Some model theory of separably closed fields

Margit Messmer

§1 Introduction.

The model theory of separably closed fields was first investigated by Eršov. Among other things he proved that the first-order theory of separably closed fields of a fixed characteristic $p \neq 0$ and of fixed degree of imperfection $e \in \omega \cup \{\infty\}$ is complete, see [6]. In 1979 C. Wood (see [24]) showed that these theories are stable, but not superstable, yielding the only examples of stable, non-superstable fields. Further model theoretic properties of these fields, like quantifier elimination, equationality, the independence relation, DOP, etc. were analysed. In 1988 F. Delon (see [5]) published a comprehensive article in which she investigated types in terms of their associated ideals in an appropriate polynomial ring, in particular proving elimination of imaginaries and giving a detailed analysis of different notions of rank.

In 1992, E. Hrushovski gave a model theoretic proof of the Mordell-Lang conjecture for function fields. In the case of characteristic $p \neq 0$ he used some of the model theoretic tools for separably closed fields, in particular an analysis of minimal types and the author's results on definability in separably closed fields.

A separably closed field can be equipped with a differential structure. Accounts of this line of work can be found in [21,22,23,10].

The purpose of these notes is to give an overview of the known results in the model theory of separably closed fields with special emphasis on the case of finite degree of imperfection. When discussing elimination of imaginaries, we give a general outline of how this property can be proved in all known examples of stable fields with additional structure

§2 A few remarks about field extensions.

All fields under consideration in this chapter will be of fixed characteristic $p \neq 0$. F, K and L always denote fields, $F[X_i, i \in I]$ the polynomial ring over F in the indeterminates $X_i, i \in I$. $\bar{F}$ stands for the (field-theoretic) algebraic closure of F and F^{p^n} for the subfield $\{x^{p^n} : x \in F\}$. By abuse of notation F^n denotes the set of n-tuples over F. To avoid confusion, we will sometimes use $[F]^n$ for the cartesian product. $\mathcal{F}_p$ is the finite field with p elements.

Definition 2.1. A polynomial $f \in F[X]$ is said to be **separable** if all its irreducible factors (in $F[X]$) have distinct roots (in $\bar{F}$). An element $x \in \bar{F}$ is said to be separable over F if its minimal polynomial over F is separable.

Note: An irreducible polynomial $f \in F[X]$ is separable iff its formal derivative f' is nonzero. An algebraic extension K of F is separable if every $x \in K$ is separable over F. Now let us define what it means for an arbitrary field extension to be separable.

Definition 2.2: (a) A p-monomial over a set $\{a_1, \dots, a_n\} \subseteq F$ is an element of the form $a_1^{e_1} \cdots a_n^{e_n}$ with $0 \leq e_i < p$. A finite set $A = \{a_1, \dots, a_n\} \subseteq F$ is *p-independent in F* if the set of p-monomials $\{m_0 = 1, \dots, m_{p^n-1}\}$ over A is linearly independent over F^p. An infinite set is p-independent if every finite subset is.

(b) A field $K \supseteq F$ is a *separable extension* of F if, whenever $A \subseteq F$ is p-independent in F, then A is p-independent in K.

(c) A set $A \subseteq F$ is a *p-basis of F* if the set of p-monomials over A form a basis for F over F^p as a vector space; i.e. A is a maximal p-independent subset of F. The cardinality of such a set A is called the degree of imperfection or Eršov-invariant of F. We will simply call it the *invariant of F* .

(d) F is said to be *separably closed* if it has no proper separable algebraic extension. $\hat{F}$ denotes the separable closure of F, that is the maximal separable algebraic extension of F (inside $\bar{F}$).

Note:

- Part (b) of the previous definition is just another way of saying that F and K^p are linearly disjoint over F^p.
- The property of being separably closed can be expressed by an infinite set of first-order sentences in the language $\mathcal{L} = \{+, -, \cdot, ^{-1}, 0, 1\}$ of fields by saying that each polynomial whose formal derivative is nonzero has a root.

§3 The theory of separably closed fields in the language of fields.

By the note at the end of the previous section we can form the first-order theory SCF_e of separably closed fields (of characteristic p) of invariant e, where $e \in \omega$ or $e = \infty$ in the language $\mathcal{L} = \{+, -, \cdot, ^{-1}, 0, 1\}$ of fields. Notice that SCF_0 is the theory of algebraically closed fields. First we show that SCF_e is complete.

We first consider the case when e is finite. We extend the language $\mathcal{L}$ by finitely many constant symbols $a_1, \ldots, a_e$ interpreted as the elements of a p-basis in each model of SCF_e. So $\mathcal{L}' = \mathcal{L} \cup \{a_1, \ldots, a_e\}$ and SCF_e' stands for the theory of separably closed fields of invariant e in the language $\mathcal{L}'$. It is clear that SCF_e and SCF_e' have the 'same' models and completeness of SCF_e' implies the completeness of SCF_e.

Definition 3.1. A theory T is *model complete* if for all models M, N of T, $M \subseteq N$ implies $M \preceq N$.

Note: T is model complete iff for all models M, N of T and every existential sentence $\exists \bar{x} \phi(\bar{x}, \bar{m})$ with $\bar{m} \subset M$ and ϕ quantifier-free, if $N \models \exists \bar{x} \phi(\bar{x}, \bar{m})$ then $M \models \exists \bar{x} \phi(\bar{x}, \bar{m})$.

Lemma 3.2. The theory SCF_e' is model complete.

Before proving the lemma we make a few remarks about varieties (in the sense of Lang, see [8]). Let Ω be an algebraically closed field. By an (affine) *variety* V we mean the zero set of a prime ideal $\mathcal{P}$ of $\Omega[X_1, \ldots, X_n]$ for some n; that is $V = \{\bar{x} \in \Omega^n : f(\bar{x}) = 0 \text{ for all } f \in \mathcal{P}\}$. Conversely, the ideal $I(V)$ associated to a variety V is given by $\{f \in \Omega[\bar{X}] : f(\bar{x}) = 0 \text{ for all } \bar{x} \in V\}$.

Let I be an ideal of $\Omega[\bar{X}]$. If I has a basis consisting of elements from $K[\bar{X}]$ with $K \subseteq \Omega$, then K is said to be a *field of definition* of I. (We will note later that there exists a minimum such field of definition, see Section 4.) The variety V is said to be *defined over* K if K is a field of definition for $I(V)$.

