Separably closed fields

FRANÇOISE DELON

Separably closed fields are stable. When they are not algebraically closed, they are rather complicated from a model theoretic point of view: they are not superstable, they admit no non trivial continuous rank and they have the dimensional order property. But they have a fairly good theory of types and independence, and interesting minimal types. Hrushovski used separably closed fields in his proof of the Mordell-Lang Conjecture for function fields in positive characteristic in the same way he used differentially closed fields in characteristic zero ([Hr 96], see [Bous] in this volume). In particular he proved that a certain class of minimal types, which he called thin, are Zariski geometries in the sense of [Mar] section 5. He then applied to these types the strong trichotomy theorem valid in Zariski geometries.

We will recall here the basic algebraic facts about fields of positive characteristic (section 1) and reprove classical model-theoretical results about separably closed fields. We will consider only the non perfect fields of finite degree of imperfection, which are the ones appearing in the proof of Hrushovski and which admit elimination of quantifiers and imaginaries in a simple natural language (section 2). We will then develop a general theory of "λ-closed subsets" and associated ideals (sections 3 and 4), which has the flavour of the classical correspondance between Zariski closed subsets and radical ideals in algebraic geometry, and which allows us to prove that all minimal types are Zariski (section 5). Finally, following Hrushovski, we define thin types and explain how algebraic groups give rise to such types (section 6).

Notation: we use the notation $\bigwedge$-definable to mean infinitely definable.

Many thanks to Gabriel Carlyle, Marcus Tressl, Carol Wood and especially Elisabeth Bouscaren and Zoé Chatzidakis for reading preliminary versions of this text and detecting many insufficiencies and/or redundancies.

1 Fields of characteristic $p > 0$

Except for facts 1.3 and 1.4, everything in this section is classical and can be found in [Bour] and [Lanl 65].

Each field $K \neq \mathbb{F}_p$ has a non trivial endomorphism, the Frobenius map $x \to x^p$. Hence $K^p := \{x^p; x \in K\}$ is a subfield of K. K is said to be perfect if $K^p = K$. For each $x \in K$ there is, in every algebraically closed field containing K, a unique y satisfying $y^{p^n} = x$. We will denote $y = x^{p^{-n}}$ and $K^{p^{-n}} := \{x^{p^{-n}}; x \in K\}$.

An irreducible polynomial over K can have multiple roots: for example $X^p - a$ is irreducible over K iff $a \in K \setminus K^p$. A polynomial is <u>separable</u> if all its roots are distinct. Let x be algebraic over K, f its minimal polynomial; x is said to be <u>separable over</u> K if f is separable, or equivalently if x has exactly degree(f) distinct conjugates over K; x is <u>purely inseparable over</u> K if $f = X^{p^n} - a$ for some integer $n \geq 1$ and some $a \in K \setminus K^p$, or equivalently if every conjugate of x is equal to x. In general f may be written as $f(X) = g(X^{p^n})$, where $g \in K[X]$ is separable, hence the extension $K \subseteq K(x)$ may be decomposed as

$$K \subseteq K(x^{p^n}) \subseteq K(x).$$

More generally, every algebraic extension $K \subseteq L$ may be decomposed as $K \subseteq L_1 \subseteq L$ where the extension $K \subseteq L_1$ is separable (:$\Leftrightarrow$ every $x \in L_1$ is separable over K) and $L_1 \subseteq L$ is purely inseparable (:$\Leftrightarrow$ every $x \in L$ is purely inseparable over L_1).

The set of separably algebraic elements over K form a subfield K^s of the algebraic closure K^a. Purely inseparable elements form a subfield $\bigcup_{n \in \mathbb{N}^*} K^{p^{-n}} =: K^{p^{-\infty}}$ of K^a. Clearly $K^a = K^s.K^{p^{-\infty}}$ and K^s and $K^{p^{-\infty}}$ are linearly disjoint over K.

K^s is called the <u>separable closure</u> of K, and K is said to be <u>separably closed</u> if $K = K^s$.

$K^{p^{-\infty}}$ is called the <u>perfect closure</u> of K.

Theorem Every finite separable extension of K is of the form $K[x]$.

This well known "primitive element theorem" does not hold in general for non separable extensions. For example, if $K = \mathbb{F}_p(X, Y)$ with X and Y algebraically independent over $\mathbb{F}_p$, and $L = K^{p^{-1}}$, one has $[L : K] = p^2$ but $[K[x] : K] = p$ for every $x \in L \setminus K$.

The relation of p-dependence, which we will define now, is adequate for describing this phenomenon.

Let $A, B \subseteq K$ and $x \in K$. We say x is <u>p-independent over</u> A in K if $x \notin K^p(A)$; B is p-<u>free</u> over A if b is p-independent over $A \cup (B \setminus \{b\})$ for all b in B. We say "p-independent" or "p-free" instead of p-independent or p-free over $\emptyset$. B p-<u>generates</u> K if $K \subseteq K^p(B)$. Now, in K, B is p-generating minimal iff it is p-free maximal iff it is p-free and p-generating. Such a B is called a p-<u>basis</u> of K. All p-bases of K have the same cardinality. If ν is this cardinality, ν is finite iff $[K : K^p]$ is finite, and in this case $p^\nu = [K : K^p]$. We call ν the <u>degree of imperfection</u> of K, where $\nu \in \mathbb{N} \cup \{\infty\}$.

$B = \{b_i; i \in I\}$ is a p-basis of K iff the monomials $m_j = m_j(B) := \prod_{i \in I} b_i^{j(i)}$, for j any map from I into $\{0, 1, ..., p-1\}$ with finite support, form a linear basis of the K^p-vector space K; B is a p-basis of K iff for any integer n, the set $\{m_j(B); j \in \{0, 1, ..., p^n - 1\}^I$ with finite support$\}$ forms a linear basis of the K^{p^n}-vector space K. Consequently, if B is a p-basis of K, then any $x \in K$ can be written uniquely as $x = \sum x_j^p m_j$, with $j \in \{0, 1, ..., p-1\}^I$ having finite support, and with $x_j \in K$, almost all zero. The x_j's are called the components of x with respect to B, or its p-components.

We can now define and characterize separable extensions which are not necessarily algebraic.

An extension $K \subseteq L$ is called separable if one of the following equivalent conditions holds, where all fields below are subfields of L^a: (i) $K^{p^{-1}}$ and L are linearly disjoint over K

(ii) $K^{p^{-\infty}}$ and L are linearly disjoint over K

(iii) every p-free subset of K is p-free in L

(iv) some p-basis of K is p-free in L.

Remarks:

1. The two definitions of separability coincide for algebraic extensions.
2. Purely transcendental extensions are separable. More precisely, if B is a p-basis of K and X is algebraically free over K, then $B \cup X$ is a p-basis of $K(X)$.
3. Every extension of a perfect field is separable.

Let $K \subseteq L \subseteq M$. If L is separable over K and M is separable over L, then M is separable over K. If $K \subseteq M$ is separable then so is $K \subseteq L$ but $L \subseteq M$ may not be separable (e.g., $K \subseteq K(x^p) \subseteq K(x)$ for x transcendental over K). The compositum of two separable extensions need not be separable, but it is separable if the two extensions are linearly disjoint.

Using transitivity, an extension of K of the form $K(x_1, ..., x_n, x_{n+1})$, where the $x_1, ..., x_n$ are algebraically independent over K and x_{n+1} is separably algebraic over $K(x_1, ..., x_n)$, is separable. Conversely, every finitely generated separable extension is of this form, as the following theorem says:

Theorem 1.1 (Separating transcendence basis theorem) *If the extension $K \subseteq K(y_1, ..., y_n)$ is separable, there exist $m \leq n$ and $i_1 < ... < i_m \leq n$ such that $y_{i_1}, ..., y_{i_m}$ are algebraically independent over K and $K(y_1, ..., y_n)$ is separably algebraic over $K(y_{i_1}, ..., y_{i_m})$.*

1.2 Note that algebraic extensions never increase the degree of imperfection, and that purely transcendental extensions increase it by the transcendence degree of the extension. Conversely, if K is perfect and B p-free in $K(B)$, then B is algebraically free over K.

Fact 1.3 *Let K be an algebraically closed field and $L = K(x_1, ..., x_n)^s$. Then $K = L^{p^\infty} := \bigcap_{n \in \mathbb{N}^*} L^{p^n}$.*

Proof: Because K is perfect, $K \subseteq L$ is separable, and we can extract from $x_1, ..., x_n$ a separating transcendence basis, say $x_1, ..., x_m$. As a separable extension of $K(x_1, ..., x_m)$, L has also imperfection degree m. By 1.2, since L^{p^∞} is a perfect subfield of L, the transcendence degree of L over L^{p^∞} is at least m. But L^{p^∞} contains K which is algebraically closed, so $L^{p^\infty} = K$. □

Fact 1.4 *Let $K \subseteq L$ be a separable extension. Then K and L^{p^∞} are linearly disjoint over K^{p^∞}.*

Proof: Let $l_1, ..., l_n \in L^{p^\infty}$ be linearly dependent over K. We have to show they are remain dependent over K^{p^∞}. It suffices to consider the case where every proper subset $\{l_{i_1}, ..., l_{i_{n-1}}\}$ is linearly free over K. Let $k_i \in K$ be such that $\sum k_i l_i = 0$. Each $k_i \neq 0$, and by taking $k_1 = 1$, we get that $k_2, ..., k_n$ are uniquely determined. Hence it is enough to prove they lie in K^{p^r} for every integer r. Since L is a separable extension of K, the fields $K^{p^{-r}}$ and L are linearly disjoint over K, therefore K and L^{p^r} are linearly disjoint over K^{p^r}. This, together with the uniqueness of the k_i's, implies that these k_i's lie in K^{p^r}. □

2 Separably closed fields. Theories and types

Most of the results in this section come from [Er], [Wo 79], [De 88] or [Me 94]. Many of them can also be found in [Me 96]. We give here a slightly different presentation, centered on types.

The theory SC of separably closed fields is axiomatizable in the language of rings: K is separably closed iff each separable polynomial f over K has a root in K. Its completions are

$AC_0 = SC +$ (char=0), and

$SC_{p,\nu} = SC +$ (char=p) + (imperfection degree = ν),

for each prime p and $\nu \in \mathbb{N} \cup \{\infty\}$. We will prove below the completeness of $SC_{p,\nu}$ for finite $\nu > 0$ and $p > 0$, and AC_0 and $SC_{p,0}$ are the theories of algebraically closed fields of given characteristic, and are known to be complete.

From now on, we fix $p > 0$ and ν finite $\neq 0$.

Theorem 2.1 *Each theory $SC_{p,\nu}$ is complete.*

Proof: When studying inclusion of one model in another, we are interested in elementary extensions, hence in our case separable extensions. Because ν is finite, a p-basis of K is still a p-basis of any $L \succeq K$. This justifies adding to the language constants for the elements of a p-basis. Let us prove that in the language $\{0,1,+,-,.\} \cup \{b_1,...,b_\nu\}$, the theory $SC_{p,\nu}$ + "$\{b_1,...,b_\nu\}$ is a p-basis", axiomatized as $\forall x\ (\exists! x_j)_{j\in p^\nu}, x = \sum x_j^p m_j(b_1,...,b_\nu)$, is model-complete and has a prime model. This will prove completeness [ChKe, 3.1.9].

