acl_T}(E) \cap F_2$ as L-structures.

We need some preparation before we give the proof. By assumption any model of Σ is an L-substructures of some model of T, so our observations in section 5.2 on L-substructures of models of some theory with quantifier elimination apply to models of Σ. Let us list for convenience what these observations import into the present situation: Let $K \models \Sigma$. Then K is $\mathrm{dcl_T}$-closed because $K \equiv_L \mathrm{Fix}(M,\sigma)$, for some model (M,σ) of TA, and $\mathrm{Fix}(M,\sigma)$ is $\mathrm{dcl_T}$-closed. If K' is another model of Σ with $K' \preccurlyeq_L K$, then $\mathrm{acl_T}(K') \cap K = K'$. If E is an L-substructure of K with $\mathrm{acl_T}(E) \cap K = E$, then obviously E is $\mathrm{dcl_T}$-closed and thus by lemma (5.35) the natural restriction map $\mathrm{Gal}(K) \longrightarrow \mathrm{Gal}(E)$ is surjective, and that K/E is regular for T. In particular K/K' is regular for T if $K' \preccurlyeq_L K$.

Recall from chapter 1 that a parameter set A in a model of T is called one-free if $\mathrm{Gal}(A) = \widehat{\mathbb{Z}}$. In the same vein we call an L-structure K one-free if it is an L-substructure of some model of T and $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$. Let us note that in the examples of fields above it is an elementary property to be one-free.

LEMMA 5.48. *Let T be a complete stable L-theory with quantifier elimination and elimination of imaginaries. Assume that TA exists and eliminates imaginaries. Further, we assume that Σ is an L-theory whose models*

are precisely the L-structures which are PAC for T and that are elementarily equivalent to the L-structure $\mathrm{Fix}(M,\sigma)$*, for some model (M,σ) of TA. Let $K \models \Sigma$.*

(1) $\mathrm{Gal}(K)$ *is procyclic. If K is $|L|$-saturated, then* $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$.
(2) *If $K \preccurlyeq_L \mathrm{Fix}(M,\sigma)$ for some $(M,\sigma) \models TA$, then* $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$ *if and only if* $\mathrm{dcl_T}\big(\mathrm{acl_T}(K), \mathrm{Fix}(M,\sigma)\big) = \mathrm{dcl_T}\big(\mathrm{Fix}(M,\sigma)\big)$.

Proof. To show (1), we may assume that $K \preccurlyeq_L \mathrm{Fix}(M,\sigma)$ for some model (M,σ) of TA. We abbreviate $F = \mathrm{Fix}(M,\sigma)$. Recall from above that K is $\mathrm{acl_T}$-closed in F. So it follows that the natural restriction map $\mathrm{res} : \mathrm{Gal}(F) \longrightarrow \mathrm{Gal}(K)$ is surjective, whence $\mathrm{Gal}(K)$ is procyclic. To show that $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$ in case K is $|L|$-saturated, we use the following claim.

Claim: Let T be a complete theory with quantifier elimination. Let A be an L-substructure of some model of T whose underlying set is $\mathrm{dcl_T}$*-closed and let $\varphi(\bar{x},\bar{y})$ be an L-formula. Then there is some set $\pi_\varphi(\bar{z})$ of L-formulas such that for any tuple $\bar{a} \in A$, π_φ is realised by $\bar{a}$ in the L-structure A if and only if $\varphi(\bar{x},\bar{a})$ is a complete consistent $L(A)$-formula in the sense of T.*

Proof of the claim. The proof is immediate, so we omit it. □

Now let $n \in \mathbb{N}$. By lemma (1.9) we have to show that there is some L-formula $\varphi(\bar{x},\bar{z})$ and some $\bar{a} \in K$ such that $\varphi(\bar{x},\bar{a})$ is a complete $L(K)$-formula with exactly n solutions in a model of T containing K, because $\mathrm{Gal}(K)$ is procyclic.

As $\mathrm{Gal}(F) = \widehat{\mathbb{Z}}$ by proposition (5.40), it follows from lemma (1.9) that there is $\varphi(\bar{x},\bar{z}) \in L$ and $\bar{m} \in F$ such that $\varphi(\bar{x},\bar{m})$ is a complete $L(F)$-formula in the sense of T with exactly n solutions in M. Let $\delta_n(\bar{z})$ be a quantifier-free L-formula such that $M \models \delta_n(\bar{c})$ if and only if $\varphi(\bar{x},\bar{c})$ has exactly n solutions in M. Then, as F is an L-substructure of M, we see that $\bar{m}$ realises $\{\delta_n(\bar{z})\} \cup \pi_{\delta_n}(\bar{z})$ in F, where π_{δ_n} is the set of L-formulae given by the claim. As $K \preccurlyeq_L F$ and because K is $|L|$-saturated, there is some realisation of $\{\delta_n(\bar{z})\} \cup \pi_{\delta_n}(\bar{z})$ in K. We have shown that $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$.

To prove (2), let (M,σ) be a model of TA with $K \preccurlyeq_L \mathrm{Fix}(M,\sigma)$. Again we abbreviate $F = \mathrm{Fix}(M,\sigma)$. We have just seen that $\mathrm{Gal}(K)$ is procyclic and that $\mathrm{res} : \mathrm{Gal}(F) \longrightarrow \mathrm{Gal}(K)$ is surjective. Clearly $\mathrm{dcl_T}(\mathrm{acl_T}(K), F) = \mathrm{acl_T}(F)$ if and only if the automorphism group $\mathrm{Aut}_T(\mathrm{acl_T}(F)/\mathrm{acl_T}(K), F)$ is trivial. By what has just been said, this is equivalent to res be an isomorphism, as any $\alpha \in \mathrm{Aut}_T(\mathrm{acl_T}(F)/\mathrm{acl_T}(K), F)$ restricts to the identity in $\mathrm{Gal}(K)$. By lemma (1.4) this in turn is equivalent to $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$. □

Proof of theorem (5.47). Let F_1 and F_2 be two models of Σ and E be a common L-substructure. Clearly $\mathrm{acl_T}(E) \cap F_1 \cong_E \mathrm{acl_T}(E) \cap F_2$ in case $F_1 \equiv_E F_2$, because by quantifier elimination of T, if F is a model of Σ containing E, and M is a model of T containing F, then any $a \in F$ which is algebraic over E inside M is algebraic over E inside F.

For the converse, we may assume that E is $\mathrm{acl_T}$-closed in F_1 and in F_2. Then F_1/E and F_2/E are regular for T by the remarks preceding lemma

(5.48). Without loss we may assume that F_2 is $|L|$-saturated, so $\mathrm{Gal}(F_2) = \widehat{\mathbb{Z}}$ by lemma (5.48.1). Choose a sufficiently saturated elementary extension Ω_2 of F_2, contained in some sufficiently saturated model of T. Then Ω_2 is PAC for T because $\Omega_2 \models \Sigma$. Furthermore Ω_2/F_2 and Ω_2/E are regular for T, again by the remarks preceding lemma (5.48). E is $\mathrm{dcl_T}$-closed because F_1 is, so $\mathrm{tp}_T(F_1/E)$ is stationary and we may assume that F_1 is independent from Ω_2 over E (in the sense of T). Thus F_1 is independent from F_2 over E. We choose topological generators σ_1 and σ_2 of $\mathrm{Gal}(F_1)$ and $\mathrm{Gal}(F_2)$ respectively, both extending the same topological generator of $\mathrm{Gal}(E)$. Further we choose an extension τ of σ_2 to $\mathrm{acl_T}(\Omega_2)$ that topologically generates $\mathrm{Gal}(\Omega_2)$. Because $\mathrm{acl_T}(F_1)$ and $\mathrm{acl_T}(F_2)$ are independent over $\mathrm{acl_T}(E)$, it follows from proposition (5.3) that $\sigma_1 \cup \sigma_2$ is elementary. We choose a lift σ_3 of $\sigma_1 \cup \sigma_2$ to $\mathrm{acl_T}(\mathrm{acl_T}(F_1), \mathrm{acl_T}(F_2)) = \mathrm{acl_T}(F_1, F_2)$ and let K denote $\mathrm{Fix}(\mathrm{acl_T}(F_1, F_2), \sigma_3)$.