Lemma 3.3. Let F be separably closed and K a separable extension of F. Then $\bar{F}$ and K are linearly disjoint over F.

Proof. Let $\{b_1, \ldots, b_n\} \subset K$ be linearly dependent over $\bar{F}$. So there are $c_1, \ldots, c_n \in \bar{F}$, not all zero, with $c_1 b_1 + \cdots + c_n b_n = 0$. Since F is separably closed, each c_i is purely inseparable over F. So there is $m \in \omega$ such that $c_i^{p^m} \in F$ for all i. So we have $c_1^{p^m} b_1^{p^m} + \cdots + c_n^{p^m} b_n^{p^m} = 0$. Now, since K is separable over F, if follows that K^{p^m} and F are linearly disjoint over F^{p^m}. Therefore we find $d_1, \ldots, d_n \in F$, not all zero, with $d_1^{p^m} b_1^{p^m} + \cdots + d_n^{p^m} b_n^{p^m} = (d_1 b_1 + \cdots + d_n b_n)^{p^m} = 0$, which says that $\{b_1, \ldots, b_m\}$ is linearly dependent over F.

Proof of 3.2. We follow Eršov's proof, see [6] and also [24, Th.1]. Let $F \subseteq K$, both models of SCF_e'. Since $\{a_1, \ldots, a_e\}$ is a p-basis of both F and K, it follows that K is a separable extension of F (p-independence is preserved!). Furthermore, since F is separably closed, F is relatively algebraically closed in K. So K is a 'regular' extension of F. Now let $\phi(x_1, \ldots, x_n)$ be a quantifier free formula over F with $K \models \exists \bar{x}\phi(\bar{x})$. Let $\bar{b} \subset K$ with $K \models \phi(\bar{b})$. Without loss of generality ϕ is in disjunctive normal form; that is

$$\phi = \bigvee_j (\bigwedge_i f_{ji}(\bar{x}) = 0 \wedge \bigwedge_k g_{jk}(\bar{x}) \neq 0),$$

with $f_{ji}, g_{jk} \in F[\bar{X}]$. Without loss of generality $K \models \bigwedge_i f_{1i}(\bar{b}) = 0 \wedge \bigwedge_k g_{1k}(\bar{b}) \neq 0$.

Now consider the prime ideal $\mathcal{P} \subseteq \bar{F}[\bar{X}, Y]$ defined as follows.

$$\mathcal{P} = \{f \in \bar{F}[\bar{X}, Y] : f(\bar{b}, 1/\prod_k g_{k1}(\bar{b})) = 0\}.$$

By the previous lemma, $\bar{F}$ and K are linearly disjoint over F, so by [8,Ch.III, Th.8] , F is a field of definition of $\mathcal{P}$ and the variety $V \subseteq \bar{F}^{n+1}$ given by $\mathcal{P}$ is defined over F. By [8,Ch.III, Th. 10], the set of points of V which are separably algebraic over F is dense in V. Since F is separably closed, there is $(\bar{c}, d) \in V \cap F^{n+1}$. Clearly, since $f_{1i}(\bar{X}) \in \mathcal{P}$ for all i and $\prod_k g_{1k}(\bar{X})Y - 1 \in \mathcal{P}$, $\bar{c}$ satisfies $\phi(\bar{x})$.

Remark 3.4. The separable closure of $\mathcal{F}_p(a_1, \ldots, a_e)$ is the prime model of SCF_e'.

Proof. Clearly the separable closure of $\mathcal{F}_p(a_1, \ldots, a_e)$ is a model of SCF_e' and it is contained in any model of SCF_e'. The claim follows from the model completeness of SCF_e'.

Theorem 3.5. (Eršov) The theory SCF_e ($e \in \omega \cup \{\infty\}$) is complete.

Proof.

For e finite, Lemma 3.2 and Remark 3.4 show that SCF_e' is complete, which implies the completeness of SCF_e.

In the case of $e = \infty$, instead of adding constant symbols for a p-basis we add infinitely many relation symbols $Q_n(x_1, \ldots, x_n)$, $n \in \omega$, interpreted as follows:

$$Q_n(x_1, \ldots, x_n) \text{ iff } \{x_1, \ldots x_n\} \text{ is} p\text{-independent}.$$

So

$$Q_n(x_1, \ldots, x_n) \text{ iff } \forall y_1 \ldots y_n(y_1^p x_1 + \cdots y_n^p x_n = 0 \to y_1 = \cdots = y_n = 0).$$

In this extended language one can show model completeness in a similar way as before. Again, the separable closure of $\mathcal{F}_p(X_i : i \in \omega)$ is the prime model which yields the completeness of SCF_∞. (For the infinite invariant part of this proof see also [24 Th.1] .)

Note:

(a) The theory SCF_e (in the language of fields) is not model complete: Let $F < K \models SCF_e$, where $K = F(b)$ with $b^p = a \in F - F^p$. Then $K \models \exists x(x^p = a)$, but $F \not\models \exists x(x^p = a)$.

(b) In the case of infinite invariant it is not possible to work in a language where we have names for a p-basis, since elementary extensions can contain new p-independent elements.

§4 Separably closed fields of finite invariant.

In the previous section we saw that the theory of separably closed fields of finite invariant is model complete if we add names for a p-basis. After extending this language by some definable function symbols, this theory will turn out to have several 'nice' model theoretic properties, such as quantifier elimination. From now on we fix e to be finite and nonzero.

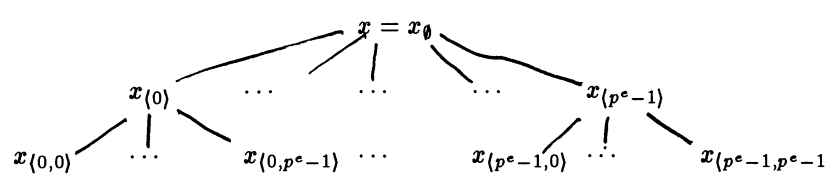
Let $F \models SCF'_e$ and let $\{m_0 = 1, \dots, m_{p^e-1}\}$ be the set of p-monomials over the p-basis $\{a_1, \dots, a_e\}$ as before. Each element of $x \in F$ can uniquely be written of the form

$$x = x^p_{\langle 0\rangle} m_0 + x^p_{\langle 1\rangle} m_1 + \dots + x_{\langle p^e\rangle} m_{p^e-1}$$

with $x_{\langle i\rangle} \in F$. Now for $0 \leq i < p^e$,

$$x_{\langle i\rangle} = x^p_{\langle i,0\rangle} m_0 + x^p_{\langle i,1\rangle} m_1 + \dots + x^p_{\langle i,p^e-1\rangle} m_{p^e-1}.$$

Continuing this process, we get a tree associated to each element $x \in F$:



Note that in the language $\mathcal{L}'$ each element in the tree is definable over x, and that x is definable over each level of the tree.