By 1.2 $b_1,...,b_\nu$ are algebraically independent over $\mathbb{F}_p$, hence the field $\mathbb{F}_p(b_1,...,b_\nu)^s$ is uniquely determined and embeds in every model.

Now, by Claim 2.2 below, any model is existentially closed in any model extension, this proves the model-completeness [ChKe, 3.1.7]. □

Claim 2.2 *Let $K \models SC_{p,\nu}$ and let L be a separable extension of K. Then L K-embeds in some elementary extension of K.*

Proof: It is enough to prove it for L finitely generated over K. By 1.1 such an L admits a separating transcendence basis $l_1,...,l_n$ over K. But any $|K|^+$-saturated elementary extension K^* of K has infinite transcendence degree over K, therefore $K(l_1,...,l_n)$ K-embeds in K^*, and $K(l_1,...,l_n)^s$ also since K^* is a model, hence so does L. □

Theorem 2.3 *(1) In the language $\mathcal{L}_{p,\nu} = \{0,1,+,-,.\} \cup \{b_1,...,b_\nu\} \cup \{f_i; i \in p^\nu\}$, the theory*

$$T_{p,\nu} = SC_{p,\nu} \cup \{\{b_1,...,b_\nu\} \text{ is a p-basis }\} \cup \{x = \sum_{i\in p^\nu} f_i(x)^p m_i(b_1,...,b_\nu)\}$$

has elimination of quantifiers.
(2) $T_{p,\nu}$ is stable not superstable.

These two results will follow from the description of types of $T_{p,\nu}$ given below.

Let $K \preceq L \models T_{p,\nu}$, with L $|K|^+$-saturated, $x \in L$. $B = \{b_1,\ldots,b_\nu\}$ is a p-basis of L, hence L contains all components x_j, $j \in p^\nu$, of x over B, as well as the components $x_{j\frown k}, k \in p^\nu$, of each x_j, and so on. We index the tree which branches p^ν times at each level by

$$p^\infty := \cup_{n\in\omega} p^{\nu n}$$

where each $p^{\nu n}$ is therefore understood as $(p^\nu)^n$ and one takes a disjoint union. We define now f_j, for $j \in p^\infty$, by setting $f_\emptyset := id$, $f_j := f_{j(n)} \circ \ldots \circ f_{j(1)}$ if $j \in p^{\nu n}$ with $n \geq 1$, and $x_j := f_j(x)$. But $p^{\nu n}$ should also be understood as $\{0,1,...,p^n-1\}^\nu$, when we write

$$x = \sum_{j\in p^{\nu n}} x_j^{p^n} \Pi_{i=1}^{\nu} b_i^{j(i)}.$$

Lemma 2.4 *$K\langle x\rangle := K(x_i; i \in p^\infty)^s$ is a prime model over $K \cup \{x\}$. It is algebraic (in the model-theoretic sense) over $K \cup \{x\}$.*

Proof: Clearly L contains $K\langle x\rangle$. Now $K \preceq K\langle x\rangle$: we already know that the extension $K \subseteq K\langle x\rangle$ is separable; it remains to prove that B still p-generates $K\langle x\rangle$. This holds, because $K\langle x\rangle$ contains all iterated p-components of x, and hence also all iterated p-components of every $y \in K\langle x\rangle$, by the following lemma. □

Lemma 2.5 *Define $x_{\leq n} = (x_i; i \in \cup_{m\leq n} p^{\nu m})$. If $K \subseteq K(\overline{z}) \subseteq L$ and y is separably algebraic over $K(\overline{z})$, then there is a non zero $d(\overline{z}) \in K[\overline{z}]$ such that, for all integer n, $y_{\leq n} \subseteq K[\overline{z}_{\leq n}, d(\overline{z})^{-1}, y]$. In particular $y_{\leq n} \subseteq K(\overline{z}_{\leq n}, y)$, hence each term in the variables $\overline{x}$ is equivalent to a rational function in $\overline{x}_{\leq n}$, for some integer n.*

Proof: Because $K(\overline{z}) \subseteq K(\overline{z}, y^p) \subseteq K(\overline{z}, y)$ and y is separable over $K(\overline{z})$, $K(\overline{z}, y) = K(\overline{z}, y^p)$. Hence $y \in K[\overline{z}, d(\overline{z})^{-1}, y^p]$ for some $d(\overline{z}) \in K[\overline{z}]$. By iteration, $y \in K[\overline{z}, d(\overline{z})^{-1}, y^{p^n}]$ for each integer n. Now as

$$d(\overline{z})^{-1} = \frac{d(\overline{z})^{p^n-1}}{d(\overline{z})^{p^n}},$$

we get that $y \in (K[\overline{z}_{\leq n}, d(\overline{z})^{-1}, y])^{p^n}(B)$. □

We want to describe the type of x over K, i.e. the isomorphism type of the field $K\langle x\rangle$ over K. We know what a separable closure is, hence we have to describe $K(x_i; i \in p^\infty)$. For this purpose, let us consider the ring

$$K[X_\infty] := K[X_i; i \in p^\infty],$$

where the X_i's are indeterminates. This ring is a countable union of Noetherian rings, hence each ideal is countably generated. We associate to x the following ideal of $K[X_\infty]$

$$I(x, K) := \{f \in K[X_\infty]; f(x_\infty) = 0\}$$

($x_\infty := (x_i; i \in p^\infty)$, we will also sometimes write $f(x)$ for $f(x_\infty)$). In order to describe the range of this map, let us give some definitions.

Definitions and notation:

1. All rings and algebras will be commutative with unit.
2. An ideal I of a K-algebra C is <u>separable</u> if, for all $f_j \in C$, $j \in p^\nu$,

$$\sum_j f_j^p m_j \in I \;\Rightarrow\; \text{each } f_j \in I,$$

where as previously $m_j = m_j(b_1, ..., b_\nu)$. Note that, given a prime ideal I of C, I is separable iff the quotient field of C/I is a separable extension of K. As an intersection of separable ideals is separable, we can speak of the <u>separable closure</u> of some ideal I, which is the smallest separable ideal containing I.

3. For $n \in \omega$,

$$K[X_{\leq n}] := K[X_i; i \in \cup_{m\leq n} p^{\nu m}],$$

and for an ideal I of $K[X_\infty]$

$$I_{\leq n} := I \cap K[X_{\leq n}].$$

Note that I is separable (or prime) iff each $I_{\leq n}$ is.
4. Let I^0 be the ideal of $K[X_\infty]$ generated by the polynomials $X_i - \sum_{j \in p^\nu} X_{i \frown j}^p m_j$, $i \in p^\infty$.

The following lemma will be used further on in section 5.

Lemma 2.6 *In an algebra over a separably closed field, any prime separable ideal is absolutely prime.*

Proof: If I is a prime separable ideal of the K-algebra C, the quotient field $Q(C/I)$ of C/I is a separable extension of K. Since the extension $K \subseteq K^a$ is purely inseparable, K^a and $Q(C/I)$ are linearly disjoint over K. □

Proposition 2.7 *The map $x \to I(x, K)$ defines a bijection between 1-types over K and prime separable ideals I of $K[X_\infty]$ containing I^0.*

Proof: This map clearly defines an injection. Consider now such an ideal I. Let M be the quotient field of $K[X_\infty]/I$. Then $K \preceq M^s$. For $x := X/I$, $I = I(x, K)$. □

The k-types are described as well, as L^k embeds in L via the following map:

$$(x_{(0)}, ..., x_{(k-1)}) \to \sum_{i \in p^{\nu n}} x_{(i)}^{p^n}.m_i$$

for n such that $p^{\nu n} \geq k$ and $x_{(k)} = ... = x_{(p^{\nu n}-1)} = 0$ (here $p^{\nu n}$ is regarded both as an integer and as the set $\{0, 1, ..., p^{\nu n} - 1\}$). If we define in the same way $K[X_{1\infty}, \ldots, X_{k\infty}] := K[X_{1i}, \ldots, X_{ki}; i \in p^\infty]$ and for $x \in L^k$, $I(x, K) := \{f \in K[X_{1\infty}, \ldots, X_{k\infty}]; f(x_\infty) = 0\}$, and if $I^0(X_i).K[X_{1\infty}, \ldots, X_{k\infty}]$ is simply denoted as $I^0(X_i)$, then

Proposition 2.8 *The map $x \to I(x, K)$ defines a bijection between k-types over K and prime separable ideals I of $K[X_{1\infty}, \ldots, X_{k\infty}]$ containing $\sum_{i=1}^k I^0(X_i)$.*

Definition: A prime ideal of $K[X_{1\infty}, \ldots, X_{k\infty}]$, separable and containing $\sum_{i=1}^k I^0(X_i)$, will be called a <u>type ideal</u>.

We now describe types over sets and prove quantifier elimination. The reader who is willing to admit this result can proceed directly to 2.11. A direct proof can also be found in [Me 96]. It is enough to consider definably closed sets. These are very close to being models, as the following lemma says.

Lemma 2.9 *Let B be the p-basis and $A \subseteq K$.*
(1) $\langle A\rangle := \mathbb{F}_p(B, f_j(A); j \in p^\infty)^s$ is a prime model over A.
(2) The definable closure of A is $(A)_{df} := \mathbb{F}_p(B, f_j(A); j \in p^\infty)$. Equivalently, A is definably closed iff it is a field, containing the p-basis B and closed under the f_i's, $i \in p^\nu$.
(3) $(A)_{df}$ is quantifier free definable over A in $\mathcal{L}_{p,\nu} \cup \{^{-1}\}$.

Proof: Clear once noted that no point of $\langle A\rangle \setminus (A)_{df}$ is definable over A since it can be moved by some A-automorphism. □

Thus a definably closed subset A of K is a subfield containing B as a p-basis and we can define as previously the rings $A[X_{1\infty}, ..., X_{k\infty}]$ and $A[X_{1\leq n}, ..., X_{k\leq n}]$, separable ideals in them, $I_{\leq n}$ for an ideal I of $A[X_{1\infty}, \dots, X_{k\infty}]$, and for $x \in L^k$,

$$I(x, A) := \{f \in A[X_{1\infty}, ..., X_{k\infty}]; f(x_\infty) = 0\}.$$

We will still denote by $I^0(X_i)$ the ideal $I^0(X_i) \cap A[X_{1\infty}, ..., X_{k\infty}]$.