Clearly K is $\mathrm{dcl_T}$-closed. σ_3 extends σ_2, so $\mathrm{Gal}(K) = \widehat{\mathbb{Z}}$. For the same reason F_2 is $\mathrm{acl_T}$-closed in K, hence the extension K/F_2 is regular for T. By lemma (5.35) $\mathrm{tp}_T(K/F_2)$ is stationary and so we can embed K over F_2 into Ω_2 because Ω_2 is PAC for T and sufficiently saturated. We denote the image by K'. K' is $\mathrm{dcl_T}$-closed because K is. Furthermore, τ restricts to an element of $\mathrm{Gal}(K')$. As the restriction maps $\mathrm{Gal}(\Omega_2) \longrightarrow \mathrm{Gal}(F_2)$ and $\mathrm{Gal}(K') \longrightarrow \mathrm{Gal}(F_2)$ are isomorphisms, it follows that the restriction of τ to $\mathrm{acl_T}(K')$ topologically generates $\mathrm{Gal}(K')$. This implies that the extension Ω_2/K' is regular for T.[11] As in the proof of theorem (4.2) the assertion follows by back-and-forth. □

Corollary 5.49. *Let F_1 and F_2 be models of Σ.*

1. *$F_1 \equiv F_2$ if and only if there are embeddings of F_1 and F_2 into models of T such that $\mathrm{acl_T}(\emptyset) \cap F_1 \cong \mathrm{acl_T}(\emptyset) \cap F_2$ as L-structures.*
2. *Let further E be a common L-substructure and $\bar{a} \in F_1$ and $\bar{b} \in F_2$ be tuples (of the same length). Then $\mathrm{tp}_{F_1}(\bar{a}/E) = \mathrm{tp}_{F_2}(\bar{b}/E)$ if and only if there are embeddings of F_1 and F_2 into models of T and an E-isomorphism of L-structures*
$$\mathrm{acl_T}(E, \bar{a}) \cap F_1 \xrightarrow{\ \varphi\ } \mathrm{acl_T}(E, \bar{b}) \cap F_2$$
with $\varphi(\bar{a}) = \bar{b}$.
3. *Let $E \subseteq F$ be models of Σ, both contained in some model of T. Then $E \preccurlyeq F$ if and only if $\mathrm{acl_T}(E) \cap F = E$ if and only if F/E is regular for T.*

Corollary 5.50. *Let $F \models \Sigma$ and A be a subset of F. Assume F is embedded in some model of T. Then the model-theoretic closure of A in the L-structure F is*
$$\mathrm{acl}_F(A) = \mathrm{acl_T}(A) \cap F\ .$$

Proof. We may assume that F is sufficiently saturated. Denote $A_0 = \mathrm{acl_T}(A) \cap F$ and let $a \in F \setminus A_0$. Let $F_0 = \mathrm{acl_T}(A_0, a) \cap F$. The extension F_0/A_0 is regular by the remarks preceding lemma (5.48), so $\mathrm{tp}_T(F_0/A_0)$ is

[11] Note that this was the Embedding Lemma in section 4.1.

stationary. We can choose an infinite sequence $(F_i)_{i<\omega}$ of realisations of $\mathrm{tp}_T(F_0/A_0)$ that are pairwise independent over A_0 in the sense of T. As A_0 is $\mathrm{acl_T}$-closed in every F_i, it follows that $F_i \cap F_j = A_0$ whenever $i \neq j$. All F_i are conjugate over A_0 (in $\mathfrak{C}$), so they are isomorphic as autonomous L-structures. We denote a_i the image of a under these isomorphisms. Now look at $D = \mathrm{dcl_T}(F_i : i < \omega) \subset \mathfrak{C}$. As $\mathrm{tp}_T(F_0/A_0)$ is stationary, so is its ω-fold free amalgam, which is $\mathrm{tp}_T(F_i : i < \omega \,/\, A_0)$. Hence D/A_0 is regular for T. Because F is PAC for T and sufficiently saturated, we may assume that $D \subset F$, and that $\mathrm{acl_T}(F_i) \cap F = F_i$ for all $i \in \mathbb{N}$. By (2) of corollary (5.49) it follows that a is not algebraic over A_0 in the sense of F. □

Note that as special cases, we obtain theorem (4.2), as well as the analogues of that theorem for the class of one-free PAC fields of fixed Ershov invariant $e \in \mathbb{N}$, as well as the analogue for the class of one-free pseudo-differentially closed differential fields of characteristic zero.

We have obtained theorem (5.47) quite recently. We are sure it can be pushed further, for example to bounded PAC structures of stable theories. For time reasons this will be done elsewhere.

5.5. Conservative Embedding

In the first part of this section we introduce the notion of conservative embedding of one structure into another. Loosely speaking, the universe of P is conserved when plunged into M. It will play a key rôle in our construction of generic automorphisms in section 5.6. We first give the definition, and then discuss examples and some first properties. In the second part of the section we show that the fixed structure $\mathrm{Fix}(M, \sigma)$ is conservatively embedded in the model (M, σ) of TA over L-elementary substructures K with

$$\mathrm{dcl_T}(\mathrm{acl_T}(K), \mathrm{Fix}(M, \sigma)) = \mathrm{acl_T}(\mathrm{Fix}(M, \sigma)) \ .$$

5.5.1. Definition and Examples. Consider an extension of languages $L \subset L'$ and let M be an L'-structure. If P is a substructure of M with respect to the language L, then a priori the structure induced on P from the L'-structure M is richer than the L-structure on P. If this is not the case, we call P conservatively embedded in M:

Definition 5.51. *Let L and L' be first-order languages with $L \subset L'$ and assume that P is an L-substructure of the L'-structure M.*

(1) *We say that P is conservatively embedded in M if every subset of (some cartesian power of) P that is L'-definable in the L'-structure M using parameters from M is L-definable in the L-structure P using parameters from P.*
(2) *If A is a subset of P, we say that P is conservatively embedded over A in M if every subset X of (some cartesian power of) P that is L'-definable in the L'-structure M using parameters from A, is L-definable in the L-structure P using parameters from A.*

If P is conservatively embedded over A in M, it is not necessarily conservatively embedded in M: for if $X \subset P$ cannot be defined over A in M, there is a priori no reason for it be definable in the structure P at all, whatever parameters we allow. In the definition we allow M to define X only with parameters from A. In return we keep control over the parameters needed to define X in P.

While part (1) of the above definition serves just as a compact way of speaking, we want to emphasise with part (2) on the property which will be crucial in the proofs of section 5.6.

REMARK 5.52. *It follows immediately from the definition that if an L-structure P is conservatively embedded in the L'-structure M and L'-definable in M without parameters, then it is stably embedded.*

The principal example of a conservatively embedded substructure we have in mind is the fixed field of a generic automorphism.

EXAMPLE 5.53. *Let $(\Omega, \sigma) \models ACFA$. Then* $\mathrm{Fix}(\Omega, \sigma)$ *is conservatively embedded in (Ω, σ) (see [**14**], proposition (1.11)). If Ω has positive characteristic and* Frob *denotes the Frobenius automorphism, then* $\mathrm{Fix}(\Omega, \sigma\mathrm{Frob}^k)$ *is conservatively embedded for all $k \in \mathbb{Z}$ (see [**15**], proposition (7.1)).*

EXAMPLE 5.54. *Let $(\Omega, d, \sigma) \models DCFA$. Then* $\mathrm{Fix}(\Omega, d, \sigma)$ *is conservatively embedded in (Ω, d, σ) (see [**7**], proposition (4.6)).*

EXAMPLE 5.55. *Let e be a natural number and $(\Omega, \sigma) \models SCFA_e$. Then* $\mathrm{Fix}(\Omega, \sigma)$ *is conservatively embedded in (Ω, σ) (see [**12**], proposition (4.3)).*

Generalising these results, we will prove in (5.64) that if TA eliminates imaginaries, then $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded in (M, σ) for any model (M, σ) of TA and for any L-automorphism ϕ that is L-definable without parameters. Indeed, this follows immediately from proposition (5.63), which states that $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded in (M, σ) over any L-elementary substructure $K \preccurlyeq_L \mathrm{Fix}(M, \sigma\phi)$ with

$$\mathrm{dcl_T}\big(\mathrm{acl_T}(K), \mathrm{Fix}(M, \sigma\phi)\big) = \mathrm{acl_T}\big(\mathrm{Fix}(M, \sigma\phi)\big)\,.$$

As in the above examples, the condition on the definable and algebraic closure of the involved structures is always satisfied, this implies in particular that, in the above examples, the fixed field is conservatively embedded over elementary substructures.

Unfortunately not every field of interest definable in our context is conservatively embedded.