Let $(p^e)^{<\omega}$ denote the set of finite tuples over the set $\{0, \dots, p^e - 1\}$. We extend the language $\mathcal{L}'$ by infinitely many unary function symbols $\lambda_\sigma, \sigma \in (p^e)^{<\omega}$, interpreted as follows:

- $\lambda_\emptyset(x) = x_\emptyset = x$.
- For $0 \leq j < p^e$, $\lambda_{\langle j\rangle}(x) = x_{\langle j\rangle}$ iff $x = \sum_{j=0}^{p^e-1} x^p_{\langle j\rangle} m_j$.
- For $\sigma \in (p^e)^{<\omega}$, $\lambda_{\sigma\langle j\rangle}(x) = \lambda_{\langle j\rangle}(\lambda_\sigma(x)) = x_{\sigma\langle j\rangle}$, as indicated in the tree.

We say that $x_{(j)}$ is the jth coordinate of x. Note that all λ_σ's are definable in the language $\mathcal{L}'$.

Definition 4.1. SCF_e^* denotes the theory of separably closed fields (of characteristic p) of invariant e $(< \omega)$ in the language $\mathcal{L}^* = \{+,-,\cdot,^{-1},0,1\} \cup \{a_1,\dots,a_e\} \cup \{\lambda_\sigma : \sigma \in (p^e)^{<\omega}\}$.

Note that by 3.2 and 3.5 SCF_e^* is model complete and complete.

Proposition 4.2. The theory SCF_e^* eliminates quantifiers.

Note: Delon in [5, Prop.27] discusses a more general language for the finite and infinite invariant yielding quantifier elimination.

Proof of Proposition 4.2.

In order to prove quantifier elimination for a theory T it suffices to show the following (Shoenfield test):

> For any ω_1-saturated model M of T and any countable model N of T, and substructures $A \subseteq N$ and $B \subseteq M$, if $A \cong B$ then this isomorphism extends to an elementary embedding of N into M.

Claim. Let $F \models SCF_e^*$ and k a substructure of F, then k has invariant e.

Proof of Claim. Clearly the invariant of k is at least e since $\{a_1,\dots,a_e\} \subseteq k$. But with any element $x \in k$, k contains all coordinates x_σ of x witnessing its p-dependence on $\{a_1,\dots,a_e\}$. This shows the invariant of k is at most e. This proves the claim.

Now let k_1 be a substructure of $K \models SCF_e^*$ with K ω_1-saturated and k_2 a substructure of $F \models SCF_e^*$ with F countable, and $k_1 \cong k_2$. Clearly $\widehat{k_1} \cong \widehat{k_2}$ with $\widehat{k_i} \models SCF_e^*$ and $\widehat{k_1} \subseteq K$. By model completeness $\widehat{k_1} \preceq K$ and $\widehat{k_2}$ embeds elementarily into K. But since K is ω_1-saturated, F also embeds elementarily into K.

This quantifier elimination results yields a very useful one-to-one correspondence between 1-types over models of SCF_e^* and certain prime ideals in a suitable polynomial ring. This feature is explored in great detail in [5]. Here we discuss a few aspects of it.

Corollary 4.3. In SCF_e^* every formula $\phi(\bar{x})$ with parameters from a model $F \models SCF_e^*$ is equivalent to a boolean combination of formulas of the form

$$f(x_{1_{\sigma_1}},\dots,x_{1_{\sigma_m}},\dots,x_{n_{\sigma_1}},\dots,x_{n_{\sigma_m}}) = 0,$$

where $f \in F[X_{1_\sigma},\dots,X_{n_\sigma} : \sigma \in (p^e)^{<\omega}]$.

Proof. First check that for all x, y and $\sigma \in (p^e)^{<\omega}$, $(x+y)_\sigma$, $(x-y)_\sigma$, $(x \cdot y)_\sigma$, $(x^{-1})_\sigma \in F(x_\tau, y_\tau : \tau \in (p^e)^{<\omega})$. For example, for $p = 3$, $e = 1$ and p-basis $\{a\}$, the first-level coordinates of $x \cdot y$ can be obtained as the first row of the matrix

$$\begin{pmatrix} x_{\langle 0\rangle} & x_{\langle 1\rangle} & x_{\langle 2\rangle} \\ x_{\langle 2\rangle}a & x_{\langle 0\rangle} & x_{\langle 1\rangle} \\ x_{\langle 1\rangle}a & x_{\langle 2\rangle}a & x_{\langle 0\rangle} \end{pmatrix} \cdot \begin{pmatrix} y_{\langle 0\rangle} & y_{\langle 1\rangle} & y_{\langle 2\rangle} \\ y_{\langle 2\rangle}a & y_{\langle 0\rangle} & y_{\langle 1\rangle} \\ y_{\langle 1\rangle}a & y_{\langle 2\rangle}a & y_{\langle 0\rangle} \end{pmatrix}$$

Now the claim follows immediately from Proposition 4.2.

The following remark shows that all information about types is contained in the 1-types.

Remark 4.4. Let $F \models SCF_e^*$. There is a definable injection from $[F]^n$ into F, and therefore from the set of n-types into the set of 1-types. Moreover, if $n = p^{m \cdot e}$ for some $m < \omega$, we get a bijection.

Proof. Let $m < \omega$ be such that $p^{m \cdot e} \geq n$. Let $\{m'_1, \ldots, m'_{p^{me}}\}$ be the set of p^m-monomials over $\{a_1, \ldots, a_e\}$; that is $\{m'_1, \ldots, m'_{p^{me}}\}$ is a basis of F over F^{p^m}. Define $\Phi : [F]^n \to F$ by

$$\Phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^{p^m} m'_i.$$

So $\Phi(\bar{x})$ is an element whose mth level of its tree consists of $(x_1, \ldots, x_n, 0, \ldots, 0)$. Φ is the desired injection.