Then we can state:

Proposition 2.10 *For every integer k, k-types over a definably closed set of parameters A are in bijection with prime separable ideals I of $A[X_{1\infty}, \dots, X_{k\infty}]$ containing $\sum_{i=1}^k I^0(X_i)$. All extensions to $\langle A\rangle$ are non forking and conjugate over A.*

Proof: A type P over A has only non forking extensions to $\langle A\rangle$ because $\langle A\rangle$ is algebraic over A. If $I := I(x, A)$ for some realization x of P, I is clearly prime, contains $\sum_{i=1}^k I^0(X_i)$ and is separable since $I(x, K)$ is. Conversely, for such an I, by classical results over Noetherian polynomial rings, the minimal prime ideals of $A^s[X_{1\leq n}, ..., X_{k\leq n}]$ containing $I_{\leq n} \otimes A^s$ are conjugate and intersect $A[X_{1\leq n}, ..., X_{k\leq n}]$ in $I_{\leq n}$. Now, by considering the dimension, we see that any prime ideal of $A^s[X_{1\leq n}, ..., X_{k\leq n}]$ intersecting $A[X_{1\leq n}, ..., X_{k\leq n}]$ in $I_{\leq n}$ is minimal over $I_{\leq n} \otimes A^s$. Therefore, the various ideals of $A^s[X_{1\infty}, \dots, X_{k\infty}]$ intersecting $A[X_{1\infty}, \dots, X_{k\infty}]$ in I are conjugate. Let Q be one such ideal. Then the quotient field of $A^s[X_{1\infty}, \dots, X_{k\infty}]/Q$ is a composite of A^s and of a subfield L which is A-isomorphic to the quotient field of $A[X_{1\infty}, \dots, X_{k\infty}]/I$. Since L is a separable extension of A, and A^s is separably algebraic over A, their composite is also separable over A, and therefore over A^s. This shows that Q is separable, hence is the ideal of a type over A^s. □

Proof of Theorem 2.3 :
(1) In the language $\mathcal{L}_{p,\nu} \cup \{^{-1}\}$, the definable closure of any set of parameters is quantifier free definable and quantifier free types over definably closed sets of parameters are complete. This implies quantifier elimination in $\mathcal{L}_{p,\nu} \cup \{^{-1}\}$. By 2.5 (or by an easy induction on the complexity of terms) any term of $\mathcal{L}_{p,\nu} \cup \{^{-1}\}$

is of the form uv^{-1}, where u and v are terms of $\mathcal{L}_{p,\nu}$. Hence any atomic formula of $\mathcal{L}_{p,\nu} \cup \{^{-1}\}$ is equivalent to some atomic formula of $\mathcal{L}_{p,\nu}$.
(2) $I(x, K)$ is countably generated, hence $|S_1(K)| \leq |K|^{\omega}$, which proves the stability. Now, in the sequence

$$K \supset K^p \supset \ldots \supset K^{p^n} \supset K^{p^{n+1}} \supset \ldots$$

of additive subgroups of K, each $K^{p^{n+1}}$ has infinite index in K^{p^n} as K^{p^n} is also a $K^{p^{n+1}}$-vector space and $K^{p^{n+1}}$ is infinite. This contradicts superstability. □

Proposition 2.11 *1. Each type $t \in S_1(K)$ has a countable field of definition D (: $\Leftrightarrow$ for any saturated $K^* \succeq K$ and any automorphism σ of K^*, σ preserves the non forking extension of t over K^* iff $\sigma|D = id_D$).*
2. For $K \preceq L \preceq F$ and $x \in F$, $t(x, L)$ does not fork over K iff $I(x, L) = L \otimes I(x, K)$ iff $t(x, L)$ has a field of definition contained in K iff L and $K\langle x\rangle$ are linearly disjoint over K.

For the proof see [De 88].

Some remarks about ranks and generics:
1. $I^0 = I(t, K)$ for t generic over K. (We mean here generic in the sense of the theory of stable groups; this notion has only been defined in this volume for the case of ω-stable groups but the reader can take the previous statement as a definition of "generic over K".)
2. By non superstability, the generic can not be U-ranked. We can see this directly: if x is generic over K and

$$K_n := K\langle x_0, x_{10}, \ldots, x_{1\ldots10}\rangle,$$

then $t(x, K_{n+1})$ forks over K_n. 3. In Section 5, we give a precise analysis of minimal types, i.e. of types with U-rank 1. In [De 88, 49], an algebraic interpretation of finite U-rank is given.
4. Any non algebraic formula contains a point having some generic p^n-component: see the remark following 3.4. Hence there is no non trivial continuous rank.

Theorem 2.12 *$T_{p,\nu}$ has elimination of imaginaries.*

Proof in the next section, see [Zie] for the definition of elimination of imaginaries.

We are now entitled to use all the machinery of stability in the context of separably closed fields. This enables us to characterize the groups interpretable in $T_{p,\nu}$ (in analogy to Weil's theorem, see [Pil, 4.12] in this volume) and to describe the interpretable fields [Me 94]. The proofs of these results use techniques

In the present paper $\subset$ and $\supset$ always denote strict inclusion.

from geometric stability theory. From this work we will quote only result 2.13 below.

For $a_1,...,a_m \in K \models T_{p,\nu}$, $K^{p^n}[a_1,...,a_m]$ is clearly definable in K. Conversely :

Theorem 2.13 *An infinite field interpretable in $K \models T_{p,\nu}$ is definably isomorphic to a subfield $K^{p^n}[a_1,...,a_m]$ of K.*

Proposition 2.14 *For $K \models T_{p,\nu}$, the field K^{p^∞} is algebraically closed, it is the largest algebraically closed subfield of K. It is $\wedge$-definable in K and, as such, is a pure field, which means that for every $F \subseteq K^k$ definable in K with parameters from K, $F \cap (K^{p^\infty})^k$ is definable in the field K^{p^∞} with parameters from K^{p^∞}.*

Proof: The field K^{p^∞} is separably closed since it is the intersection of separably closed fields (each K^{p^n} being isomorphic to K). It is also perfect, hence algebraically closed. It is clearly the largest algebraically closed subfield of K. By quantifier elimination any formula $\phi(x_1,...,x_k,\bar{c})$ of $\mathcal{L}_{p,\nu}$ is a Boolean combination of equations

$$f(x_{1\leq n},...,x_{k\leq n},\bar{c}_{\leq n}) = 0$$

for some integer n and some $f \in \mathbb{F}_p[X_{1\leq n},...,X_{k\leq n},\overline{C}_{\leq n}]$. For $x \in K^{p^\infty}$, the p^n-components of x are all zero, except the one corresponding to the p^n-monomial 1, which is equal to $x^{p^{-n}}$, hence quantifier free definable in the ring language. Now, as the trace over a subfield of a Zariski closed set is Zariski closed in the small field, we get that, for $x_1,...,x_k \in K^{p^\infty}$, $\phi(x_1,...,x_k,\bar{c})$ is equivalent to a formula of the ring language in $x_1,...,x_k$ with parameters from K^{p^∞} (one can also use directly the fact that in a stable theory if A is infinitely definable in a model M, then any definable subset of A is definable with parameters from A). □

Proposition 2.15 *Let $F \subseteq K^k$ be definable with parameters from K, and $h : F \to K$ be a map definable with parameters from K. Then there exist $C_1,...,C_m \subseteq (K^{p^\infty})^k$ definable in the field K^{p^∞} with parameters from K^{p^∞} and such that*
- $F \cap (K^{p^\infty})^k = C_1 \cup ... \cup C_m$ and
- each $h \restriction C_i$, for $i = 1,...,m$, is a composition of rational functions and of the inverse of the Frobenius (these functions $h \restriction C_i$'s may have parameters from K).

Proof: By quantifier elimination and compactness there are an integer n and definable $D_1,...,D_m \subseteq K^k$ such that each $h \restriction D_i$ is a rational function in $x_{1\leq n},...,x_{k\leq n}$ (the proof is along the same lines as the similar statement for algebraically closed fields, see [Pil, 1.5] this volume). By 2.14 each $D_i \cap (K^{p^\infty})^k$ is definable in K^{p^∞} and, arguing as in the proof of 2.14, for $x \in K^{p^\infty}$, all terms of the sequence $x_{\leq n}$ are zero except $x^{p^{-n}}$. □

Definition: An infinite $\bigwedge$-definable subset A is minimal if the trace on A of any definable subset is finite or cofinite in A. It follows trivially from 2.14 that the $\bigwedge$-definable field K^{p^∞} is minimal. Conversely :

Proposition 2.16 *An infinite field k which is $\bigwedge$-interpretable in $K \models T_{p,\nu}$ and minimal is definably isomorphic to K^{p^∞}.*

Proof: By [Hr 90], the stability of $T_{p,\nu}$ implies that there exist a field k^* interpretable in K and definable subfields $(k_n)_{n\in\omega}$ of k^* such that $k = \bigcap_{n\in\omega} k_n$. By 2.13, k^* is definably isomorphic to a subfield $l := K^{p^n}[a_1, ..., a_m]$. Via this isomorphism, each k_n becomes a subfield l_n of l containing K^{p^∞}. Hence $\bigcap l_n \supseteq K^{p^\infty}$. As a minimal field is algebraically closed, and K^{p^∞} is the largest algebraically closed field contained in K, $\bigcap l_n = K^{p^\infty}$. □

Remark: Decidability and stability of separably closed fields with infinite imperfection degree are proved along the same lines. It is also possible to describe the types and to give a natural language eliminating quantifiers in this setting. But we do not know any language eliminating imaginaries. Thus we are unable to characterize the interpretable groups and fields.

3 λ-closed subsets of affine space

Let us fix $K \preceq L \models T_{p,\nu}$. We will consider some particular subsets of L^k which are $\bigwedge$-definable with parameters from K.
Recall that if $x \in L^k$ and $f \in K[X_{1\infty}, \ldots, X_{k\infty}]$, we allow ourselves to write $f(x)$ for $f(x_\infty)$ (or more accurately for $f(x_{1\infty}, \ldots, x_{k\infty})$).

Definition: Given a set of polynomials S of $K[X_{1\infty}, \ldots, X_{k\infty}]$, we define

$$V(S) = \{x \in L^k;\ \text{ each polynomial of } S \text{ vanishes on } x\}$$

("for all $f \in S, f(x) = 0$" will also be denoted "$S(x) = 0$"). Such a $V(S)$ is called λ-closed (with parameters in K) in L^k. It is defined by a countable conjunction of first-order formulas (each ideal of $K[X_{1\infty}, \ldots, X_{k\infty}]$ is countably generated).

The following properties are clear.

Proposition 3.1 *For ideals I, J and I_α of $K[X_{1\infty}, \ldots, X_{k\infty}]$, we have*

$$V(I \cdot J) = V(I) \cup V(J) = V(I \cap J)$$
$$V(\sum_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$$
$$V(K[X_{1\infty}, \ldots, X_{k\infty}]) = \emptyset$$
$$V(0) = L^k.$$

(Note that the equality $V(I) \cup V(J) = V(I \cap J)$ does not generalise to infinite intersections and unions.) As a corollary:

Proposition 3.2 *The λ-closed sets are the closed sets of some topology over L^k.*

Remark: In this topology, as in the classical Zariski topology on L^k, the points of K^k are the unique separated points of L^k, hence it is T_0 iff $K = L$. On the other hand, it is not Noetherian, as the following sequence (of λ-closed sets of L) shows:
$V(X_0) \supset V(X_0, X_{10}) \supset V(X_0, X_{10}, X_{110}) \supset \dots \supset V(X_0, X_{10}, \dots, X_{11\dots10}) \supset \dots$
(X is here a single variable, and the indices describe its iterated p-components).

Definition: Given $A \subseteq L^k$, we define its canonical ideal $I(A, K)$, or $I(A)$ when there is no ambiguity,

$$I(A) := \{f \in K[X_{1\infty}, \dots, X_{k\infty}];\ \forall a \in A,\ f(a) = 0\}$$

("$\forall a \in A,\ f(a) = 0$" will also be denoted "$f(A) = 0$"). In particular we write now $I(x)$ for the ideal previously denoted as $I(x, K)$.

Remarks:
1. $I(\cup A_\alpha) = \cap I(A_\alpha)$.
2. $V(I(A))$ is the closure of A in the topology defined above, or λ-closure.