EXAMPLE 5.56. *Let again $(\Omega, \sigma) \models ACFA$. Then* $\mathrm{Fix}(\Omega, \sigma)$ *is a proper subfield of* $\mathrm{Fix}(\Omega, \sigma^2)$ *that is not definable in the pure field* $\mathrm{Fix}(\Omega, \sigma^2)$. *This follows from proposition (2.12) of [**13**], which states that if F is a pseudo-finite field and S is an infinite subset of F definable using parameters, any element of F is of the form $a + b + cd$ for suitable $a, b, c, d \in S$.*

EXAMPLE 5.57. *Let $(\Omega, d, \sigma) \models DCFA$ and consider the (difference) field of constants $\mathcal{C}$ (defined by the formula $d(x) = 0$). $\mathcal{C}$ is not stably*

embedded in (Ω, d, σ) *(see [7], proposition (4.5)). So by (5.52) it cannot be conservatively embedded.*

For $\emptyset$-definable L-substructures, being conservatively embedded over a subset is preserved under elementary extensions:

LEMMA 5.58. *Let* $M_1 \preccurlyeq M_2$ *be an elementary extension of* L'*-structures and* $\varphi \in L'$ *a formula without parameters. Assume that* $\varphi(M_1)$ *is an* L*-substructure of* M_1 *for some* $L \subset L'$ *and* $A \subset \varphi(M_1)$*. Then* $\varphi(M_1)$ *is conservatively embedded in* M_1 *over* A *if and only if so is* $\varphi(M_2)$ *in* M_2*.*

Proof. The proof is straightforward using relativisation of quantifiers. □

5.5.2. Conservative Embedding of the Fixed Structure. The aim of this section is to prove proposition (5.63), which states that if T is a stable L-theory with quantifier elimination and elimination of imaginaries such that TA exists and eliminates imaginaries, and if (M, σ) is a model of TA, then $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded over every L-elementary substructure K with

$$\mathrm{dcl_T}\big(\,\mathrm{acl_T}(K), \mathrm{Fix}(M,\sigma)\big) = \mathrm{acl_T}\big(\mathrm{Fix}(M,\sigma)\big)\,.$$

Notice that in the case of fields, this last condition is always satisfied. For example if k and F are pseudo-finite fields with $k \preccurlyeq F$, then $k^{\mathrm{alg}}F = F^{\mathrm{alg}}$. The reason is that the absolute Galois groups are $\widehat{\mathbb{Z}}$.

We have seen in proposition (4.18) what the induced structure on the fixed field $\mathrm{Fix}(\Omega, \sigma)$ from models (Ω, σ) of $ACFA$ is. With the notation as in proposition (4.18), if $k \preccurlyeq \mathrm{Fix}(\Omega, \sigma)$ considered as pure fields, then all $e_{j,n}$ are already contained in k^{eq}. So knowing that $\mathrm{Fix}(\Omega, \sigma)$ is stably embedded is already enough in this case. Working without fields, we have no explicit description of the induced structure. Proposition (5.63) bypasses this problem.

That the above condition is in fact necessary follows from the next proposition.

PROPOSITION 5.59. *Let* T *eliminate imaginaries and* $(N, \sigma) \preccurlyeq (M, \sigma)$ *be models of* T_σ*. Then* $\mathrm{dcl_T}\big(\,\mathrm{acl_T}(\mathrm{Fix}(N,\sigma))\,,\,\mathrm{Fix}(M,\sigma)\,\big) = \mathrm{acl_T}\big(\,\mathrm{Fix}(M,\sigma)\,\big)$.

We note that if (N, σ) and (M, σ) were models of TA, the proposition would follows from lemma (5.48) and proposition (5.40).

Proof. We denote $F_M = \mathrm{Fix}(M, \sigma)$ and $F_N = \mathrm{Fix}(N, \sigma)$. The automorphism σ (of M) restricts to topological generators of $\mathrm{Gal}(F_M)$ and $\mathrm{Gal}(F_N)$ respectively because $F_M = \mathrm{Fix}(\mathrm{acl_T}(F_M), \sigma)$ and $F_N = \mathrm{Fix}(\mathrm{acl_T}(F_N), \sigma)$. Hence both $\mathrm{Gal}(F_M)$ and $\mathrm{Gal}(F_N)$ are procyclic and the restriction map $\mathrm{Gal}(F_M) \xrightarrow{\mathrm{res}} \mathrm{Gal}(F_N)$ is surjective. Thus $\mathrm{Aut}_T\big(\mathrm{acl_T}(F_M)/\mathrm{acl_T}(F_N), F_M\big)$ is trivial if and only if res is an isomorphism. So by lemma (1.4) and corollary (1.9), it suffices to show that for all $n \in \mathbb{N}$ and $\bar{b} \in \mathrm{acl_T}(F_M)$ of degree n over F_M there is $\bar{c} \in \mathrm{acl_T}(F_N)$ of degree n over F_N.

To see this, note that as σ generates $\mathrm{Gal}(F_M)$ and $\bar{b}$ has degree n over F_M, we have

$$(M,\sigma) \models \exists \bar{x} \;\; \sigma^n(\bar{x}) = \bar{x} \wedge \bigwedge_{i=1}^{n-1} \sigma^i(\bar{x}) \neq \bar{x}$$

and thus

$$(N,\sigma) \models \exists \bar{x} \;\; \sigma^n(\bar{x}) = \bar{x} \wedge \bigwedge_{i=1}^{n-1} \sigma^i(\bar{x}) \neq \bar{x} \;,$$

and we are done. □

LEMMA 5.60. *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries and let ϕ be an automorphism of T which is L-definable over $\emptyset$. Assume that TA exists and eliminates imaginaries. If $(M,\sigma) \models TA$ and $K \preccurlyeq_L \mathrm{Fix}(M,\sigma\phi)$, then $\mathrm{dcl}_\sigma(K) = K$ and $\mathrm{acl}_\sigma(K) = \mathrm{acl}_\mathrm{T}(K)$. Furthermore $\mathrm{acl}_\mathrm{T}(K) \cap \mathrm{Fix}(M,\sigma\phi) = K$.*

Proof. $\mathrm{Fix}(M,\sigma\phi)$ is an L-substructure of M and ϕ is quantifier-free definable by quantifier elimination of T. So $\sigma|_{\mathrm{Fix}(M,\sigma\phi)} = \phi^{-1}$ is an L-definable automorphism of the L-structure $\mathrm{Fix}(M,\sigma\phi)$. As $K \preccurlyeq_L \mathrm{Fix}(M,\sigma\phi)$ it follows that $\sigma(K) = K$, so $\mathrm{acl}_\sigma(K) = \mathrm{acl}_\mathrm{T}(K)$ by corollary (5.12). As σ is an L_σ-isomorphism, $\mathrm{Fix}(M,\sigma\phi)$ is dcl_σ-closed, and again because $\sigma|_{\mathrm{Fix}(M,\sigma\phi)} = \phi^{-1}$ and $K \preccurlyeq_L \mathrm{Fix}(M,\sigma\phi)$ we conclude that $\mathrm{dcl}_\sigma(K) = K$.

If $a \in M$ is algebraic over K and fixed by $\sigma\phi$, then a is algebraic over K in the L-substructure $\mathrm{Fix}(M,\sigma\phi)$ of M by quantifier elimination of T. □

LEMMA 5.61. *Let T be a stable theory eliminating imaginaries, A a set of parameters, $p \in S(\mathrm{acl}(A))$ and $\beta \in \mathrm{Aut}(\mathfrak{C}/A)$ an automorphism of the monster model of T over A. Then $\beta(p) = p$ if and only if $p|_{\mathrm{acl}(A)\cap\mathrm{Fix}(\beta)}$ is stationary.*

Proof. $\beta(p) = p$ if and only if β leaves the canonical basis of p pointwise fixed. By elimination of imaginaries, the latter is equivalent to the canonical basis be contained in $\mathrm{acl}(A) \cap \mathrm{Fix}(\beta)$. □

LEMMA 5.62. *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries and let ϕ be an automorphism of T which is L-definable over $\emptyset$. Assume that TA exists and eliminates imaginaries.*

Let $(M,\sigma) \models TA$ be sufficiently saturated. If $K \preccurlyeq_L \mathrm{Fix}(M,\sigma\phi)$ with $\mathrm{dcl}_\mathrm{T}\big(\mathrm{acl}_\mathrm{T}(K), \mathrm{Fix}(M,\sigma\phi)\big) = \mathrm{acl}_\mathrm{T}\big(\mathrm{Fix}(M,\sigma\phi)\big)$ then the natural restriction map

$$\mathrm{res} : \mathrm{Aut}_{L_\sigma}\big((M,\sigma)/K\big) \longrightarrow \mathrm{Aut}_L\big(\,\mathrm{Fix}(M,\sigma\phi)/K\,\big)$$

is surjective. Here $\mathrm{Aut}_L\big(\,\mathrm{Fix}(M,\sigma\phi)/K\,\big)$ denotes the group of automorphisms over K of the L-structure $\mathrm{Fix}(M,\sigma\phi)$.