For $F \models SCF_e^*$, the automorphisms $Aut(F)$ of F act on the types over F by acting on the parameters. For $F[X_i : i \in I]$, a polynomial ring over F, $Aut(F)$ also acts on the ideals of $F[X_i : i \in I]$ by acting on the coefficients of the polynomials.

Corollary 4.5. Let $F \models SCF_e^*$. There is a (natural) one-to-one correspondence between complete 1-types over F and 'certain' prime ideals in the polynomial ring $F[X_\sigma : \sigma \in (p^e)^{<\omega}]$, given as follows. Let q be a 1-type over F, then the ideal $I(q)$ associated to q is given by

$$I(q) = \{f \in F[X_\sigma; \sigma \in (p^e)^{<\omega}] : `f(\bar{x_\sigma}) = 0' \in q\}.$$

Moreover, any automorphism $\alpha \in Aut(F)$ fixes q (setwise) iff α fixes $I(q)$ (setwise).

Proof. Immediate from Corollary 4.3. Note that $I(q)$ is a prime ideal since q is a complete type.

Note:

- (Delon) We call an ideal I of $F[X_\sigma;\sigma \in (p^e)^{<\omega}]$ *separable* if for all $f_0,\dots,f_{p^e-1} \in F[X_\sigma : \sigma \in (p^e)^{<\omega}]$,
$$f_0^p m_0 + \cdots f_{p^e-1}^p m_{p^e-1} \in I \text{ implies } f_0,\dots,f_{p^e-1} \in I.$$
The 'certain' ideals occurring as ideals of types are exactly the prime ideals which are separable in this sense and contain
$$\left\{ X_\sigma - \sum_{i=0}^{p^e-1} X^p_{\sigma\widehat{\ }(i)} m_i : \sigma \in (p^e)^{<\omega} \right\}.$$
- (Delon) The same one-to-one-correspondence holds for types over definably closed sets, see [5, Prop.33] .
- This kind of description of types in terms of ideals also arises in algebraically closed fields and in differentially closed fields.

Corollary 4.6. (Wood) The theory SCF_e^* is stable, not superstable.

Proof.

Let $F \models SCF_e^*$ with $|F|^{\aleph_0} = |F|$. By Corollary 4.5 the number of 1-types over F is at most the number of ideals of $F[X_\sigma;\sigma \in (p^e)^{<\omega}]$. For an ideal $I \subseteq F[X_\sigma;\sigma \in (p^e)^{<\omega}]$ let
$$I_n = I \cap F[X_\sigma : \sigma \in (p^e)^n],$$
where $(p^e)^n$ denotes the set of tuples over $\{0,\dots,p^e-1\}$ of length at most n. $F[X_\sigma : \sigma \in (p^e)^n]$ is a noetherian ring, since it is a polynomial ring with finitely many indeterminates. Therefore I_n is finitely generated. So there are at most $|F|$ possible different I_n for each n. But $I = \cup_{n\in\omega} I_n$, which shows that there at most $|F|^{\aleph_0} = |F|$ possible different ideals I.

To see that SCF_e^* is not superstable, we show that
$$F > F^p > F^{p^2} > \cdots > F^{p^i} > \cdots$$
forms an infinite descending chain of definable additive subgroups, each of infinite index in the preceding one. (The same can be shown for the corresponding multiplicative subgroups.) Since F is definably isomorphic to F^p via the Frobenius map $x \mapsto x^p$, it suffices to show that the index of F^p in F is infinite. But this follows from the following theorem of Poizat's, see [12, Th.5.10].

> Let F be a stable field. The F has no definable (additive or multiplicative) subgroup of finite index.

We can also see this directly. Let $a \in F - F^p$ and $b, c \in F^* = F - \{0\}$ with $b \neq c$. ab^p and ac^p lie in different (additive) cosets modulo F^p, since $ab^p - ac^p = d^p$ implies $a = (\frac{d}{b-c})^p$, a contradiction.

This corollary also shows that the theories SCF_e and SCF'_e from Section 3 are stable, not superstable for $e \in \omega$. The same holds for SCF_∞, see [24, Th.3] and [5, p.63].

Note. Separably closed fields are the only known stable, non-superstable fields.

Next we want to list several model-theoretic properties of the theory SCF_e^*.

1. Quantifier elimination implies that SCF_e^* is an *equational theory* for $e < \omega$. This was shown by G.Srour, see [17]. It is not known whether SCF_∞ is equational.

2. Result 5.10 together with 4.5 and 4.6 show that the theory SCF_e^* of separably closed fields with $e < \omega$ *eliminates imaginaries.* (For definitions, etc. see Section 5)

3. *DOP* (*'The Dimensional Order Property'*) is a non-structure property which for a superstable theory T yields the maximal number of models of in each cardinality $\geq 2^{|T|}$. In [1], Bouscaren proved that every superstable theory with a stable theory of pairs does not have *DOP*. Subsequently Delon showed that separably closed fields provide an example of a stable theory with stable pairs which has *DOP*. In fact, in [3] a strengthened, infinitary version, called ω-*DOP*, is proved. The authors show that there is a family of independent models K_i, $i \in \omega$, each containing a fixed model K_0, and a type p over the prime model over $\bigcup_i K_i$ such that for all $j \in \omega$, p is orthogonal to $\bigcup_{i \neq j} K_i$.

Among other things, the proof makes use of the fact that there is an algebraic description of (in)dependence, which we want to mention here.

4. Forking in SCF_e^*

Fact 4.7. Let $F \subseteq K$ be models of SCF_e^* and p a complete type over K realized by some $x \in L \geq K$. Then p does not fork over F iff $F(x_\sigma : \sigma \in (p^e)^{<\omega})$ and K are algebraically disjoint over F. This is equivalent to saying that $F(x_\sigma : \sigma \in (p^e)^{<\omega})$ and K are linearly disjoint over F.

For proofs and further details see [5, p.31ff.].