From now on in this section, L is ω_1-saturated.

Proposition 3.3 ("Nullstellensatz") 1. *The map $A \to I(A)$ defines a bijection between λ-closed subsets of the affine space L^k with parameters in K, and ideals of $K[X_{1\infty}, \dots, X_{k\infty}]$ which are separable and contain $\sum_{i=1}^k I_i^0$. The inverse map is $I \to V(I)$.*
2. *An ideal of $K[X_{1\infty}, \dots, X_{k\infty}]$ is of the form $I(A)$ iff it is the intersection of all type ideals containing it.*

Consequently, given an ideal I of $K[X_{1\infty}, \dots, X_{k\infty}]$, $I(V(I))$ is the separable closure of the ideal $I + \sum I_i^0$.

The proof of 3.3 will use the following facts.

Notation: For an ideal I of $K[X_{1\infty}, \dots, X_{k\infty}]$,

$$I_{\leq n} := I \cap K[X_{1\leq n}, \dots, X_{k\leq n}].$$

Note that the condition "$I_{\leq n}(x) = 0$" is first-order in x.

Fact 3.4 *Let q be an ideal of $K[X_{1\leq n}, \dots, X_{k\leq n}]$, prime, separable and containing $\sum_{i=1}^k I_{i\leq n}^0$. Then there exists a k-type P satisfying $I(P)_{\leq n} = q$.*

Proof: Since q is prime separable, by Claim 2.2, the fraction field of $K[X_{1\leq n}, ..., X_{k\leq n}]/q$ K-embeds in some elementary extension of K. Let x_{ij}, for $i = 1, ..., k$ and $j \in \cup_{m\leq n} p^{\nu m}$, be the images of $X_{ij} + q$ under this embedding. As $q \supseteq \sum_{i=1}^{k} I_i^0$, the x_{ij}'s, $j \in \cup_{m\leq n} p^{\nu m}$, are the iterated p-components of $x_i (= x_{i\emptyset})$. Take now $P := t(x_1, ..., x_k; K)$. □

Remark: One can prove the following more precise fact: there exists a unique type ideal $I(P)$ intersecting $K[X_{1\leq n}, ..., X_{k\leq n}]$ in q and minimal for inclusion. If r is the Krull dimension of q, the type P has r p^n-components which are independent realizations of the generic. The proof is in the same spirit as the proof of 5.3.(3).

Fact 3.5 *A separable ideal of a K-algebra is radical.*

Proof: If a separable ideal contains some power x^n, it contains x^{p^m} for all $p^m \geq n$ and hence also x by separability. □

Fact 3.6 *Let I, Q, J be ideals. Suppose that $I = Q \cap J$ is separable, $J \not\subseteq Q$ and Q is prime. Then Q is separable.*

Proof: Suppose that $f = \sum_j f_j^p m_j \in Q$; choose $g \in J \setminus Q$. Then $g^p f \in I$, and each $gf_j \in I$ by separability of I. Since Q is prime, this implies that $f_j \in Q$. □

Proof of 3.3 : 1. Using the relations

$$\begin{aligned} I(V(I(A))) &= I(A) \\ V(I(V(I))) &= V(I), \end{aligned}$$

we see that A is λ-closed iff $A = V(I(A))$, and that $A \to I(A)$ and $I \to V(I)$ define reciprocal bijections between λ-closed sets and ideals of the form $I(A)$ for $A \subseteq L^k$. An ideal of the form $I(A)$ is clearly separable and contains $\sum I_i^0$. Conversely, let I be an ideal of $K[X_{1\infty}, \ldots, X_{k\infty}]$, separable and containing $\sum_i I_i^0$, and $g \in K[X_{1\leq n}, ..., X_{k\leq n}] \setminus I$. Then for all integer m

$$g \in K[X_{1\leq n+m}, ..., X_{k\leq n+m}] \setminus I_{\leq n+m}.$$

By classical results on commutative rings, since $I_{\leq n+m}$ is radical there exists a prime ideal q of $K[X_{1\leq n+m}, ..., X_{k\leq n+m}]$ containing $I_{\leq n+m}$ but not g. We may choose this q to be minimal prime over $I_{\leq n+m}$. By 3.6 q is separable and by 3.4 there is some type P satisfying $I(P)_{\leq n+m} = q$, hence $g \notin I(P)$. On a point realizing P, $I_{\leq n+m}$ vanishes and not g, that is, if $K\langle P\rangle$ denotes the prime model over K and some realization of P,

$$K\langle P\rangle \models \exists x\ I_{\leq n+m}(x) = 0 \wedge g(x) \neq 0.$$

K and L must satisfy the same formula, and then, by ω_1-saturation, L satisfies

$$\exists x\ I(x) = 0 \wedge g(x) \neq 0.$$

This proves $g \notin I(V(I))$, and finally $I(V(I)) = I$.

2. An intersection of type ideals is clearly separable and contains $\sum_i I_i^0$. Conversely a λ-closed set A is $\wedge$-definable, hence

$$A = \cup\{\text{ realizations of } P \text{ in } L^k;\ P \text{ complete } k\text{-type } \vdash x \in A\},$$

Therefore

$$I(A) = \cap\{I(P);\ P \text{ complete } k\text{-type } \vdash x \in A\}.$$ □

Proposition 3.7 *Ideals of λ-closed sets are stable under sum, i.e. $I(A \cap B) = I(A) + I(B)$ for A and B λ-closed.*

This proposition is slightly surprising because there is no analogous result in algebraic geometry, the sum of two radical ideals not being in general a radical ideal. The difference here comes from the fact that the polynomial rings we are working with are not Noetherian. The ideals we are considering, which have to contain $\sum_{i=1}^k I_i^0$, are resolutely of non finitary type. In particular, $(I + J)_{\leq n}$ will in general strictly contain $I_{\leq n} + J_{\leq n}$, which need not be a separable ideal of $K[X_{1\leq n}, \ldots, X_{k\leq n}]$.

By 3.3, it suffices to show that $I(A) + I(B)$ is separable. Thus, the result follows immediatly from:

Lemma 3.8 *Let I and J be ideals of $K[X_{1\infty}, \ldots, X_{k\infty}]$ separable and containing $\sum_{i=1}^k I_i^0$. Then $I + J$ is separable.*

Proof: Let $\sum x_j^p m_j = a + b$, with $x_j, a, b \in K[X_{1\leq n}, \ldots, X_{k\leq n}], a \in I, b \in J$, and write

$$a \equiv \sum a_j^p m_j \pmod{\sum I_i^0},$$

$$b \equiv \sum b_j^p m_j \pmod{\sum I_i^0},$$

with

$$a_j, b_j \in K[X_{1\leq n+1}, \ldots, X_{k\leq n+1}].$$

Since I and J are separable and contain $\sum I_i^0$, $a_j \in I$ and $b_j \in J$. Now

$$\sum (x_j - a_j - b_j)^p m_j \in \sum I_i^0,$$

and $\sum I_i^0$ is separable, hence

$$x_j - a_j - b_j \in \sum I_i^0.$$

Therefore $x_j \in I + J$. □

Proposition 3.9 *$T_{p,\nu}$ has elimination of imaginaries.*

Proof: We will prove that any definable subset D of some K^k has a field of definition, which means that there is a field $K_0 \subseteq K$ such that, for $K^* \succeq K$ and any automorphism σ of K^*, the canonical extension of D over K^* is invariant under σ iff $\sigma|K_0 = \mathrm{id}_{K_0}$. By quantifier elimination, D is defined by a formula

$$\vee_i(\wedge_j P_{i,j}(x) = 0 \wedge Q_i(x) \neq 0)$$

with $P_{i,j}, Q_i \in K[X_{1\infty}, \ldots, X_{k\infty}]$. Now, σ preserves D iff it preserves the formula in $x^\frown y$, where $y = (y_i)_i$,

$$\vee_i(\wedge_j P_{i,j}(x) = 0 \wedge Q_i(x).y_i = 1).$$

Hence it is enough to prove the result for D λ-closed, which follows by 3.3 from the existence of the field of definition of an ideal. □

Definitions:

1. In a topological space, a closed set is irreducible if it is not the proper union of two closed subsets.
2. A maximal irreducible closed subset of some closed set A is called an irreducible component of A.
3. A point of some irreducible closed subset A is called generic in A if its closure is A.

Proposition 3.10 *In an arbitrary topological space,*
1. a closed set is the union of its closed irreducible subsets;
2. if a closed set A is the union of finitely many maximal irreducible closed sets A_i, then the A_i's are all the irreducible components of A.

Proof: For 1. note that the closure of a singleton is irreducible, and that a closed set is the union of closures of its points. For 2. let $A = F_1 \cup \ldots \cup F_n \supseteq F$, with $F, F_1, \ldots, F_n$ irreducible closed sets. For $i = 1, \ldots, n$, $F = (F_i \cap F) \cup (\cup_{j \neq i} F_j \cap F)$, and by irreducibility of F, either $F \subseteq F_i$ or $F \subseteq \cup_{j \neq i} F_j$. An induction shows that some F_i contains F. □

Proposition 3.11 *A λ-closed set A is irreducible iff $I(A)$ is prime.*

Proof: Consider three λ-closed subsets $A = B \cup C$. Then $I(A) = I(B) \cap I(C) \supseteq I(B) \cdot I(C)$. If $A \supset B, C$, then $I(A) \subset I(B), I(C)$ and there exist $f \in I(B) \setminus I(A)$ and $g \in I(C) \setminus I(A)$, so $fg \in I(A)$. Hence $I(A)$ is not prime if A is reducible. Conversely if $I(A)$ is not prime, there are f and $g \in K[X_{1\infty}, \ldots, X_{k\infty}] \setminus I(A)$ such that $fg \in I(A)$. Then

$$B := \{a \in A; f(a) = 0\}, \text{ and}$$

$$C := \{a \in A; g(a) = 0\}$$

are proper λ-closed subsets of A, and $A = B \cup C$. □

Remarks:

1. By 3.11, a point x of an irreducible λ-closed set A is generic in A iff $I(x) = I(A)$. We can also give the following interpretation. We just proved that A is irreducible iff $I(A)$ is prime, therefore there is some k-type P satisfying $I(P) = I(A)$. Thus the generic points of A are exactly the realizations of P. Note that P is strictly included in A unless A is a singleton, in which case P is realized.

2. There is a priori no reason why 3.10.2 should remain true when A has infinitely many components. The dual problem over ideals is as follows. We know that

$$I(A) = \cap\{I(P); P\ k\text{-type completing } A\}.$$

We can partly reduce the intersection and write

$$I(A) = \cap\{Q; Q \text{ prime separable ideal } \supseteq I(A) \text{ and minimal for this property}\},$$

as a decreasing intersection of prime separable ideals is again prime separable. Is such an intersection reduced ? (An intersection $\cap_{\alpha<\alpha_0} Q_\alpha$ is reduced if for all $\alpha_1 < \alpha_0$, $\cap_{\alpha<\alpha_0, \alpha\neq\alpha_1} Q_\alpha$ strictly contains $\cap_{\alpha<\alpha_0} Q_\alpha$.) A priori not. Hence we do not know how well in general these irreducible components behave.

Definition: A set of the form $V(I)$ for a finitely generated I is called λ-closed of finite type (in [Me 94] such sets are called basic λ-closed.)