Proof. We abbreviate $F = \mathrm{Fix}(M,\sigma\phi)$. By quantifier elimination of T and as F is an L-substructure of M, any automorphism $\alpha \in \mathrm{Aut}_L(\,F/K\,)$ is a partial elementary map in the sense of T. It commutes with $\sigma|_F$ because $\sigma|_F = \phi^{-1}$ and ϕ is an L-definable over $\emptyset$ automorphism of F.

We are going to lift α to a permutation $\tilde{\alpha}$ of $\mathrm{acl_T}(F)$ that is elementary in the sense of T and commutes with σ. As $\mathrm{acl_T}(F) = \mathrm{acl}_\sigma(F)$ by lemma (5.60), remark (5.9) then implies that $\tilde{\alpha}$ is elementary in the sense of TA. Then in particular α is an automorphism of the induced structure from (M, σ) on F. So by saturation of (M, σ), lemma (4.15) implies that α lifts to an automorphism of (M, σ) over K.

To lift α we work entirely in T. α is an elementary permutation of the set F and commutes with σ. Let $\bar{a} \in F$. As $\mathrm{acl_T}(K) \cap F = K$ by lemma (5.60) and because α leaves K pointwise fixed, it follows from lemma (5.61) that $tp_T(\bar{a}/K)$ is stationary. So $tp_T(\alpha(\bar{a})/K)$ is stationary too and equals $tp_T(\bar{a}/K)$, again because α is the identity on K. As any $\bar{b} \in \mathrm{acl_T}(K)$ is independent from F over K it follows that $tp_T(\bar{a}/K\bar{b}) = tp_T(\alpha(\bar{a})/K\bar{b})$, hence $tp_T(\bar{a}, \bar{b}) = tp_T(\alpha(\bar{a}), \bar{b})$. This shows that the map $\mathrm{id}|_{\mathrm{acl_T}(K)} \cup \alpha$ is elementary. It lifts uniquely to an elementary permutation $\tilde{\alpha}$ of $\mathrm{dcl_T}(\mathrm{acl_T}(K), F)$, which is $\mathrm{acl_T}(F)$ by assumption. $\tilde{\alpha}$ commutes with σ by construction, so we are done. □

Note that this lemma is in a sense stronger than the statement that $\mathrm{Fix}(M, \sigma\phi)$ is stably embedded, since we lift the automorphisms of $\mathrm{Fix}(M, \sigma\phi)$ over K with respect to the L-structure, not the induced structure, see lemma (4.15). However, stable embeddedness of $\mathrm{Fix}(M, \sigma\phi)$ seems not to follow from the statement of the above lemma.

Proposition 5.63. *Let T be a stable theory with quantifier elimination and elimination of imaginaries and let ϕ be an automorphism of T which is L-definable over $\emptyset$. Assume that TA exists and has elimination of imaginaries.*

Let (M, σ) be a model of TA and $K \preccurlyeq_L \mathrm{Fix}(M, \sigma\phi)$. If

$$\mathrm{dcl_T}\big(\mathrm{acl_T}(K), \mathrm{Fix}(M, \sigma\phi)\big) = \mathrm{acl_T}\big(\mathrm{Fix}(M, \sigma\phi)\big),$$

then $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded over K in (M, σ).

Proof. First note that if (N, σ) is an elementary extension of (M, σ), then $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded over K in (M, σ) if and only if $\mathrm{Fix}(N, \sigma\phi)$ is so in (N, σ) by lemma (5.58). Furthermore it follows from proposition (5.59) that $\mathrm{dcl_T}\big(\mathrm{acl_T}(K), \mathrm{Fix}(N, \sigma\phi)\big) = \mathrm{acl_T}\big(\mathrm{Fix}(N, \sigma\phi)\big)$. So we may assume that (M, σ) is sufficiently saturated.

Let X be a subset of (some cartesian power of) $\mathrm{Fix}(M, \sigma\phi)$ that is K-definable in (M, σ). By lemma (5.62) we can lift any automorphism of $\mathrm{Fix}(M, \sigma\phi)$ over K to an automorphism of (M, σ) over K, which shows that for any tuple $a \in \mathrm{Fix}(M, \sigma\phi)$ the type of a over K in the sense of $\mathrm{Fix}(M, \sigma\phi)$ (relativised to $\sigma\phi(x) = x$) implies modulo the theory of (M, σ) the type of a over K in (M, σ). Hence by compactness X is definable in the L-structure $\mathrm{Fix}(M, \sigma\phi)$ using parameters from K. □

As a special case of proposition (5.63) we obtain the following result. It was proved before in the cases of fields: when T is ACF by Chatzidakis, Hrushovski and Peterzil in [**15**], for separably closed fields with generic automorphism by Chatzidakis in [**12**], when T is DCF_0 by Bustamante-Medina in [**7**] and for strongly minimal T by Pillay in [**52**].

COROLLARY 5.64. *Let T be a stable L-theory with quantifier elimination and elimination of imaginaries and let ϕ be an automorphism of T which is L-definable over $\emptyset$. Assume that TA exists and eliminates imaginaries. Let (M, σ) be a model of TA. If TA eliminates imaginaries then* $\mathrm{Fix}(M, \sigma\phi)$ *is conservatively embedded in* (M, σ).

As we will see in the next section, the converse in the above proposition is also true for countable T and sufficiently saturated models (M, σ) of TA, and for totally transcendental T and any model (M, σ) of TA: namely in either case, if $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded over K, then

$$\mathrm{dcl_T}(\,\mathrm{acl_T}(K), \mathrm{Fix}(M, \sigma\phi)\,) = \mathrm{acl_T}(\mathrm{Fix}(M, \sigma\phi))\,.$$

5.6. Prescribed Fixed Structures

In this section we prove the main theorems of this chapter, theorems (5.65) and (5.68) and then discuss some first variants.

THEOREM 5.65. *Let T be a countable complete stable L-theory with quantifier elimination and elimination of imaginaries and ϕ be an L-automorphism of T which is L-definable without parameters. Assume that TA exists and has elimination of imaginaries.*

Let (M, σ) be a model of TA and $K \preccurlyeq_L \mathrm{Fix}(M, \sigma\phi)$ be an L-elementary substructure. If $\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded over K in (M, σ), then there is some model $(N, \sigma) \equiv (M, \sigma)$ with $\mathrm{Fix}(N, \sigma\phi) = K$.

Proof. In view of lemma (5.58) we may assume that (M, σ) is sufficiently saturated.[12] We construct (N, σ) with the aid of the following (standard) chain argument. Starting with $N_0 = \mathrm{acl}_\sigma(K)$, whose set of elements fixed by $\sigma\phi$ is precisely K by (5.60), we build an ascending chain $(N_\nu)_{\nu<\omega}$ of acl_σ-closed L-substructures of (M, σ) with the property that

- if $\varphi(\bar{x})$ is a quantifier-free consistent $L_\sigma(N_\nu)$-formula then φ has a realisation in $N_{\nu+1}$ and
- $\mathrm{Fix}(N_\nu, (\sigma\phi)|_{N_\nu}) = K$ for all $\nu < \omega$.

Then we let $N = \bigcup N_\nu$. By model completeness of TA, any L_σ-formula is equivalent modulo TA to an existential formula. So by Tarski's Test $(N, \sigma|_N)$ will be an elementary substructure of (M, σ), with $\mathrm{Fix}(N, \sigma\phi) = K$ by construction.

The only delicate point is to ensure $\mathrm{Fix}(N_\nu, \sigma\phi) = K$ for all $\nu < \omega$. We handle this using the following proposition.

PROPOSITION 5.66. *Let T be a countable stable L-theory with quantifier elimination and elimination of imaginaries. Suppose that TA exists and has elimination of imaginaries. Let $(M, \sigma) \models TA$ and A be an acl_σ-closed subset of (M, σ) such that $\mathrm{Fix}(A, \sigma\phi) \preccurlyeq_L \mathrm{Fix}(M, \sigma\phi)$, where ϕ is an*

[12] Passing to a sufficiently saturated elementary extension is not necessary if T is totally transcendental, see theorem (5.69) below.