This description of forking says that two elements x and y are model-theoretically independent over some model F of SCF_e^* iff their trees $\{x_\sigma : \sigma \in (p^e)^{<\omega}\}$ and $\{y_\sigma : \sigma \in (p^e)^{<\omega}\}$ are algebraically independent over F. Similar descriptions of independence we find in algebraically closed fields and differentially closed fields.

5. Non-FCP. The theory SCF_e^* does not have the 'finite cover property' (non-*FCP*). The proof can be copied from the Chapter 'Model Theory of Differential Fields' by D. Marker, replacing differential polynomials there by polynomials in the polynomial ring $F[X_{1_\sigma}, \ldots, X_{n_\sigma} : \sigma \in (p^e)^{<\omega}]$. There an explicit proof of 'uniform bounding' is given. Non-FCP follows by Shelah's FCP-Theorem

(see [16, Ch.II, Th.2.2(8)]) using elimination of imaginaries and the stability of SCF_e^*.

6. Groups and fields. (For details see [9]) As in algebraically closed fields and differentially closed fields the question arises of whether the groups definable in a separably closed field are related to 'classical' groups. Results by Weil, van den Dries and Hrushovski showed that any infinite group definable in an algebraically closed field is definably isomorphic to an algebraic group. For a proof of this result see [2].

In analogy to (abstract) algebraic groups (over algebraically closed fields) we introduce the notion of an F-algebraic group for a separably closed field $F \models SCF_e^*$.

Definition 4.9. A subset $A \subseteq [F]^n$ is called *F-closed* if there are polynomials $f_1, \ldots, f_m \in F[X_1, \ldots, X_n], m \in \omega$ such that

$$A = \{\bar{x} \in [F]^n : f_i(\bar{x}) = 0 \text{ for } i = 1, \ldots, m\}.$$

We call $V = V_1 \cup \ldots \cup V_k$ a *variety* in F if there are F-closed 'charts' $U_i \subseteq [F]^n$ and bijections $f_i : V_i \to U_i$ such that $U_{ij} = f_i(V_i \cap V_j)$ are F-open subsets of U_i and such that the $f_{ij} = f_j \circ f_{i^{-1}} : U_{ij} \to U_{ji}$ are rational functions over F, for $1 \leq i, j \leq k$.

We call $\langle G, \cdot \rangle$ an *F-algebraic group* if G is a variety in F such that the maps $(x, y) \mapsto x \cdot y$ and $x \mapsto x^{-1}$ are morphisms with respect to the topology defined above, i.e. are locally F-rational functions.

Prop 4.9. Every infinite group G interpretable in a model F of SCF_e^* is definably isomorphic to an F-algebraic group.

Sketch of proof. A natural topology on F^n is the λ-topology given as follows.

> A subset $A \subseteq F^n$ is called *basic λ-closed* if there are finitely many polynomials $f_i \in F[X_{1_\sigma}, \ldots, X_{n_\sigma} : \sigma \in (p^e)^{<\omega}]$ such that $A = \{\bar{x} \in [F]^n : \bigwedge_i f_i(x_{1_{\sigma_1}}, \ldots, x_{1_{\sigma_l}}, \ldots, x_{n_{\sigma_1}}, \ldots, x_{n_{\sigma_l}}) = 0\}$.
>
> *λ-varieties* are defined in analogy to varieties in F, where the charts U_i are basic λ-closed, the U_{ij}'s are basic λ-open, the f_{ij}'s are rational functions over F as before in the $\bar{x} \in U_{ij}$ (not in the expanded tuples). A *λ-algebraic group* is a λ-variety such that multiplication and inversion are F-rational functions on each chart.

So let G be an infinite group interpretable in $F \models SCF_e^*$. First it is shown that G is definably isomorphic to a λ-algebraic group.

Since SCF_e^* eliminates imaginaries we can assume that G is a definable group. By 4.4, without loss of generality, $G \subseteq F$. Moreover, since G is connected-by-finite it suffices to consider the case where G is connected.

By increasing the arity of the set on which G is defined, we find a group G' definably isomorphic to G such that multiplication is a rational function for independent generic elements of G'. Then we can cover G' by finitely many translates of a λ-open 'generic' subset on which multiplication and inversion are rational functions, so that G' is equipped with the structure of a λ-alebraic group.

Finally the following fact allows us to turn this λ-algebraic group into an F-algebraic group.

> Let A be a λ-closed subset of $F \models SCF_e^*$ defined by a formula of the form $f(x_{\sigma_1}, \ldots, x_{\sigma_n}) = 0$ with $f \in F[X_\sigma; \sigma \in (p^e)^{<\omega}]$. Then A is in definable bijection with an F-closed subset B of $[F]^m$ for some $m \in \omega$ defined by $g(\bar{x}) = 0$ for some $g \in F[X_1, \ldots X_m]$.

To see this, first let $L \in \omega$ be the maximal length of all tuples $\sigma_1, \ldots, \sigma_n$ occuring in f. We can assume that all σ_i are of the same length L, by replacing the x_{σ_i} by the corresponding term in the x_τ's, where τ has length L. Now let $m = p^{L \cdot e}$ and define the map $\Phi : F \to [F]^m$ as follows.

$$x \mapsto (x_{\tau_1}, \ldots, x_{\tau_m}),$$

where $\{\tau_1, \ldots, \tau_m\}$ are all the tuples in $(p^e)^{<\omega}$ of length L, or equivalently $(x_{\tau_1}, \ldots, x_{\tau_m})$ is the Lth level of the tree of x. Clearly the image B of A under Φ is defined by the same polynomial f viewed as an element of $F[X_1, \ldots, X_m]$.

As a corollary of the previous result one can prove the following Rosenlicht-style theorem (see [15]) for infinite groups interpretable in SCF_e^*.

Corollary 4.10. Let G be a connected infinite group interpretable in a separably closed field $F \models SCF_e^*$. Then $G/Z(G)$ is definably isomorphic to a linear F-algebraic group. ($Z(G)$ denotes the center of G.)

Note: By a linear F-algebraic group we mean an F-closed subgroup of $GL_N(F)$ for some $N < \omega$, the general linear group over F .

Now we can classify the infinite fields interpretable in SCF_e^*.

Theorem 4.11. Let K be a field interpretable in a separably closed field $F \models SCF_e^*$ of finite invariant. Then K is definably isomorphic to a finite (purely inseparable) extension of F. In particular, K is itself separably closed.