Remark:
Any λ-closed set is an intersection of λ-closed sets of finite type:

$$x \in V(I) \text{ iff } \wedge_n\, x \in V(I_{\leq n}).$$

And a λ-closed set is definable iff it has finite type. Indeed, by compactness, an infinite conjunction of first-order formulas which expresses a first-order condition is equivalent to a finite sub-conjunction. In other words, quantifier elimination can be restated as follows: a definable set is a finite Boolean combination of λ-closed sets of finite type.

We wish now to make the connection between $V(I)$ and the $I_{\leq n}$'s more precise.

Notation:

1. To x in L^k, we associate (cf. 2.5)

$$x_{\leq n} := (x_i; i \in \cup_{m\leq n} p^{\nu m}) \in K^{k(1+p^\nu+\ldots+p^{\nu n})}.$$

So $x, x_\emptyset$ and $x_{\leq 0}$ are canonically identifiable, and the $x_{\leq n}$'s form a projective system with limit x_∞. For $D \subseteq K^k$, define

$$D_{\leq n} := \{x_{\leq n}; x \in D\} \subseteq K^{k(1+p^\nu+\ldots+p^{\nu n})}.$$

Quantifier elimination implies that for any definable D there is some integer n such that $D_{\leq n}$ is quantifier free definable in the ring language.

2. For $D \subseteq L^{k(1+p^\nu+\ldots+p^{\nu n})}$ and an ideal I of $K[X_{1\leq n},\ldots,X_{k\leq n}]$,

$$I^{(n)}(D) := \{f \in K[X_{1\leq n},\ldots,X_{k\leq n}]; f(D) = 0\},$$

$$V^{(n)}(I) := \{x \in L^{k(1+p^\nu+\ldots+p^{\nu n})}; I(x) = 0\}.$$

If we identify x and x_∞, a set of the form $V(I)$ can be understood as living in the projective limit of the $L^{k(1+p^\nu+\ldots+p^{\nu n})}$, $n \in \omega$, and then $V(I)_{\leq n}$ appears as the projection of a λ-closed set. It is not in general Zariski closed in $L^{k(1+p^\nu+\ldots+p^{\nu n})}$, but we have the following

Lemma 3.12 *Suppose $I = I(V(I))$. Then*

$$I_{\leq n} = I^{(n)}(V^{(n)}(I_{\leq n})) = I^{(n)}(V(I)_{\leq n}).$$

Hence the Zariski closure of $V(I)_{\leq n}$ in $L^{k(1+p^\nu+\ldots+p^{\nu n})}$ is $V^{(n)}(I_{\leq n})$.

Proof: $V^{(n)}(I_{\leq n}) \supseteq V(I)_{\leq n}$, hence $I^{(n)}(V^{(n)}(I_{\leq n})) \subseteq I^{(n)}(V(I)_{\leq n})$. And clearly $I_{\leq n} \subseteq I^{(n)}(V^{(n)}(I_{\leq n}))$. Now, if $f \in K[X_{1\leq n},\ldots,X_{k\leq n}] \setminus I_{\leq n}$, there is some $x \in L^k$ satisfying $I(x) = 0 \wedge f(x) \neq 0$, hence $I^{(n)}(V(I)_{\leq n}) \subseteq I_{\leq n}$. $\square$

4 λ-closed subsets of a fixed type

In this section we relativize the notion of closed set introduced previously to the set of realizations of a single type: we consider only tuples from L^k whose coordinates all realize a fixed one-type over a small set of parameters.

The hypotheses are the following: $K_0 \preceq K \preceq L \models T_{p,\nu}$. The fixed one-type is defined over K_0, the closed sets are defined over K.

We suppose that L is $|K_0|^+$-saturated. Recall from the previous section that a λ-closed set is defined by a countable conjunction of equations.

Notation:

. P is a complete 1-type over K_0,

. $K_0\langle P\rangle$ is the prime model over K_0 and some realization of P,

. $P_i := P(x_i)$,

. P^k is the conjunction $\wedge_{i=1}^k P(x_i)$, which, even on K_0, is incomplete unless $k = 1$ or P is the type of some element in K_0,

. $P_1 \otimes \ldots \otimes P_k$ is the complete k-type over K_0 of an independent k-tuple of realizations of P, i.e. the type over K_0 corresponding to the ideal $\Sigma I(P_i)$ (following the notation introduced before Proposition 2.8, $I(P_i)$ denotes an ideal of $K[X_{i\infty}]$ as well as of $K[X_{1\infty},\ldots,X_{k\infty}]$).

. For $R \in S_1(K_0)$, $h(R;K)$ is the non forking extension of R to K i.e. the type over K corresponding to the ideal $I(R).K[X_{1\infty},\ldots,X_{k\infty}]$. This ideal is isomorphic to $I(R) \otimes_{K_0} K$ and will sometimes also be denoted as $I(R)$. In such a way, I^0 may denote an ideal of $K'[X_\infty]$ for any $K' \succeq K_0$.

. $P(L)$ is the set of realizations of P in L.

Definition: 1. $A \subseteq P^k$ is λ-closed in P^k, with parameters from K, if it is the trace on P^k of some λ-closed subset, with parameters from K, of the affine space, i.e. $A = V(I) \cap P^k$.

2. If $A = V(I) \cap P^k$, A is λ-closed of finite type in P^k if it is the trace of some λ-closed subset of finite type of the affine space.

Remarks:

1. A possible interpretation of λ-closed subsets of P^k is as follows. Since P is a complete type, for $x = (x_1, \ldots, x_k) \in P^k$, all fields $K_0\langle x_i\rangle$ are K_0-isomorphic to $K_0\langle P\rangle$. The question arises how these k copies of $K_0\langle P\rangle$ relate to each other, and relate to K. If K and all $K_0\langle x_i\rangle$'s are linearly disjoint over K_0 (which is possible, since the extensions $K_0 \subseteq K$ and $K_0 \subseteq K_0\langle x_i\rangle$ are regular), then $K[x_{1\infty}, \ldots, x_{k\infty}] \simeq_K K \otimes_{K_0} K_0[x_{1\infty}] \otimes_{K_0} \ldots \otimes_{K_0} K_0[x_{k\infty}]$ and $I(x, K) = \sum I(P_i) \otimes_{K_0} K = I(h(P_1 \otimes \ldots \otimes P_k; K))$. At the other extreme, the fields $K_0\langle x_i\rangle$ may coincide, for example if $x_1 = x_2 = \ldots = x_k$.

For $A = V(I) \cap P^k$, the condition "$x \in A$" is equivalent to the following

each $K_0\langle x_i\rangle \simeq_{K_0} K_0\langle P\rangle$ and
$K[x_{1\infty}, \ldots, x_{k\infty}]$ is a quotient of $K[X_{1\infty}, \ldots, X_{k\infty}]/I$.

2. For $A = V(I) \cap P^k$, A is the set of points of $V(I + \sum I(P_i))$ having their coordinates generic in the λ-closed set defined (over K_0) by the ideal $I(P)$. Hence A is not λ-closed in the affine space, except when P is realized in K_0.

3. Any λ-closed subset of P^k is $\bigwedge$-definable in L^k over some set of cardinality $|K_0|^+$.

4. A λ-closed subset $A = V(I) \cap P^k$ of P^k is of finite type iff $A = D \cap P^k$ for some D definable in the affine space iff $A = V(I_{\leq n}) \cap P^k$ for some integer n (by compactness applied to : $x \in P^k \vdash x \in D \leftrightarrow \bigwedge_n x \in V(I_{\leq n})$).

Proposition 4.1 *The map $A \to I(A)$ defines a bijection between the non empty λ-closed subsets of P^k and the ideals I of $K[X_{1\infty}, \ldots, X_{k\infty}]$ such that $I = \cap\{Q; Q \in \mathcal{Q}\}$, with a non empty*

$$\mathcal{Q} := \{Q \textit{ an ideal of } K[X_{1\infty}, \ldots, X_{k\infty}]; Q \textit{ is prime, separable, } Q \supseteq I$$

$$\textit{and } Q \cap K_0[X_{i\infty}] = I(P_i) \textit{ for } i = 1, \ldots, k\}$$

(in particular such an ideal I is separable and satisfies $I \cap K_0[X_{i\infty}] = I(P_i)$, for $i = 1, \ldots, k$). The inverse map is $I \to V(I) \cap P^k$.

Proof: If A is a λ-closed subset of P^k, it is Λ-definable, hence

$$I(A) = \cap\{I(R); R \text{ a complete } k\text{-type over } K, R \vdash A\}.$$

Now each $I(R)$ is prime, separable, extends $I(A)$ and, as A is contained in P^k and is not empty, intersects each $K_0[X_{i\infty}]$ in $I(P_i)$. Conversely, let I be some ideal of $K[X_{1\infty}, \dots, X_{k\infty}]$ satisfying $I = \cap\{Q; Q \in \mathcal{Q}\}$, for $\mathcal{Q} := \{Q; Q$ prime, separable, $Q \supseteq I$ and $Q \cap K_0[X_{i\infty}] = I(P_i)$ for $i = 1, \dots, k\}$ non empty, and $g \in K[X_{1\leq n}, \dots, X_{k \leq n}] \setminus I$. Then $g \notin Q_{n+m}$ for some $Q = I(R) \in \mathcal{Q}$ and every integer m, hence

$$K\langle R\rangle \models \exists x\ [Q_{\leq n+m}(x) = 0 \wedge g(x) \neq 0].$$

The same argument as in 3.3, using this time the $|K_0|^+$-saturation of L, shows

$$L \models \exists x\ [I(x) = 0 \wedge \wedge_{i=1}^{k} I(x_i; K_0) = I(P_i) \wedge g(x) \neq 0],$$

in other words

$$L \models \exists x\ [x \in (P^k \cap V(I)) \wedge g(x) \neq 0].$$

It follows that $g \notin I(P^k \cap V(I))$. □

A reducible (respectively irreducible) λ-closed subset of the affine space may have an irreducible (respectively a reducible) trace on P^k, but an irreducible λ-closed subset of P^k is the trace of some irreducible λ-closed subset of the affine space, as we have:

Proposition 4.2 *A λ-closed subset A of P^k is irreducible in P^k iff $V(I(A))$ is irreducible in the affine space iff $I(A)$ is prime.*

Proof: Same proof as for 3.11. □

So, as in the case of affine space, a λ-closed subset A of P^k is irreducible iff $I(A)$ is prime iff there is an $x \in L^k$ such that $I(x) = I(A)$. All such x have the same type, which completes P^k and is the type corresponding to $I(A)$. They are the generic points of $V(I(A))$ (as a closed subset of the affine space) and also the generic points of A (as a closed subset of P^k).