L-automorphism of M which is L-definable over $\emptyset$. If $\mathrm{Fix}(M,\sigma\phi)$ *is conservatively embedded over* $\mathrm{Fix}(A,\sigma\phi)$ *in* (M,σ)*, then*

$$\mathrm{acl}_\sigma(A,\bar a)\cap \mathrm{Fix}(M,\sigma\phi)=\mathrm{Fix}(A,\sigma\phi)$$

for any tuple $\bar a\in M$ *whose quantifier-free* L_σ*-type* $\mathrm{qftp}_\sigma(\bar a/A)$ *over* A *is locally isolated.*

Proof of 5.66. In view of lemma (5.58) we may assume that (M,σ) is sufficiently saturated. Let $\bar a$ be a tuple in M whose quantifier-free L_σ-type is locally isolated. We abbreviate $\mathrm{Fix}(A,\sigma\phi)$ by K and show first that

$$\mathrm{dcl_T}(\mathrm{cl}_\sigma(A,\bar a))\cap \mathrm{Fix}(M,\sigma\phi)=K\ .$$

Let $b\in \mathrm{dcl_T}(\mathrm{cl}_\sigma(A,\bar a))$ be fixed by $\sigma\phi$. Then b is L-definable over $A,\sigma^{-n}(\bar a),\dots,\sigma^{-1}(\bar a),\bar a,\sigma(\bar a),\dots,\sigma^n(\bar a)$ for some $n\in\mathbb{N}$, and, as $\sigma\phi(b)=b$, applying $(\sigma\phi)^n$ we see that b is already L-definable over $A,\bar a,\dots,\sigma^n(\bar a)$ for some $n\in\mathbb{N}$ since $\sigma\phi$ is an L_σ-isomorphism. So there is some L-formula

$$\psi(\bar x_0,\bar x_1,\dots,\bar x_n;z,\bar y)$$

and $\bar e\in A$ such that $\psi(\bar a,\sigma(\bar a),\dots,\sigma^n(\bar a);z,\bar e)$ defines b in M. As T eliminates quantifiers, we may assume that ψ is quantifier-free. Let

$$\Delta=\{\,\psi(\bar x,\sigma(\bar x),\dots,\sigma^n(\bar x);z,\bar y)\ ,\ \sigma\phi(z)=z\,\}$$

and choose an $L_\sigma(A)$-formula $\delta(\bar x)\in\mathrm{qftp}_\sigma(\bar a/A)$ isolating $\mathrm{qftp}_\sigma(\bar a/A)|_\Delta$.

Consider the L_σ-formula

$$\Phi(z)\ =\ \exists\bar x\ \ \Big(\delta(\bar x)\ \wedge\ \psi(\bar x,\sigma(\bar x),\dots,\sigma^n(\bar x);z,\bar e)\ \wedge\ \sigma\phi(z)=z\Big)$$

with parameters from A and let X be the subset of $\mathrm{Fix}(M,\sigma\phi)$ defined by Φ. We claim that X is L_σ-definable in (M,σ) over $A\cap\mathrm{Fix}(M,\sigma\phi)$. To see this, note that both A and $\mathrm{Fix}(M,\sigma\phi)$ are dcl_σ-closed. TA eliminates imaginaries by assumption, so on the one hand $\mathrm{Fix}(M,\sigma\phi)$ is stably embedded by remark (5.28), whence the canonical parameter of X is in $\mathrm{Fix}(M,\sigma\phi)$. On the other hand the canonical parameter of X is also in A. Thus X is L_σ-definable in (M,σ) over $A\cap\mathrm{Fix}(M,\sigma\phi)=K$.

By assumption $\mathrm{Fix}(M,\sigma\phi)$ is conservatively embedded over K in (M,σ), so it follows that X is L-definable over K in the L-structure $\mathrm{Fix}(M,\sigma\phi)$.

X is non-empty because $b\in X$, hence $\mathrm{Fix}(M,\sigma\phi)\models\exists z\ z\in X$. But $K\preccurlyeq_L\mathrm{Fix}(M,\sigma\phi)$, so $K\models\exists z\ z\in X$, whence there is $\lambda\in X(K)$.

We have shown that the $L_\sigma(A)$-formula

$$\psi(\bar x,\sigma(\bar x),\dots,\sigma^n(\bar x);\lambda,\bar e)$$

is consistent with $\delta(\bar x)$ for some $\lambda\in K$. Thus

$$\psi(\bar x,\sigma(\bar x),\dots,\sigma^n(\bar x);\lambda,\bar e)\in\mathrm{qftp}_\sigma(\bar a/A)$$

and therefore $b=\lambda\in K$, because $\psi(\bar a,\dots,\sigma^n(\bar a);z,\bar e)$ has exactly one solution in M. This shows that $\mathrm{dcl_T}(\mathrm{cl}_\sigma(A,\bar a))\cap\mathrm{Fix}(M,\sigma\phi)=K$.

Finally we show that any tuple $\bar a$ with $\mathrm{dcl_T}(\mathrm{cl}_\sigma(A,\bar a))\cap\mathrm{Fix}(M,\sigma\phi)=K$ has the property that

$$\mathrm{acl}_\sigma(A,\bar a)\cap\mathrm{Fix}(M,\sigma\phi)=K\ .$$

Indeed, by corollary (5.12) we have $\mathrm{acl}_\sigma(A,\bar a) = \mathrm{acl}_{\mathrm{T}}(\mathrm{dcl}_{\mathrm{T}}(\mathrm{cl}_\sigma(A,\bar a)))$, so the next lemma (5.67) implies that any $b \in \mathrm{acl}_\sigma(A,\bar a)$ which is fixed by $\sigma\phi$ is algebraic over

$$\mathrm{dcl}_{\mathrm{T}}(\mathrm{cl}_\sigma(A,\bar a)) \cap \mathrm{Fix}(M,\sigma\phi) = K\ .$$

It follows that $b \in \mathrm{acl}_{\mathrm{T}}(K)$. As A is algebraically closed and contains K we conclude that $b \in A$ and thus, as $\sigma\phi(b) = b$, that $b \in K$. □

Lemma 5.67. *Let T be any theory with elimination of imaginaries and B a definably-closed set. If α is an automorphism of a sufficiently saturated model mapping B into itself and if b algebraic over B and fixed by α, then b is algebraic over $B \cap \mathrm{Fix}(\alpha)$.*

Proof. Choose an $L(B)$-formula ψ isolating the type of b over B. As b is fixed by α, ψ is invariant under α and thus the canonical parameter for ψ is in $B \cap \mathrm{Fix}(\alpha)$. □

To complete the proof of theorem (5.65), let A be an acl_σ-closed subset of M such that $\mathrm{Fix}(A,\sigma\phi) = K$ and $\varphi(\bar x)$ be a consistent quantifier-free $L_\sigma(A)$-formula. TA is quantifier-free stable by lemma (5.23) and countable because T is. By proposition (5.24) and by saturation of (M,σ) we can choose a tuple $\bar a \in (M,\sigma)$ satisfying φ whose quantifier-free type $\mathrm{qftp}_\sigma(\bar a/A)$ over A (in the sense of (M,σ)) is locally isolated. Then proposition (5.66) implies that $\mathrm{acl}_\sigma(A,\bar a) \cap \mathrm{Fix}(M,\sigma\phi) = \mathrm{Fix}(A,\sigma\phi)$. The proof of theorem (5.65) is complete. □

The next two theorems characterise the L-elementary substructures over which $\mathrm{Fix}(M,\sigma\phi)$ is conservatively embedded as exactly those occurring as fixed structures $\mathrm{Fix}(N,\sigma\phi)$ of elementary submodels. Needless to say that theorem (5.68) gives a partial converse to proposition (5.63) for countable languages, whereas theorem (5.69) gives a converse to proposition (5.63) for totally transcendental T.

Theorem 5.68. *Let T be a countable complete stable L-theory with quantifier elimination and elimination of imaginaries and ϕ be an L-automorphism of T which is L-definable without parameters. Assume that TA exists and has elimination of imaginaries.*

Let (M,σ) be a model of TA and $K \preccurlyeq_L \mathrm{Fix}(\bar M,\sigma\phi)$. Assume that (M,σ) is $|K|^+$-saturated. Then the following are equivalent:

1. *There is some $(N,\sigma) \preccurlyeq (M,\sigma)$ with $\mathrm{Fix}(N,\sigma\phi) = K$.*
2. *$\mathrm{Fix}(M,\sigma\phi)$ is conservatively embedded over K in (M,σ).*
3. *$\mathrm{dcl}_{\mathrm{T}}\big(\mathrm{acl}_{\mathrm{T}}(K), \mathrm{Fix}(M,\sigma\phi)\big) = \mathrm{acl}\big(\mathrm{Fix}(M,\sigma\phi)\big)$.*

Proof. (3) implies (2) is proposition (5.63) and *(2) implies (1)* is (the proof of) theorem (5.65): we only needed that (M,σ) is $|K|^+$-saturated. To see that *(1) implies (3)* let $(N,\sigma) \preccurlyeq (\bar M,\sigma)$ and note that then $(N,\sigma\phi) \preccurlyeq (M,\sigma\phi)$. Both $(N,\sigma\phi)$ and $(M,\sigma\phi)$ being models of T_σ, the assertion follows from proposition (5.59). □

Let us examine once more the proof of theorem (5.65). The only place where we use saturation of (M, σ) is where we realise a locally isolated quantifier-free type containing the formula $\varphi(\bar{x})$. As mentioned earlier in lemma (5.23), TA is quantifier-free totally transcendental if T is totally transcendental. So in this case proposition (5.24) allows us to choose a tuple $\bar{a}$ realising $\varphi(\bar{x})$ whose quantifier-free type is even isolated, rather than locally isolated only. For such $\bar{a}$, following the proof of (5.66) word by word, we then obtain $\mathrm{acl}_\sigma(A\bar{a}) \cap \mathrm{Fix}(M, \sigma\phi) = K$. We have proved the following theorem, in which no countability and no saturation is needed.