Sketch of Proof.

By Corollary 4.10 the additive group K^+ as well as the multiplicative group K^* are both linear F-algebraic groups which are the F-rational points of some linear algebraic groups V^+ and V^*, respectively, in the algebraic closure $\tilde{F}$ of F. Since K^* acts on K^+ by multiplication, one can show that V^* acts on V^+. After restricting to the semisimple part of V^*, we are in the situation to apply Zil'ber's field theorem (see [12, Theorem 3.7]) and find an algebraically closed field $\mathcal{K}$ definable in F which is definably isomorphic to $\tilde{F}$ by [12, Theorem 4.15]

, via a definable isomorphism Φ. We arranged that K be definably embedded into $\mathcal{K}$. So Φ carries K onto a subfield of some finite extension of F. But it is easily seen that such a subfield must contain F^{p^n} for some n. Now F^{p^n} is isomorphic to F itself, so K is definably isomorphic to a finite extension of F.

Using an ultraproduct argument, it can also be shown that any infinite field K definable in a separably closed field F of infinite invariant is itself separably closed of infinite invariant, and $char(K) = char(F)$.

As a corollary of the previous theorem, Hrushovski observed the following. Note that in a saturated model, a set X, which is defined by a possibly infinite conjunction of formulas, is called *minimal* if for every definable (with parameters) set A, the intersection of X with A is finite or cofinite in X.

Corollary 4.12. Let F be a separably closed field of finite invariant and K an infinite minimal field defined in F by an infinite conjunction of formulas. Then K is definably isomorphic to $F^{p^\infty} = \cap_n F^{p^n}$, the maximal perfect, algebraically closed subfield of F.

Proof. By [12, Cor.5.21] K is the intersection of fields L_i each definable in F. By Proposition 4.11, each L_i is definably isomorphic to a finite extension K_i of F. By applying the map $x \mapsto x^{p^n}$ for some large enough n to the K_i's, we get an infinite descending chain of definable subfields K_i' of F. By [9, Cor.3.2], each K_i' contains F^{p^∞}. But since K is minimal, $\cap K_i' = F^{p^\infty}$.

§5 Elimination of imaginaries in fields.

In model theory we often find structures which are given on definable sets modulo some definable equivalence relation, for example a definable group modulo some definable normal subgroup or projective space over some field, etc. These structures are, in a strict sense, not definable. Often one says that they are interpretable in the theory T , or definable in T^{eq}. If a theory T *eliminates imaginaries*, each such interpretable structure is definably isomorphic to an (honestly) definable structure (see Fact 5.2(a) below). We will explore this property in the case of stable fields. For a general discussion of elimination of imaginaries, see for example [13]. Most of the discussion here will appear in [10].

Definition 5.1. A first-order theory T with monster model $\mathcal{M}$ is said to *eliminate imaginaries* if for every definable (with parameters) set $A \subset \mathcal{M}^n$, there is a finite set $B \subset \mathcal{M}$ such that for every automorphism σ of $\mathcal{M}$, σ fixes A setwise if and only if σ fixes B pointwise.

Fact 5.2. (a) If the theory T eliminates imaginaries and the definable closure (=*dcl*) of the empty set contains at least two elements, then for every definable equivalence relation E on $\mathcal{M}^n$ there is a definable function f from $\mathcal{M}^n$ to $\mathcal{M}^m$ for some m such that for all $\bar{x},\bar{y}$, $E(\bar{x},\bar{y})$ iff $f(\bar{x})=f(\bar{y})$.

(b) If the theory T eliminates imaginaries then for every definable set $A \subset \mathcal{M}^n$ there is a minimum definably closed set B such that A is definable over B.

Proof. For (a) see [13, Th.16.16] . (b) is immediate from the definition.

Remark 5.3. The theory SCF_e for $e \in \omega \cup \{\infty\}$ (in the language of fields) does not eliminate imaginaries.

Proof.
(See [5]) Let F be a saturated model of SCF_e. Then we find can two elements x, y in $F - F^p$ which lie in the same (multiplicative) coset modulo F^{*^p} and such that $\mathcal{F}_p(x) \cap \mathcal{F}_p(y) = \mathcal{F}_p$. Now $\mathcal{F}_p(x)$ and $\mathcal{F}_p(y)$ are two definably closed sets over which the coset xF^{*^p} is definable. But clearly xF^{*^p} is not definable over $\mathcal{F}_p(x) \cap \mathcal{F}_p(y) = \mathcal{F}_p$, contradicting Fact 5.2(b).

At this point we would like to pick the example from the previous proof and show how the quotient group F^*/F^{*^p} can be eliminated in the theory SCF_e^*.

We consider the specific example when $p=3$ and $e=1$ with the p-basis being $\{a\}$. The two elements $x, y \in F^*$ lie in the same coset modulo F^{*^3} iff

$$\frac{x_{(1)}^3 + 2x_{(2)}^3 a}{x} = \frac{y_{(1)}^3 + 2y_{(2)}^3 a}{y}.$$

Note that $x = x_{(0)}^3 + x_{(1)}^3 a + x_{(2)}^3 a^2$, and similarly for y. The equation above implies that

$$\begin{aligned} x_{(1)}y_{(0)} &= x_{(0)}y_{(1)}, \\ x_{(2)}y_{(0)} &= x_{(0)}y_{(2)}, \\ x_{(1)}y_{(2)} &= x_{(2)}y_{(1)}, \end{aligned}$$

which implies that $\frac{x}{y} \in F^{*^3}$. So the definable closure of

$$\frac{x_{(1)}^3 + 2x_{(2)}^3 a}{x}$$

is the minimum definably closed set over which xF^{*^3} is definable. Or in terms of Fact 4.8(a), the quotient group F^*/F^{*^3} can be eliminated by the definable map

$$x \mapsto \frac{x_{(1)}^3 + 2x_{(2)}^3 a}{x}.$$

There is a weaker version of elimination of imaginaries.

Definition 5.4. A theory T with monster model $\mathcal{M}$ has *weak elimination of imaginaries* if for every definable set $A \subset \mathcal{M}^n$ there is a formula $\phi(\bar{x}, \bar{y})$ such that there are only finitely many tuples $\bar{a}_1, \ldots, \bar{a}_m$ such that $\phi(\bar{x}, \bar{a}_i)$ defines A.