From 4.2 follows:

Corollary 4.3 *Let $C \subseteq A$ be λ-closed subsets of P^k. Then C is an irreducible component of A (in P^k) iff $V(I(C))$ is an irreducible component of $V(I(A))$ (in the affine space).*

Proof: C is an irreducible component of A in P^k iff $I(C)$ is a type ideal containing $I(A)$ and minimal among ideals corresponding to a type completing P^k. But, in this case, $I(C)$ is also minimal among all type ideals containing $I(A)$. Indeed for Q such an ideal, $I(A) \subseteq Q \subseteq I(C)$, hence, for each $i = 1, \dots, k$,

$$I(P_i) = I(A) \cap K[X_{i\infty}] \subseteq Q \cap K[X_{i\infty}] \subseteq I(C) \cap K[X_{i\infty}] = I(P_i),$$

hence $I(Q) \cap K[X_{i\infty}] = I(P_i)$. □

Remark 4.4 *An ideal I of $K[X_{1\infty},\dots,X_{k\infty}]$, separable and intersecting each $K[X_{i\infty}]$ in $I(P_i)$, is the canonical ideal of some λ-closed subset of the affine space, thus $I = \cap\mathcal{Q}$ for $\mathcal{Q} :=$ { minimal prime ideals containing I }. Let us define*

$$\mathcal{Q}_1 := \{Q \in \mathcal{Q}; Q \cap K[X_{i\infty}] = I(P_i),\ for\ i = 1,...,k\}.$$

Then $V(I) \cap P^k \neq \emptyset$ iff $\mathcal{Q}_1 \neq \emptyset$, and in this case $I(V(I) \cap P^k) = \cap\mathcal{Q}_1$.

Proof: 1. Clearly any $Q \in \mathcal{Q}_1$ is an $I(R)$ for some type R satisfying $R \subseteq V(I) \cap P^k$. Hence $\mathcal{Q}_1 \neq \emptyset$ implies that $V(I) \cap P^k \neq \emptyset$.
2. One has

$$V(I) \cap P^k \subseteq V(I) \cap V(I(P^k)),$$

hence by 3.7

$$I(V(I) \cap P^k) \supseteq I(V(I) \cap V(I(P^k))) = I + I(P^k) = I.$$

Consequently any $m \in V(I) \cap P^k$ satisfies $I(m) \supseteq I$ and, by definition of $\mathcal{Q}$, there is $Q \in \mathcal{Q}$ satisfying $I(m) \supseteq Q \supseteq I$. But, as we saw in the proof of 4.3, such a Q must belong to $\mathcal{Q}_1$. Thus $V(I) \cap P^k \neq \emptyset$ implies that $\mathcal{Q}_1 \neq \emptyset$.
3. Clearly $I(V(I) \cap P^k) \subseteq \cap\mathcal{Q}_1$. Conversely, let $f \in K[X_{1\infty},\dots,X_{k\infty}] \setminus I(V(I) \cap P^k)$ and $m \in V(I) \cap P^k$ satisfying $f(m) \neq 0$. As previously, there is $Q \in \mathcal{Q}$, hence $Q \in \mathcal{Q}_1$, satisfying $I \subseteq Q \subseteq I(m)$ and a fortiori $f \notin Q$. □

We can give an example of a separable ideal I intersecting each $K[X_{i\infty}]$ in $I(P_i)$ and not being the ideal of any λ-closed subset of P^k. Take $I = Q_1 \cap Q_2$ in $K[X_\infty, Y_\infty]$, for

$Q_1 := (I(P(X)), X - Y)$

$Q_2 := (X - a, Y - b)$,

where a and b are two distinct zeros of $I(P)$ in K_0. In this case $I \subset Q_1 = I(V(I) \cap P^2)$.

5 λ-closed subsets of a minimal type

We now add the further condition that the complete type we are working with is minimal (see definition after 2.15). We still have $K_0 \preceq L \models T_{p,\nu}$ and L is $|K_0|^+$-saturated; $P \in S_1(K_0)$ is a minimal type.

We are going to show that P is Zariski, in the sense of [Mar] section 5. First let us recall the meaning of the U-rank, (or Lascar rank) which is used in this definition, in our specific context.

Definitions: Suppose P minimal. Let $K_0 \preceq K \preceq L$ and $x_1,\dots,x_{k+1} \in P(L)$.

1. The rank over K of a tuple from P is defined inductively as follows:
$$\begin{aligned} rk(x_1;K) &= 0 \text{ if } x_1 \in K \\ &= 1 \textit{ if not}, \end{aligned}$$

and,

$$\begin{aligned} rk(x_1,...,x_k,x_{k+1};K) &= rk(x_1,...,x_k;K) && \text{if } x_{k+1} \in K\langle x_1,...,x_k\rangle \\ &= rk(x_1,...,x_k;K)+1 && \text{if not} \end{aligned}$$

(the consistancy of this definition follows from the minimality of P).

2. We will say that $x_1,\ldots,x_k$ are independent over K if $rk(x_1,...,x_k;K) = k$, or equivalently $I(x_1,...,x_k,K) = \sum I(P_i)$.

3. For A an $\wedge$-definable subset of P^k, with parameters from K_A, where $K_0 \preceq K_A \preceq L$ and $|K_0| = |K_A|$,

$$rk(A) := \max\{rk(x;K_A); x \in A(L)\}.$$

This rank does not depend on the choice of such a K_A (nor on L).

As particular $\wedge$-definable subsets A of P^k with few parameters, we will consider λ-closed subsets, with arbitrary parameters from L. Indeed as noted previously such an A requires only countably many parameters: the elements of a field of definition F_A of $I(A,L)$. We will consider A to be defined over some K_A, $F_A \subseteq K_A$, $K_0 \preceq K_A \preceq L$, $|K_A| = |K_0|$, to follow the conventions of the previous sections. We will say that A is irreducible if it is irreducible as a λ-closed set over K_A. The following facts tell us that working over such a field of definition is legitimate.

Fact 5.1 1) *Let $K \preceq L$ and I be an ideal of $K[X_{1\infty},\ldots,X_{k\infty}]$. Then I is prime or separable iff $I \otimes_K L$ is.*
2) *Let A be a λ-closed subset of L^k defined over K_A, $K_A \preceq K \preceq L$. Then A is irreducible as a K_A-closed set iff it is irreducible as a K-closed set.*

Proof: 1) Let J be an ideal of some ring $K[X_1,\ldots,K_m]$, generated by $f_1,\ldots,f_n$ and for each $i \leq n$, let b_i denote the sequence of coefficients of f_i. Then the fact that J is prime, or separable, is a first order property of the $b_i's$ in K (see for example [De 88]). The result then follows by elementary inclusion.
2) is a direct consequence of 1). □

Fact 5.2 *Let A be an irreducible λ-closed subset of $P(L)^k$, defined over K_A, satisfying $K_0 \preceq K_A \preceq L$ and $|K_0| = |K_A|$. Then $P(L)^k$ contains generic points over K_A and one has for such a's,*

$$rk(A) = rk(a;K_A).$$

Proof: The existence of such a's follows from the $|K_0|^+$-saturation of L. Now $a \in P(L)^k$ is generic over K_A iff $I(a,K_A) = I(A,K_A) \subseteq I(x,K_A)$, for each $x \in A$. If $rk(x;K_A) = r = rk(x_{i_1},...,x_{i_r};K_A)$, we have $I(x,K_A) \cap K_A[X_{i_1},...,X_{i_r}] = \sum_{j=1}^r I(P_{i_j})$, which implies $I(a,K_A) \cap K_A[X_{i_1},...,X_{i_r}] = \sum_{j=1}^r I(P_{i_j})$ and hence that $rk(a;K_A) \geq r$. □

We will see below (Proposition 5.6) that any λ-closed subset of a minimal type is of finite type. Hence in order to show that any minimal type is a Zariski geometry in the sense of [Mar] section 5, we must show that the following conditions hold.

i) Every λ-closed set in P^k is a finite union of irreducible λ-closed sets.

ii) If $A \subset B$ are λ-closed subsets of P^k and B is irreducible, then $rk(A) < rk(B)$.

iii) (Dimension theorem) If A is a λ-closed irreducible subset of P^k, $rk(A) = m$ and $B = \{\overline{x} \in P^k : x_i = x_j\}$, then $rk(C) \geq m-1$ for every non-empty irreducible component C of $A \cap B$.

Proposition 5.3 *Let P be minimal, $(a_1, ..., a_k) \in P^k$ and K, $K_0 \preceq K \preceq L$. Suppose that $a_1, ..., a_r$ are independent over K, and that $a_{r+1}, ..., a_k$ are algebraic over $(K, a_1, ..., a_r)$, hence separably algebraic over $K(a_{1\infty}, ..., a_{r\infty})$. Choose n such that*

$$[K(a_{1\infty}, ..., a_{r\infty})(a_{r+1}, ..., a_k) : K(a_{1\infty}, ..., a_{r\infty})] =$$

$$[K(a_{1\leq n}, ..., a_{r\leq n}, a_{r+1}, ..., a_k) : K(a_{1\leq n}, ..., a_{r\leq n})].$$

Let $Q = I(a_1, ..., a_k, K)$ and define, for $m \in \omega$,

$$M_m = K[X_{1\leq n+m}, ..., X_{r\leq n+m}, X_{r+1\leq m}, ..., X_{k\leq m}].$$

(1) There is $d \in K[X_{1\leq n}, ..., X_{r\leq n}] \setminus \sum_{i=1}^{r} I(P_i)_{\leq n}$ such that, for each $i = r+1, ..., k$, $m \in \mathbb{N}$ and $j \in p^{\nu m}$,

$$a_i \in K[a_{1\leq n}, ..., a_{r\leq n}, a_i^{p^m}, d(a_1, ..., a_r)^{-1}],$$

$$a_{i,j} \in K[a_{1\leq n+m}, ..., a_{r\leq n+m}, a_i, d(a_1, ..., a_r)^{-1}].$$

(2) $h(P_1 \otimes ... \otimes P_r; K)(x_1, ..., x_r) \cup \{f_1(x) = ... = f_l(x) = 0\} \vdash tp(a_1, ..., a_k; K)$,

for $f_1, ... f_l$ generating $Q \cap M_0$.

(3) Q is the unique prime separable ideal of $K[X_{1\infty}, \dots, X_{k\infty}]$ which intersects $K[X_{1\infty}, ..., X_{r\infty}]$ in $\sum_{i=1}^{r} I(P_i)$ and contains $\sum_{i=r+1}^{k} I_i^0$ and $Q \cap M_0$.

(4) $Q \cap M_m$ is the unique prime separable ideal of M_m which intersects $K[X_{1\leq n+m}, ..., X_{r\leq n+m}]$ in $\sum_{i=1}^{r} I(P_i)_{\leq n+m}$, and contains $\sum_{i=r+1}^{k} I_{i\leq m}^0$ and $Q \cap M_0$.

(5) $Q \cap M_m$ is the unique minimal prime separable ideal of M_m which intersects each $K[X_{i\leq n+m}]$ in $I(P_i)_{\leq n+m}$ for $i = 1, ..., r$, and each $K[X_{i\leq m}]$ in $I_{i\leq m}^0$ for $i = r+1, ..., k$, contains $Q \cap M_0$ and not d.

(6) Q is the unique minimal prime separable ideal of $K[X_{1\infty}, \dots, X_{k\infty}]$ which intersects each $K[X_{i\infty}]$ in $I(P_i)$ for $i = 1, ..., k$, contains $Q \cap M_0$ and not d.