THEOREM 5.69. *Let T be a complete totally transcendental L-theory with quantifier elimination and elimination of imaginaries and ϕ be an L-automorphism of T which is L-definable without parameters. Assume that TA exists and has elimination of imaginaries.*

Let (M, σ) be a model of TA and $K \preccurlyeq_L \mathrm{Fix}(\bar{M}, \sigma\phi)$. Then the following are equivalent:

1. *There is some $(N, \sigma) \preccurlyeq (M, \sigma)$ with $\mathrm{Fix}(N, \sigma\phi) = K$.*
2. *$\mathrm{Fix}(M, \sigma\phi)$ is conservatively embedded over K in (M, σ).*
3. *$\mathrm{dcl_T}\big(\mathrm{acl_T}(K), \mathrm{Fix}(M, \sigma\phi)\big) = \mathrm{acl}\big(\mathrm{Fix}(M, \sigma\phi)\big)$.*

We have also proved the following theorem, which in the case when T is ACF was proved independently by Zoé Chatzidakis (unpublished). In view of proposition (5.63), its proof is an easy consequence of the proof of theorem (5.65).

COROLLARY 5.70. *Let T be a countable complete stable L-theory with quantifier elimination and elimination of imaginaries. Assume that TA exists and has elimination of imaginaries.*

Let $(\phi_i)_{i \in I}$ be a family of L-automorphisms of T, with each ϕ_i L-definable over $\emptyset$, and (M, σ) be a model of TA. If A is an acl_σ-closed subset of (M, σ) such that for all $i \in I$, $\mathrm{Fix}(A, \sigma\phi_i) \preccurlyeq_L \mathrm{Fix}(M, \sigma\phi_i)$ and

$$\mathrm{dcl_T}\big(\mathrm{acl_T}(\mathrm{Fix}(A, \sigma\phi_i)), \mathrm{Fix}(M, \sigma\phi_i)\big) = \mathrm{acl_T}\big(\mathrm{Fix}(M, \sigma\phi_i)\big)\,,$$

then there is a model $(N, \sigma) \equiv (M, \sigma)$ of TA such that for all $i \in I$

$$\mathrm{Fix}(N, \sigma\phi_i) = \mathrm{Fix}(A, \sigma\phi_i)\ .$$

If T is totally transcendental, we can choose (N, σ) to be an elementary submodel of (M, σ).

We end this section noting that the countability of L in the above theorems is used only to ensure that the locally isolated quantifier-free types are dense. Newelski shows in [**48**] and [**49**] that it is consistent with ZFC that for any stable theory T of cardinality less than $2^{\aleph_0}$ with $\kappa(T) \leq \aleph_1$ and for any parameter set A the locally isolated types are dense in $S_T(A)$. It follows from this that there are models of ZFC in which our theorem is true under the assumption that $|T| < 2^{\aleph_0}$ and $\kappa(T) \leq \aleph_1$ instead of countability of T.

5.7. Applications: Fixed Fields of Generic Automorphisms

We finally come to the original motivation behind the results of the previous sections: their application to the case of fields. Recall that $\mathrm{abs}(k)$ denotes the absolute part of the field k and ϕ_p the Frobenius homomorphism in positive characteristic.

5.7.1. Pseudo-finite fields and models of $ACFA$. The case of pseudo-finite fields was dealt with in chapter 4. We include theorem (5.71) below and its proof out of theorem (5.65) for the sake of completeness, as well as its variant, theorem (5.72), whose proof is somehow already present in chapter 4, but which we did not state there explicitly.

THEOREM 5.71. *Any pseudo-finite field k is isomorphic to the fixed field of some model of $ACFA$. Furthermore, in positive characteristic, for every $n \in \mathbb{Z}$ there is some model (Ω, σ) of $ACFA$ such that $\mathrm{Fix}(\Omega, \sigma\phi_p^n) = k$.*

Proof. Choose a topological generator σ of the absolute Galois group $\mathrm{Gal}(k)$ of k. The difference field $(k^{\mathrm{alg}}, \sigma)$ extends to some model (Ω, σ) of $ACFA$. Of course k is algebraically closed in $\mathrm{Fix}(\Omega, \sigma)$, whence, as both fields are pseudo-finite, the extension $\mathrm{Fix}(\Omega, \sigma)/k$ is elementary by corollary (4.5.3). Also, it follows that $k^{\mathrm{alg}}\mathrm{Fix}(\Omega, \sigma) = \mathrm{Fix}(\Omega, \sigma)^{\mathrm{alg}}$. So theorem (5.69) implies that there is some model $(K, \sigma) \models ACFA$ such that $\mathrm{Fix}(K, \sigma) = k$.

For the furthermore, let (Ω, τ) be a model of $ACFA$ such that $k = \mathrm{Fix}(\Omega, \tau)$ and put $\sigma = \tau\phi_p^{-n}$. Then (Ω, σ) is a model of $ACFA$, too, and $\mathrm{Fix}(\Omega, \sigma\phi_p^n) = k$. □

Note that any choice of a generator of $\mathrm{Gal}(k)$ in the above proof gives non-elementarily equivalent models of $ACFA$ having fixed field k.

As an application of corollary (5.70) we obtain in positive characteristic the following theorem, which was shown to us by Zoé Chatzidakis (unpublished).

THEOREM 5.72. *Let (K, σ) be an algebraically closed difference field and $\Sigma \subseteq \mathbb{Z}$ such that for all $n \in \Sigma$ the fixed fields $\mathrm{Fix}(K, \sigma\phi_p^n)$ are pseudo-finite. Then there is some model (Ω, σ) of $ACFA$ such that for all $n \in \Sigma$*

$$\mathrm{Fix}(\Omega, \sigma\phi_p^n) = \mathrm{Fix}(K, \sigma\phi_p^n) \ .$$

5.7.2. One-free pseudo-differentially closed fields and models of $DCFA$. In this subsection we prove the following theorem.

THEOREM 5.73. *Any difference-differential field (F, d, σ) of characteristic zero whose fixed differential field (k, d) is pseudo-finite and pseudo-differentially closed embeds into some model (Ω, d, σ) of $DCFA$ such that*

$$\mathrm{Fix}(\Omega, d, \sigma) = (k, d) \, .$$

First we need a difference-differential version of lemma (4.25). Though we need it only in characteristic zero, we state and prove it for arbitrary characteristic.

LEMMA 5.74. *Any difference-differential field (F, d, σ) whose fixed differential field (k, d) has procyclic absolute Galois group admits an extension $(F^{\mathrm{sep}}, \bar{d}, \bar{\sigma})$ with* $\mathrm{Fix}(F^{\mathrm{sep}}, \bar{d}, \bar{\sigma}) = (k, d)$.

Proof. Let us first note that if (K, d) is a differential field and σ is a field automorphism of K that commutes with the derivation d (so an automorphism of the differential field (K, d)), then any lift $\bar{\sigma}$ of σ to K^{sep} will be compatible with the unique derivation $\bar{d}$ on K^{sep} extending d. Indeed, if $\alpha \in K^{\mathrm{sep}}$ and $p(X) \in K[X]$ is the minimal polynomial of α, then $\bar{d}(\alpha) = -\frac{p^d(\alpha)}{p'(\alpha)}$, where p' is the formal derivative of p and p^d is the polynomial obtained by applying d to the coefficients of p (see [**75**], the argument there is also valid in positive characteristic for separably algebraic field extensions). Using this and the assumption that σ commutes with d, one computes right away that $\bar{\sigma}\bar{d}(\alpha) = \bar{d}\bar{\sigma}(\alpha)$.