Note that a theory has elimination of imaginaries iff for every definable set $A \subset \mathcal{M}^n$ there is a formula $\phi(\bar{x}, \bar{y})$ such that there is a unique tuple $\bar{a}$ such that $\phi(\bar{x}, \bar{a})$ defines A. In the theory of fields these two definitions of elimination of imaginaries are equivalent.

Fact 5.5. Let T be the theory of a field. Then T has weak elimination of imaginaries iff T has elimination of imaginaries.

Proof. See [14, Cor.6]. Let $\phi(\bar{x}, \bar{y})$ be a formula in the language of T. We give the idea of the proof in the case where $\bar{y}$ has length one. Let $a_1, \ldots, a_m$ be the only elements such that $\phi(\bar{x}, a_i)$ defines $A \subset \mathcal{M}^n$. Let $f_1(y_1, \ldots, y_m), \ldots, f_m(y_1, \ldots, y_m)$ be the symmetric functions in $y_1, \ldots, y_m$; that is

$$f_1(\bar{y}) = \sum_{i=1}^{m} y_i$$

$$f_2(\bar{y}) = \sum_{i \neq j} y_i y_j$$

$$\vdots$$

$$f_m(\bar{y}) = \prod_{i=1}^{m} y_i.$$

Now define the formula $\psi(\bar{x}, \bar{z})$ to be

$$\exists y_1 \ldots \exists y_m \Big(\phi(\bar{x}, y_1) \wedge \bigwedge_{i=1}^{m} \forall \bar{x} \phi(\bar{x}, y_1) \leftrightarrow \phi(\bar{x}, y_i) \wedge \bigwedge_{i \neq j} y_i \neq y_j \wedge \bigwedge_{i=1}^{m} z_i = f_i(\bar{y})\Big).$$

Now $(f_1(\bar{a}), \ldots, f_m(\bar{a}))$ is the only tuple $\bar{b}$ such that $\psi(\bar{x}, \bar{b})$ defines A.

The proof is based on the fact that using symmetric functions, we can code up finite sets as finite tuples. In the general case when $\bar{y}$ has length l, one can code the set $\{\bar{a_1}, \ldots, \bar{a_m}\}$ by the tuple with consists of the coefficients of

$$\prod_{i=1}^{m} (Y + a_{i1} X_1 + a_{i2} X_2 + \cdots + a_{il} X_l)$$

Definition 5.6. Let T be an arbitrary first-order theory and p an n-type over a model M of T. A definably closed set $A \subseteq M$ is said to be the *canonical base of* p if for every automorphism σ of $\mathcal{M}$, σ fixes p iff σ fixes A pointwise.

To point out the connection between elimination of imaginaries and the existence of canonical basis we include the following lemma.

Lemma 5.7. Let T be a stable theory with elimination of imaginaries. Then every type has a canonical base.

Proof.

Let p be an n-type over a model M of T. Then p is definable over M. This means that for every formula $\phi(\bar{x},\bar{y})$ over the empty set there is a formula $d\phi(\bar{y})$ over M such that for all $\bar{a} \subset M$, $\phi(\bar{x},\bar{a}) \in p$ iff $M \models d\phi(\bar{a})$.

Since T eliminates imaginaries, for each $d\phi(\bar{y})$ there is a finite set B_ϕ such that every automorphism fixes the set defined by $d\phi(\bar{y})$ setwise iff it fixes B pointwise. Now let A be the definable closure of the union of all B_ϕ. It is easy to check that A is the canonical base for p.

The converse of the previous Lemma is not true. The theory of an infinite set in the pure language of equality is a counterexample. But we have the following.

Proposition 5.8. (Evans, Pillay, Poizat, see [7]) Let T be a stable theory such that each n-type over M has a canonical base for every model M of T. Then T has weak elimination of imaginaries.

Proof.

Let $A \subseteq \mathcal{M}^n$ be a set defined by $\phi(\bar{x},\bar{a})$ and let E be the following equivalence relation.

$$\bar{y}E\bar{z} \text{ iff } \forall\bar{x}\phi(\bar{x},\bar{y}) \leftrightarrow \phi(\bar{x},\bar{z}).$$

Furthermore let

$$C = \{\bar{y} : \underbrace{\forall\bar{x}\phi(\bar{x},\bar{y}) \leftrightarrow \phi(\bar{x},\bar{a})}_{\psi(\bar{y},\bar{a})}\} = \text{ the class of } \bar{a}.$$

Pick p, a nonforking extension of $\psi(\bar{y},\bar{a})$ to $\mathcal{M}$, and let B be the canonical base of p. Note that each $\sigma(B)$ gives rise to a nonforking extension of $\psi(\bar{y},\bar{a})$ to $\mathcal{M}$, of which there is only a bounded number. Thus B has only a bounded number of images under automorphisms σ which preserve C.

Claim 1. C is defined over B.
Proof of Claim 1. Let σ be an automorphism of $\mathcal{M}$ fixing B. So σ fixes p and $\psi(\bar{y},\sigma(\bar{a})) \in p$, defining the equivalence class $\sigma(C)$ of E. Since equivalence classes are disjoint, it follows that $\sigma(C) = C$. Thus each automorphism fixing B fixes C. Hence C is defined over B by some formula $\theta(\bar{y},\bar{b})$, $\bar{b} \subset B$, proving the claim.

Claim 2. There is only a finite number of $\bar{b}'$ with the same type as $\bar{b}$ over the empty set such that $\theta(\bar{y},\bar{b}) \leftrightarrow \theta(\bar{y},\bar{b}')$.
Proof of Claim 2. If σ is an automorphism of $\mathcal{M}$ with $\sigma(\bar{b}) = \bar{b}'$ such that $\theta(\bar{y},\bar{b}) \leftrightarrow \theta(\bar{y},\bar{b}')$, then σ preserves C. Since $\bar{b} \subset B$, there is only a bounded number of such images $\bar{b}'$ by the note above. So by compactness there is only a finite number of $\bar{b}'$'s. This proves the claim.