Proof: (1) Since each a_i is separable over $K(a_{1\leq n}, ..., a_{r\leq n})$, by 2.5, there is a polynomial $d \in K[X_{1\leq n}, ..., X_{r\leq n}] \setminus \sum_{i=1}^{r} I(P_i)_{\leq n}$ such that, for $i = r+1, ..., k$ and for all $m \in \mathbb{N}$,

$$a_i \in K[a_{1\leq n}, ..., a_{r\leq n}, a_i^{p^m}, d(a_1, ..., a_r)^{-1}].$$

Hence, for some $e \in \mathbb{N}$,

$$d(a_1, ..., a_r)^{p^m \cdot e}.a_i = b_i(a_1, ..., a_r, a_i)$$

with $b_i \in K[X_{1\leq n}, ..., X_{r\leq n}, X_i^{p^m}]$. We can decompose

$$b_i(X_1, ..., X_r, X_i) \equiv \sum_{j \in p^{\nu m}} b_{ij}(X_1, ..., X_r, X_i)^{p^m}.m_j \text{ (modulo } \sum_{i=1}^{r} I_i^0)$$

with $b_{ij} \in K[X_{1\leq n+m}, ..., X_{r\leq n+m}, X_i]$, which proves

$$a_{i,j} = b_{ij}(a_1, ..., a_r, a_i).d(a_1, ..., a_r)^{-e} \in K[a_{1\leq n+m}, ..., a_{r\leq n+m}, a_i, d(a_1, ..., a_r)^{-1}].$$

(2) is an equivalent formulation of (3).

(3) If Q' is an ideal of type satisfying the conditions, it does not contain d and it contains the polynomials

$$d(X_1, ..., X_r)^{p^m \cdot e}.X_i - b_i(X_1, ..., X_r, X_i)$$

for $i = r+1, ..., k$, because these polynomials belong to $M_0 \cap Q$. Since Q' contains $\sum_1^k I_i^0$ and is separable, the proof of (1) above shows that Q' contains the polynomials

$$d(X_1, ..., X_r)^e.X_{ij} - b_{ij}(X_1, ..., X_r, X_i).$$

Hence Q' describes the same type as Q, and $Q' = Q$.

(4) For q such an ideal of M_m, M_m/q is K-isomorphic to $K[a_{1\leq n+m}, ..., a_{r\leq n+m}, a_{r+1\leq m}, ..., a_{k\leq m}]$.

(5) Let q be an ideal satisfying the condition. By the proof of (3), it contains $d(X_1, ..., X_r)^e.X_{ij} - b_{ij}(X_1, ..., X_r, X_i)$. Let $R_m = M_m[d^{-1}]$. In R_m, the ideal generated by $Q \cap M_0, \sum_{i=1}^{k}(I(P_i) \cap M_m)$, and the polynomials $d(X_1, ..., X_r)^e.X_{ij} - b_{ij}(X_1, ..., X_r, X_i)$ for $i = r+1, ..., k$ and $j \in p^{\nu m}$, is prime and therefore equals the ideal generated by $Q \cap M_m$. Hence $R_m.q \supseteq R_m.(Q \cap M_m)$. Since $d \notin q$, $R_m.q$ and $R_m.(Q \cap M_m)$ intersect M_m respectively in q and $Q \cap M_m$, therefore $q \supseteq Q \cap M_m$.

(6) is obvious from (5). □

Proposition 5.4 *Let P be minimal and $A \subset B$ be two λ-closed irreducible subsets of P^k. Then $rk(A) < rk(B)$.*

Proof: We assume A non empty. Define $r := rk(A), l := rk(B)$. By definition of the rank, $r \leq l$. Let K be a field containing fields of definition for $I(A, L)$ and $I(B, L)$, chosen such that $K_0 \preceq K \preceq L$ and $|K_0| = |K|$. In the rest of the proof, genericity, independance and canonical ideals are relative to K. Let a and b be generics of A and B respectively, then $I(a) = I(A) \supseteq I(b) = I(B)$. Hence, if $a_{i_1}, ..., a_{i_r}$ are independent, so are $b_{i_1}, ..., b_{i_r}$. Reorder the indices so that $a_1, ..., a_r$ are independent, and $b_1, ..., b_l$ are independent. Choose n so that $b_{l+1}, ..., b_k$ are separably algebraic over $K(b_{1\leq n}, ..., b_{l\leq n})$ and $a_{r+1}, ..., a_k$ separably algebraic over $K(a_{1\leq n}, ..., a_{r\leq n})$, and define

$$M_m = K[X_{1\leq n+m}, ..., X_{l\leq n+m}, X_{l+1\leq m}, ..., X_{k\leq m}].$$

Then $\dim(I(B) \cap M_m) = \dim(I(B) \cap K[X_{1\leq n+m}, ..., X_{l\leq n+m}])$ and

$$\dim(I(A) \cap M_m) = \dim(I(A) \cap K[X_{1\leq n+m}, ..., X_{l\leq n+m}]),$$

where "dim" here denotes the Krull dimension of the ideal. Now,

$$I(A) = \cup_m (I(A) \cap M_m),$$

$$I(B) = \cup_m (I(B) \cap M_m),$$

and $I(A) \supset I(B)$. So for some m, $I(A) \cap M_m$ strictly contains $I(B) \cap M_m$. Since they are both prime, this implies $\dim(I(A) \cap M_m) < \dim(I(B) \cap M_m)$, and therefore $I(A) \cap K[X_{1\leq n+m}, ..., X_{l\leq n+m}]$ strictly contains $I(B) \cap K[X_{1\leq n+m}, ..., X_{l\leq n+m}]$, i.e. $a_1, ..., a_l$ are not independent. □

Corollary 5.5 *Idem with A non necessarily irreducible.*

Proof: A is the union of its irreducible λ-components. □

Proposition 5.6 *If P is minimal, any λ-closed subset of P^k is of finite type.*

Proof: The proof is by induction on the rank of a λ-closed subset A of P^k. If $rk(A) = 0$ then (by compactness and by $|K_0|^+$-saturation of L) A is finite. Suppose the result true for all λ-closed subsets of P^k of rank $< r$.

Claim: If R is a complete type of rank $\leq r$ realized in P^k, then $V(I(R) \cap P^k)$ is of finite type.

Proof of the Claim: Take a field K, containing a field of definition for $I(R, L)$ and satisfying $K_0 \preceq K \preceq L$ and $|K_0| = |K|$, and consider ranks and canonical ideals above K. As in 5.3, find n and d and define M_m such that $I(R)$ is the unique minimal prime separable ideal of $K[X_{1\infty}, \ldots, X_{k\infty}]$ intersecting each $K[X_{i\infty}]$ in $I(P_i)$, containing $I(R) \cap M_0$ and not d. By 5.5, as $I(R)$ is irreducible, the λ-closed subset B of P^k defined by $B := V(I(R), d) \cap P^k$ has rank $\leq r - 1$, and therefore, by induction hypothesis,

$$B = V(I(R) \cap M_m, d) \cap P^k,$$

for some m. We prove now that $V(I(R)) \cap P^k = V(I(R) \cap M_m) \cap P^k$. Let $a \in V(I(R) \cap M_m) \cap P^k$. If $d(a) \neq 0$ then $I(a)$ contains $I(R)$, as it contains $\sum_{i=1}^k I(P_i)$, $I(R) \cap M_0$ and not d. If $d(a) = 0$, then $a \in B$, hence $a \in V(I(R))$. □

Let now A be a λ-closed subset of P^k of rank r, defined over K, $K_0 \preceq K \preceq L$ and $|K_0| = |K|$, and R_α, $\alpha < \alpha_0$, the distinct complete k-types over K completing A. Hence, working over K, we have the equivalence

$$P^k(x) \vdash x \in A \leftrightarrow \vee_{\alpha<\alpha_0} R_\alpha(x) \leftrightarrow \vee_{\alpha<\alpha_0} x \in V(I(R_\alpha)).$$

Now, each R_α has rank $\leq r$ and, by the claim, modulo P^k, each $V(I(R_\alpha))$ is of finite type. Hence the above equivalence holds between an infinite conjunction (the definition of A) and an infinite disjunction. By compactness it is also equivalent to a finite subdisjunction. □

Proposition 5.7 *If P is minimal, each λ-closed subset of P^k is union of finitely many irreducible λ-closed subsets of P^k.*

Proof: Follows from the proof of 5.6. □

Now we can prove the Dimension theorem:

Proposition 5.8 *Let P be minimal, A an irreducible λ-closed subset of P^k of rank r, B a diagonal hyperplane of equation $X_{i_1} = X_{i_2}$, for some $i_1, i_2 \in \{1, ..., k\}$, and C a non-empty irreducible component of $A \cap B$. Then $rk(C) \geq r - 1$.*

The proof is rather long. The key argument is given by the following claim:

Claim: Let I and J be ideals of non empty λ-closed subsets of P^k, Q a minimal prime ideal containing $I + J$ and K, containing a field of definition of I, J and Q satisfying $K_0 \preceq K \preceq L$ and $|K_0| = |K|$. Suppose further that a is a generic zero of Q over K, $a \in P^k$, and that

$$rk(V(Q) \cap P^k) = rk(a_1, ..., a_l, K) = l.$$

Let $n \in \mathbb{N}$ be such that $a_{l+1}, ..., a_k$ are separably algebraic over $K(a_{1\leq n}, ..., a_{l\leq n})$, with

$$[K(a_{1\infty}, ..., a_{l\infty}, a_{l+1}, ..., a_k) : K(a_{1\infty}, ..., a_{l\infty})] =$$
$$[K(a_{1\leq n}, ..., a_{l\leq n}, a_{l+1}, ..., a_k) : K(a_{1\leq n}, ..., a_{l\leq n})].$$

For $m, n_1, ..., n_k \in \mathbb{N}$, define

$$M_{m,(n_1,\dots,n_k)} := K[X_{1\leq n_1+m},\dots,X_{k\leq n_k+m}],$$

and for any $\mathcal{I} \subseteq K[X_{1\infty},\dots,X_{k\infty}]$, $\mathcal{I}_{m,(n_1,\dots,n_k)} := M_{m,(n_1,\dots,n_k)} \cap \mathcal{I}$.
Then there exists some integer N such that for each $m, n_1, \dots, n_k$ satisfying $n_1,\dots,n_l \geq n + n_{l+1},\dots,n+n_k$, $Q_{m,(n_1,\dots,n_k)}$ is the intersection of $M_{m,(n_1,\dots,n_k)}$ with some minimal prime ideal of $M_{N+m,(n_1,\dots,n_k)}$ containing $I_{N+m,(n_1,\dots,n_k)} + J_{N+m,(n_1,\dots,n_k)}$.

Note that, for $n_1 = \dots = n_l = n$, $n_{l+1} = \dots = n_k = 0$ and $\overline{n} := (n_1,\dots,n_k)$, the ring considered in and after 5.3,

$$M_m := K[X_{1\leq n+m},\dots,X_{l\leq n+m},X_{l+1\leq m},\dots,X_{k\leq m}],$$

is equal to $M_{m,\overline{n}}$. Also a particular case of the claim asserts that $Q \cap M_m$ is the intersection of M_m with some ideal of M_{N+m} which is minimal prime over $I_{N+m} + J_{N+m}$.