By the above consideration, any lift $\bar{\sigma}$ of σ to F^{sep} yields a difference-differential field $(F^{\mathrm{sep}}, \bar{d}, \bar{\sigma})$. By lemma (4.25) there is such $\bar{\sigma}$ such that $\mathrm{Fix}(F^{\mathrm{sep}}, \bar{\sigma}) = k$, which proves the lemma. □

Proof of theorem (5.73). By the previous lemma (5.74) we may assume that F is an algebraically closed field. Embed (F, d, σ) into some model (Ω, d, σ) of $DCFA$. The pure fields k and $K = \mathrm{Fix}(\Omega, d, \sigma)$ are pseudo-finite, so it follows as in the proof of theorem (5.71) that $k \preccurlyeq K$ as pure fields, and that $k^{\mathrm{alg}}K = K^{\mathrm{alg}}$. Now proposition (5.8) of [**53**] states that two pseudo-differentially closed differential fields of characteristic zero are elementarily equivalent as differential fields if and only if they are elementarily equivalent as pure fields. It follows therefrom that $(k, d) \preccurlyeq (K, d)$ as differential fields. As both are subdifferential fields of (Ω, d, σ), their algebraic closure in the sense of DCF_0 coincides with their field-theoretic algebraic closure, so corollary (5.70), with the family of $\emptyset$-definable L_d-automorphisms consisting of the identity only, implies there is some model of $DCFA$ whose fixed differential field is (k, d). □

COROLLARY 5.75. *Any pseudo-finite pseudo-differentially closed differential field (k, d) of characteristic zero is the fixed differential field of some model (Ω, d, σ) of $DCFA$.*

REMARK 5.76. *By the argument in the proof of lemma (5.74), we may choose any generator σ of the absolute Galois group of k and apply (5.73) to the difference-differential field $(k^{\mathrm{alg}}, d, \sigma)$. As in the case of pseudo-finite fields, this shows that there are in fact many non-elementarily equivalent models of $DCFA$ having (k, d) as fixed field.*

5.7.3. One-free PAC fields and models of $SCFA$. Last but not least we come to discuss the case of one-free PAC fields of finite Ershov invariant and separably closed fields with a generic automorphism.

THEOREM 5.77. *Any difference field (F, σ) whose fixed field k is one-free PAC and of finite Ershov invariant e embeds into some model (Ω, σ) of $SCFA_{e,b}$ such that* $\mathrm{Fix}(\Omega, \sigma) = k$.

Proof. First we may assume that F is separably closed by lemma (4.25).

Second, note that the field extension F/k is separable. Indeed, this is true for any difference field (F,σ): let $\bar{c} \in k = \mathrm{Fix}(F,\sigma)$ be a finite tuple, and assume that $\bar{c}$ is p-independent in k but p-dependent in F. Then there is a minimal number r such that the p-monomials

$$m_{i_0}(\bar{c}), \ldots, m_{i_r}(\bar{c})$$

are linearly dependent over F^p, for some $i_0, \ldots, i_r$. So we can write say $m_{i_0}(\bar{c})$ as a sum

$$m_{i_0}(\bar{c}) = \sum a_j^p m_{i_j}(\bar{c})$$

for some unique $a_j \in F$. Applying σ to this equation we obtain

$$m_{i_0}(\bar{c}) = \sum \sigma(a_j)^p m_{i_j}(\bar{c})$$

because $m_i(\bar{c}) \in k$, whence $\sigma(a_j) = a_j$ for all j by minimality of r. But this contradicts the choice of $\bar{c}$.

Now we choose a p-basis $\bar{b} = b_1, \ldots, b_e$ of k. Of course $\bar{b}$ is also a p-basis of k^{sep}. We expand k^{sep} to an $L(\bar{b})$-structure, where $L(\bar{b})$ is the ring language augmented by constant symbols $\bar{b} = b_1, \ldots, b_e$. By the above, $\bar{b}$ is p-independent in F.

Now lemma (2.2) of [**12**] states that if (K,σ) is a difference field with finite p-basis B and $K(\bar{a})_\sigma$ is a finitely generated separable difference field extension of (K,σ), then $K(\bar{a})_\sigma$ embeds into some difference field with p-basis B. So for any finite tuple $\bar{a} \in F$, the difference field $k^{\mathrm{sep}}(\bar{a})_\sigma$ embeds into some separably closed difference field with p-basis $\bar{b}$, or in other words (as $\bar{b}$ is fixed by σ), $k^{\mathrm{sep}}(\bar{a})_\sigma$ embeds into some model of $(SCF_{e,b})_\sigma$. Thus by compactness (F,σ) embeds into some model of $(SCF_{e,b})_\sigma$, and consequently into some model (Ω,σ) of $SCFA_{e,b}$ by model completeness.

$\bar{b}$ is a p-basis of Ω and is fixed by σ, whence $\bar{b}$ is a p-basis of $\mathrm{Fix}(\Omega,\sigma)$. It follows that the extension $\mathrm{Fix}(\Omega,\sigma)/k$ is separable, and that k is algebraically closed in $\mathrm{Fix}(\Omega,\sigma)$. So $\mathrm{Fix}(\Omega,\sigma)/k$ is a regular extension, and hence elementary by theorem (5.47), as both k and $\mathrm{Fix}(\Omega,\sigma)$ are PAC for $SCF_{e,b}$.[13] Clearly $k^{\mathrm{sep}}\mathrm{Fix}(\Omega,\sigma) = \mathrm{Fix}(\Omega,\sigma)^{\mathrm{sep}}$, so theorem (5.65) shows that there is some model (K,σ) of $SCFA_{e,b}$ having fixed field k. □

Corollary 5.78. *Any one-free PAC field k of finite degree of imperfection e is the fixed field of some model (Ω,σ) of $SCFA_{e,b}$.*

Proof. Choose a topological generator σ of $\mathrm{Gal}(k)$ and apply the previous theorem to the difference field $(k^{\mathrm{sep}},\sigma)$. □

Remark 5.79. *Again the above proof shows with theorem (5.10) that there are many non-elementarily equivalent models of $SCFA_{e,b}$ having fixed field k.*

[13] we could also use corollary (20.4.3) of [**22**].

Bibliography

[1] **J. Ax**: *Solving diophantine problems modulo every prime.* Annals of Mathematics **85** (1967), 161-183.

[2] **J. Ax**: *The Elementary Theory of Finite Fields.* Annals of Mathematics **88** (1968), 239-271.

[3] **J. Ax, S. Kochen**: *Diophantine Problems over Local Fields I.* American Journal of Mathematics **87** (1965), 605-630.

[4] **J. Ax, S. Kochen**: *Diophantine Problems over Local Fields II. A Complete Set of Axioms for p-Adic Number Theory.* American Journal of Mathematics **87** (1965), 631-648.

[5] **J. Ax, S. Kochen**: *Diophantine Problems over Local Fields III: Decidable Fields.* Annals of Mathematics **83** (1966), 437-456.

[6] **J. T. Baldwin, S. Shelah**: *Model Companions of T_{Aut} for stable T.* Notre Dame Journal of Formal Logic **42** (2001), 121-142.

[7] **R. Bustamante-Medina**: *Differentially Closed Fields of Characteristic zero with a Generic Automorphism.* Revista de Matemática: Teoría y Aplicaciones 2007 **14**, 81-100.

[8] **R. Bustamante-Medina**: *Théorie des modèles des corps différentiellement clos avec un automorphisme génerique.* Thèse de Doctorat, available at http://www.logique.jussieu.fr/modnet/Publications/Preprint server/

[9] **Z. Chatzidakis**: *Théorie des modèles des corps finis et pseudo-finis.* Lecture Notes, available at http://www.logique.jussieu.fr/www.zoe/index.html

[10] **Z. Chatzidakis**: *Model Theory of Difference Fields.* in Peter Cholak (ed.): The Notre Dame lectures. Wellesley, MA: A K Peters; Urbana, IL: Association for Symbolic Logic. Lecture Notes in Logic 18, 45-96 (2005)

[11] **Z. Chatzidakis**: *A Survey on the Model Theory of Difference Fields.* in Haskell, Deirdre (ed.) et al.: Model Theory, Algebra, and Geometry. Cambridge University Press. Math. Sci. Res. Inst. Publ. 39, 65-96 (2000).

[12] **Z. Chatzidakis**: *Generic automorphisms of separably closed fields.* Illinois Journal of Mathematics **45** (2001), 693-733.

[13] **Z. Chatzidakis, L. van den Dries, A. Macintyre**: *Definable sets over finite fields.* Journal für die reine und angewandte Mathematik **427** (1992), 107-135.