Now again by compactness, there is a formula $\chi(\bar{z})$ in the type of $\bar{b}$ over the empty set which implies the statement of claim 2. Define

$$\phi^*(\bar{y},\bar{z}) = \theta(\bar{y},\bar{z}) \wedge \chi(\bar{z}).$$

Then the formula

$$\Gamma(\bar{x},\bar{z}) = \exists\bar{y}\,[\phi(\bar{x},\bar{y}) \wedge \phi^*(\bar{y},\bar{z}) \wedge \forall\bar{y}_1(\phi^*(\bar{y}_1,\bar{z}) \rightarrow [\forall\bar{x}_1\phi(\bar{x}_1,\bar{y}) \leftrightarrow \phi(\bar{x}_1,\bar{y}_1)])]$$

has the property that there are only finitely many $\bar{b}$'s such that $\Gamma(\bar{x},\bar{b})$ defines A.

Corollary 5.9. Let T be the theory of a stable field such that for each model M of T each n-type over M has a canonical base. Then T has elimination of imaginaries.

Proof. By 5.8 and 5.5.

As mentioned before, there are several examples of stable fields (with additional structure) where we find a one-to-one correspondence between complete n-types and certain ideals in an appropriate polynomial ring. This immediately yields the existence of canonical bases as follows.

Let F be a field and $F[X_j : j \in J]$ a polynomial ring over F. In Section 3 we discussed the notion of a 'field of definition' of an ideal I of $F[X_j : j \in J]$. In fact every such ideal I has a *minimum field of definition* $C(I)$ contained in any other field of definition and obtained in the following way.

> Let M be the set of monomials over $\{X_j : j \in J\}$. Then there is a subset M_0 of M which is a basis for $F[X_j : j \in J]/I$. So modulo I, every monomial $m_k \in M$ can uniquely be written as $\sum_l a_{kl}m_l$ with $a_{kl} \in F$, $m_l \in M_0$. Then $C(I)$ is the subfield of F generated by all the a_{kl}.

Moreover, $C(I)$ has the property that for any automorphism σ of F, σ fixes I (setwise) iff σ fixes $C(I)$ pointwise. For proofs see for example [8].

Now we can formulate a general recipe for proving elimination of imaginaries in certain stable fields.

Prop 5.10. Let T be the theory of a stable field. Suppose that for every $n \geq 1$ there is a (possibly infinite) set of indeterminates X_i, $i \in J$, such that for each model F of T there is a one-to-one correspondence between complete n-types over F and certain ideals in the polynomial ring $F[X_i : i \in J]$, such that for every automorphism σ of F (as a T-structure), σ fixes the type (setwise) iff σ fixes the corresponding ideal (setwise). Then T eliminates imaginaries.

Proof. For any n-type p over F let $I(p)$ be the corresponding ideal. Then the definable closure of its minimum field of definition $C(I(p))$ is the canonical base of p. Therefore, by Corollary 5.9, T eliminates imaginaries.

References

[1] E. Bouscaren, *Dimensional order property and pairs of models.* Thèse d'état.

[2] E. Bouscaren, *Model-theoretic versions of Weil's theorem on pregroups.* The Model Theory of Groups. Ed. A.Nesin and A.Pillay. University of Notre Dame Press, 1989, pp.177–185.

[3] Z. Chatzidakis, Cherlin G., Shelah S., Srour G., Wood C. *Orthogonality in separably closed fields.* Classification Theory. Ed. J. Baldwin. New York, Springer, 1985, pp. 72–88.

[4] G. Cherlin and S. Shelah, *Superstable fields and groups.* Annals of Mathematical Logic, vol.18 (1980), pp.227–270.

[5] F. Delon, *Ideaux et types sur les corps séparablement clos.* Supplément au Bulletin de la société Mathématique de France. Mémoire No.33. Tome 116 (1988).

[6] J. Eršov, *Fields with a solvable theory.* Doklady Akadéemii Nauk SSSR, vol.174 (1967), pp.19–20; English translation, Soviet Mathematics, vol.8 (1967), pp.575–576.

[7] D. Evans, A. Pillay, B. Poizat, *A group in a group* Algebra i Logika, No.3 (1990), pp.368–378.

[8] S. Lang, *Introduction to algebraic geometry.* Interscience publisher, New York, 1958.

[9] M. Messmer, *Groups and fields interpretable in separably closed fields.* Transactions of the AMS, vol.344 (1994), pp. 361–377.

[10]M. Messmer and C. Wood, *Separably closed fields with higher derivations I.* Journal of Symbolic Logic, to appear.

[11] A. Pillay, *An Introduction to stability theory.* Clarendon Press, Oxford, 1983.

[12] B. Poizat, *Groupes stables.* Nur alMantiq walMa'arifah, Villeurbanne,1987.

[13] B. Poizat, *Cours de théories des modèles.* Nur almantiq walMa'arifah, Villeurbanne, 1985.

[14] B. Poizat, *Une théorie de Galois imaginaire.* The Journal of Symbolic Logic, vol.48 (1983), pp.1151–1171.

[15] M. Rosenlicht, *Some basic theorems on algebraic groups.* American Journal of Mathematics, vol.78 (1956), pp.401–443.

[16] S. Shelah, *Classification theory and the number of non-isomorphic models.* North-Holland, 2nd ed., 1990.

[17] G. Srour, *The independence relation in separably closed fields.* The Journal of Symbolic Logic, vol.51 (1986), pp.715–725.

[18] L.P.D. Van den Dries, *Definable groups in characteristic 0 are algebraic groups.* Abstracts of the American Mathematical Society, vol.3 (1982), p.142.

[19] L.P.D. Van den Dries, *Weil's group chunk theorem: a topological setting.* Illinois Journal of Mathematics, vol.34 (1990), pp.127–139.

[20] Weil,A. *On algebraic groups of transformations.* American Journal of Mathematics, vol.77 (1955), pp.203–271.

[21] C. Wood, *The model theory of differential fields of characteristic $p \neq 0$.* Proceedings of the AMS, Vol.40 (1973), pp.577–584.

[22] C. Wood, *Prime model extensions for differential fields of characteristic* $p \neq 0$. The Journal of Symbolic Logic, vol.39 (1974), pp.469–477.

[23] C. Wood, *The model theory of differential fields revisited.* Israel Journal of Mathematics, vol.25 (1976), pp.331–352.

[24] C. Wood, *Notes on the stability of separably closed fields.* The Journal of Symbolic Logic, vol.44 (1979), pp.412–416.