[14] **Z. Chatzidakis, E. Hrushovski**: *Model Theory of Difference Fields.* Trans. Amer. Math. Soc. **351** (1999), 2997-3071.

[15] **Z. Chatzidakis, E. Hrushovski, Y. Peterzil**: *Model Theory of Difference Fields, II: Periodic Ideals and the Trichotomy in all Characteristics.* Proceedings of the London Mathematical Society **85** (2002) 257-311.

[16] **Z. Chatzidakis, A. Pillay**: *Generic Structures and Simple Theories.* Annals of Pure and Applied Logic **95** (1998), 71-92.

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

[18] **F. Delon**: *Idéaux et Types sur les Corps séparablement clos.* Mém. Soc. Math. France (N.S.) **33** (1988), 1-76.

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

[20] **S. Eilenberg, N. Steenrod**: *Foundations of Algebraic Topology.* Princeton University Press, 6th printing 1966.

[21] **Y. Ershov**: *Fields with a Solvable Theory.* (English Translation) Sov. Math. Doklady **8** (1967) 575-576.
[22] **M. Fried, M. Jarden**: *Field Arithmetic.* 2nd revised and enlarged ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge 11. Springer (2005).
[23] **W.D. Geyer, M. Jarden**: *Non-PAC fields whose Henselian closures are separably closed.* Math. Res. Lett. **8** (2001) 509-519.
[24] **R. Hartshorne**: *Algebraic Geometry.* Springer GTM 52.
[25] **A. Hasson, E. Hrushovski**: *DMP in Strongly Minimal Sets.* Journal of Symbolic Logic **72** (2007), 1019-1030.
[26] **E. Hrushovski**: *Pseudo-finite fields and related structures.* in Bélair, L. et al. (ed.): Model Theory and Applications. Quaderni di Matematica **11** (2002), 151-212.
[27] **E. Hrushovski**: *The Manin-Mumford Conjecture and the Model Theory of Difference Fields.* Annals of Pure and Applied Logic **112** (2001), 43-115.
[28] **E. Hrushovski**: *The Elementary Theory of the Frobenius Automorphism.* Preprint 2006.
[29] **E. Hrushovski, A. Pillay**: *Weakly Normal Groups.* in Paris Logic Group (eds): Logic Colloquium 1985, Stud. Logic Found. Math. **122**, Noth-Holland 1987, 233-244.
[30] **W. Hodges** *Model Theory.* Encyclopedia of Mathematics and Its Applications 42. Cambridge University Press 1993.
[31] **B. Kim, A. Pillay**: *Simple Theories.* Annals of Pure and Applied Logic **88** (1997), 149-164.
[32] **J. Koenigsmann**: *Definable Valuations.* Prépublications de l'Equipe de Logique No. 50, 1995; to appear in the Journal of Algebra.
[33] **A.H. Lachlan** *A property of stable theories.* Fundamenta Mathematicae **77** (1972), 9-20.
[34] **S. Lang**: *Introduction to Algebraic Geometry.* Interscience, 1958.
[35] **S. Lang**: *Algebra.* Fourth Edition, Springer 2002.
[36] **D. Lascar** *Les beaux automorphismes.* Archive for Mathematical Logic **31** (1991), 55-68.
[37] **D. Lascar**: *Autour de la Propriété du Petit Indice.* Proc. London Math. Soc. (3) 62 (1991) 25-53.
[38] **D. Lascar, A. Pillay**: *Hyperimaginaries and Automorphism Groups.* Journal of Symbolic Logic **66** (2001), 127-143.
[39] **A. Macintyre**: *Generic Automorphisms of Fields.* Annals of Pure and Applied Logic **88** (1997) 165-180.
[40] **A. Macintyre**: *Nonstandard Analysis and Cohomology.* in N.J. Cutland et al (ed.): Nonstandard Methods and Applications. Lecture Notes in Logic **25** 2006.
[41] **A. Martin-Pizarro**: *Galois Cohomology of Fields with a dimension.* Journal of Algebra **298** (2006), 34-40.
[42] **A. Martin-Pizarro**: *Elliptic and hyperelliptic curves over supersimple fields in characteristic 2.* Journal of Pure and Applied Algebra **204** (2006), 368-379.
[43] **A. Martin-Pizarro, A. Pillay**: *Elliptic and Hyperelliptic Curves over Supersimple Fields.* J. London Math. Soc. (2) 69 (2004) 1-13.
[44] **A. Martin-Pizarro, F. O. Wagner**: *Supersimplicity and Quadratic Extensions.* Preprint 2005.
[45] **H. Matsumura**: *Commutative Ring Theory.* Cambridge University Press 1986.
[46] **J. S. Milne**: *Algebraic Geometry.* Lecture Notes, available at http://www.jmilne.org/
[47] **D. Mumford**: *The Red Book of Varieties and Schemes.* Lecture Notes in Mathematics 1358, Springer 1988.
[48] **L. Newelski**: *Independence Results for Uncountable Superstable Theories.* Israel Journal of Mathematics, Vol.65, No.1 (1989), p.59-78.
[49] **L. Newelski**: *More on Locally Atomic Models.* Fundam. Math. 136, No.1, 21-26 (1990).
[50] **A. Pillay**: *Notes on Model Companions of Stable Theories with an Automorphism.* Preprint, available at ...

[51] **A. Pillay**: *Remarks on Galois Cohomology and Definability.* Journal of Symbolic Logic **62** (1997) 487-492.
[52] **A. Pillay**: *Strongly Minimal Sets with a Generic Automorphism.* Lecture Notes 2005.
[53] **A. Pillay, D. Polkowska**: *On PAC and Bounded Substructures of a Stable Structure.* Journal of Symbolic Logic **71** (2006), 460-472.
[54] **A. Pillay, B. Poizat**: *Corps et Chirurgie.* Journal of Symbolic Logic **60** (1995), 528-533.
[55] **A. Pillay, T. Scanlon, F. O. Wagner**: *Supersimple Fields and Division Rings.* Mathematical Research Letters **5** (1998), 473-483.
[56] **B. Poizat**: *A Course in Model Theory: An Introduction to Contemporary Mathematical Logic.* Springer 2000.
[57] **B. Poizat**: *Theorie de Galois Imaginaire.* Journal of Symbolic Logic **48** (1983) 1151-1170.
[58] **D. Polkowska**: *On Simplicity of bounded pseudoalgebraically closed structures.* Preprint 2005.
[59] **A. Prestel**: *Pseudo Real Closed Fields.* in: Set Theory and Model Theory, Lecture Notes in Mathematics, Springer 1979.
[60] **A. Prestel, M. Ziegler**: *Model Theoretic Metheods in the Theory of Topological Fields.* J. Reine Angew. Math. **299** (1978) 318-341.
[61] **L. Ribes**: *Introduction of Profinite Groups and Galois Cohomology.* Queen's Papers in Pure and Applied Mathematics No. 24, 1970.
[62] **L. Ribes, P. Zalesskii**: *Profinite Groups.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, Springer 2000.
[63] **M. Ryten**: *Model Theory of Finite Difference Fields and Simple Groups.* Dissertation Thesis, Leeds 2007.
[64] **P. Samuel, O. Zariski**: *Commutative Algebra Volume 1.* van Nostrand 1958.
[65] **P. Samuel, O. Zariski**: *Commutative Algebra Volume 2.* van Nostrand 1960.
[66] **S. Shelah**: *Simple Unstable Theories.* Ann. Math. Logic 19 (1980), pp. 177-203
[67] **S. Shelah** *Classification Theory.* Revised Edition, Noth-Holland 1990.
[68] **J.P. Serre** *Galois Cohomology.* Springer 2002.
[69] **J.P. Serre** *Local Fields.* Springer 1979.
[70] **K. Tent, M. Ziegler**: *A course in Model Theory.* to appear.
[71] **F. O. Wagner**: *Simple Theories.* Kluwer Academic Publishers 2000.
[72] **C. Wood**: *Differentially Closed Fields.* in Elisabeth Bouscaren (ed.): Model Theory and Algebraic Geometry. Lecture Notes in Mathematics, Springer 1998.
[73] **C. Wood**: *Notes on the Stability of Separably Closed Fields.* Journal of Symbolic Logic **44** (1979) 412-416.
[74] **M. Ziegler**: *Stabilitätstheorie.* Vorlesungsskript 1989, available at http://home.mathematik.uni-freiburg.de/ziegler/
[75] **M. Ziegler**: *Anfänge der Differentialalgebra.* Preprint 2002, available at http://home.mathematik.uni-freiburg.de/ziegler/

Index