Proof of the Claim: In order to simplify notation, we rename
$Y = (X_{1\leq n},\dots,X_{l\leq n})$
X any of the variables $X_{l+1},\dots,X_k$, say X_{l+1}.
by Proposition 5.3 there is $d \in K[Y] \setminus Q$ such that

$$a_{l+1} \in K[a_{1\leq n},\dots,a_{l\leq n},d(a_1,\dots,a_l)^{-1},a_{l+1}^{p^m}],$$

for each integer m. Hence, for each m, there are some $e \in K[X,Y]$ and $\sigma \in \mathbb{N}$, such that

$$(*) \qquad d(Y)^{p^m\cdot\sigma}.X + e(X^{p^m},Y) \in Q \cap M_0.$$

Now $I + J$ is separable by 3.8 and by the Nullstellensatz is an intersection of type ideals, which we can choose minimal. By 5.7 only finitely many of them, say $Q_1,\dots Q_r$, correspond to types completing P^k, hence

$$I + J = Q_1 \cap \dots \cap Q_r \cap S$$

with $V(S) \cap P^k = \emptyset$. By 4.3 each Q_i is minimal over $I + J$ and by 3.10, Q is one of them, say Q_1. Take $g \in Q_2 \cap \dots \cap Q_r \cap S \setminus Q$. Then $g.Q \subseteq I + J$. Fix $N \in \mathbb{N}$ such that

$$g \in K[X_{\leq N},Y_{\leq N}], \text{ and further}$$
$$g.(Q \cap M_0) \subseteq (I \cap M_N) + (J \cap M_N).$$

Then, by $(*)$, there exist $u \in I \cap M_N$ and $v \in J \cap M_N$ such that

$$g^{p^m}.[d(Y)^{p^m\cdot\sigma}.X + e(X^{p^m},Y)] = u + v.$$

Let us decompose

$$e(X^{p^m},Y) \equiv \sum_{j\in p^{\nu m}} e_j^{p^m}.m_j \text{ (modulo } (\sum_i I_i^0) \cap M_m)$$

$$u \equiv \sum_{j \in p^{\nu m}} u_j^{p^m}.m_j \text{ (modulo } (\sum_i I_i^0) \cap M_{N+m})$$

$$v \equiv \sum_{j \in p^{\nu m}} v_j^{p^m}.m_j \text{ (modulo } (\sum_i I_i^0) \cap M_{N+m}),$$

where $e_j \in K[X, Y_{\leq m}], u_j$ and $v_j \in M_{N+m}$ and more precisely, since I and J are separable, $u_j \in I \cap M_{N+m}$ and $v_j \in J \cap M_{N+m}$. Therefore

$$\sum [g.(d^\sigma.X_j + e_j) - u_j - v_j]^{p^m}.m_j \in \sum_i I_i^0 \cap M_{N+m},$$

hence, by separability of $\sum_i I_i^0$,

$$g.(d^\sigma.X_j + e_j) - u_j - v_j \in \sum_i I_i^0$$

and finally, since I and J contain $\sum_i I_i^0$,

$$g.(d^\sigma.X_j + e_j) \in (I \cap M_{N+m}) + (J \cap M_{N+m}).$$

We argue now for $X_{l+2}, ..., X_k$ just as we did for $X = X_{l+1}$, and so get an integer N and polynomials $\alpha_i \in K[X_{1 \leq n}, ..., X_{l \leq n}] \setminus Q$ and $g_i \in K[X_{i \leq N}, X_{1 \leq n+N}, \ldots, X_{l \leq n+N}] \setminus Q$, for $i = l+1, ...k$, such that:
for all $m \in \mathbb{N}$ and $j \in p^{\nu m}$, there are $\beta_{i,j} \in K[X_i, X_{1 \leq n+N+m}, ..., X_{l \leq n+N+m}]$ for which $g_i.(\alpha_i.X_{i,j} + \beta_{i,j}) \in (I \cap M_{N+m}) + (J \cap M_{N+m})$.
By applying this result to $j \in p^{\nu(m+n_i)}$, we get

$$g_i.(\alpha_i.X_{i,j} + \beta_{i,j}) \in (I \cap M' + J \cap M'),$$

with

$$M' := K[X_i, X_{1 \leq n+N+m+n_i}, ..., X_{l \leq n+N+m+n_i}]$$
$$\subseteq K[X_i, X_{1 \leq N+m+n_1}, ..., X_{l \leq N+m+n_l}] \subseteq M_{N+m,\overline{n}}.$$

Since there is at most one prime ideal of $M_{m,\overline{n}}$ intersecting $K[X_{1\infty}, ..., X_{l\infty}]$ in $\sum_1^l I(P_i)_{\leq n_i+m}$, containing $Q \cap M_0$, each $g_i.(\alpha_i.X_{i,j} + \beta_{i,j})$ and no $\alpha_i.g_i$ for $i = l+1, ..., k$ and $j \in p^{\nu(m+n_i)}$, every prime ideal of $M_{N+m,\overline{n}}$ intersecting $K[X_{1\infty}, ..., X_{l\infty}]$ in $\sum_1^l I(P_i)_{\leq n_i+m+N}$, containing $I_{N+m,\overline{n}}$ and $J_{N+m,\overline{n}}$ and no $\alpha_i.g_i$, intersects $M_{m,\overline{n}}$ in $Q_{m,\overline{n}}$. □

Proof of Proposition 5.8 : Let us choose once more a field K, containing fields of definition for $I(A, L), I(B, L)$ and $I(C, L)$, satisfying $K_0 \preceq K \preceq L$ and $|K_0| = |K|$. Independence and genericity are considered relatively to this K.

Definition: We will say that $X_{i_1}, ..., X_{i_l}$ are <u>independent modulo some irreducible</u> λ-<u>closed subset</u> F <u>of</u> P^k if , for $(a_1, ..., a_k)$ a generic point of F,

$a_{i_1}, \ldots, a_{i_l}$ are independent. One variable $X_{i_{l+1}}$ is <u>algebraic over</u> $X_{i_1}, \ldots, X_{i_l}$ <u>modulo</u> F if $a_{i_{l+1}} \in K\langle a_{i_1}, \ldots a_{i_l}\rangle$.

We come back to the proof of 5.8. If $A \cap B = \emptyset$ or $A \subseteq B$, there is nothing to prove. Suppose therefore that $A \cap B$ is non empty and that $A \cap B \neq A$.

I. We consider first the case where X_{i_1} and X_{i_2} are independent modulo A and X_{i_1} independent modulo C. Thus we are allowed to rename $X_1, \ldots, X_k$ as X, U, V, Y, Z where
- X, Y, Z are tuples, we will then denote their length by ℓ,
- U and V are variables,
- modulo A, (X, U, V, Y) is independent, and Z algebraic over (X, U, V, Y),
- the equation defining B is $U = V$,
- modulo C, (X, U) is independent, and V, Y, Z are algebraic over (X, U)

(U and V are given, choose X and then Y). So we have to prove that there is in fact no Y, in other words that $\ell Y = 0$.

Let $n \in \mathbb{N}$ be such that
- modulo $I(A)$, Z is algebraic over $K(X_{\leq n}, U_{\leq n}, V_{\leq n}, Y_{\leq n})$ of same degree as over $K(X_\infty, U_\infty, V_\infty, Y_\infty)$,
- modulo $I(C)$, V, Y and Z are algebraic over $K(X_{\leq n}, U_{\leq n})$ of same degree as over $K(X_\infty, U_\infty)$.

We are going to work with variables $X_{\leq 2n+m+m'}, U_{\leq 2n+m+m'}, V_{\leq n+m}, Y_{\leq n+m+m'}$ and $Z_{\leq m}$, where m and m' are arbitrary integers. Note that the depth of the components is chosen in order to witness the dependence relation modulo A or C. The corresponding polynomial ring is

$$M_{m,m'} := K[X_{\leq 2n+m+m'}, U_{\leq 2n+m+m'}, V_{\leq n+m}, Y_{\leq n+m+m'}, Z_{\leq m}].$$

For an ideal $\mathcal{I}$ of $K[X_{1\infty}, \ldots, X_{k\infty}]$ we define

$$\mathcal{I}_{m,m'} := \mathcal{I} \cap M_{m,m'}.$$

By Lemma 2.6, the ideals $I(A)_{m,m'}, I(B)_{m,m'}, I(C)_{m,m'}$ and, for all integer s, $I(P)_{\leq s}$ are absolutely prime and therefore define over L^a irreducible varieties, which we will denote by $A_{m,m'}, B_{m,m'}, C_{m,m'}$ and $\overline{P}_{\leq s}$. The varieties $A_{m,m'}, B_{m,m'}$ and $C_{m,m'}$ are subvarieties of

$$E_{m,m'} := \overline{P}^{\ell X+1}_{\leq 2n+m+m'} \times \overline{P}_{\leq n+m} \times \overline{P}^{\ell Y}_{\leq n+m+m'} \times \overline{P}^{\ell Z}_{\leq m}.$$

Let us now compute the dimensions of all these varieties. A generic point of $A_{m,m'}$ is the projection of some generic point of A (identifying x and x_∞ as in 3.12), and the same holds for $B_{m,m'}, C_{m,m'}, \overline{P}_{\leq s}$ and $E_{m,m'}$. Hence we have, using the function $f(s) := \dim(\overline{P}_{\leq s})$,

$$\dim(A_{m,m'}) = (\ell X + 1).f(2n + m + m') + f(n + m) + \ell Y.f(n + m + m')$$

$$\dim(B_{m,m'}) = (\ell X + 1).f(2n + m + m') + \ell Y.f(n + m + m') + \ell Z.f(m)$$

$$\dim(C_{m,m'}) = (\ell X + 1).f(2n + m + m')$$

$\dim(E_{m,m'}) = (\ell X+1).f(2n+m+m')+f(n+m)+\ell Y.f(n+m+m')+\ell Z.f(m)$.

By the claim, $C_{m,m'}$ is the projection over $E_{m,m'}$ of some irreducible component D of $A_{m+N,m'} \cap B_{m+N,m'}$ where N is independent of m and m'. This implies, if $\pi : E_{m+N,m'} \to E_{m,m'}$ is the canonical projection,

$$\dim(C_{m,m'}) = \dim D - \dim(\pi^{-1}(c))$$

for c a generic of $C_{m,m'}$, hence

$$\dim(C_{m,m'}) \geq \dim D + \dim(E_{m,m'}) - \dim(E_{m+N,m'}).$$

Consider the set

$$E := P^{\ell X+1}_{\leq 2n+m+m'+N} \times P_{\leq n+m+N} \times P^{\ell Y}_{\leq n+m+m'+N} \times P^{\ell Z}_{\leq m+N}$$

As $C \neq \emptyset, D \cap E \neq \emptyset$ too. Furthermore each point of $D \cap E$ is simple on D as each of its coordinates is generic, hence simple in the corresponding irreducible variety (see [Lan 58, VIII section 2, Prop.6]:

- $x_{1 \leq 2n+m+m'+N}, \ldots, x_{\ell X+1 \leq 2n+m+m'+N}$ are each generic points of $\overline{P}_{\leq 2n+m+m'+N}$,
- $x_{\ell X+2 \leq n+m+N}$ is generic in $\overline{P}_{\leq n+m+N}$,
- $x_{\ell X+3 \leq n+m+m'+N}, \ldots, x_{\ell X+\ell Y+2 \leq n+m+m'+N}$ are each generics of $\overline{P}_{\leq n+m+m'+N}$,
- $x_{\ell X+\ell Y+3 \leq m+N}, \ldots, x_{k \leq m+N}$ are each generics of $\overline{P}_{\leq m+N}$.

We can then apply, inside $E_{m+N,m'}$, the classical dimension theorem of algebraic geometry (see for instance [Lan 58, VIII section 5, theorem 5]), hence

$$\dim D \geq \dim(A_{m+N,m'}) + \dim(B_{m+N,m'}) - \dim(E_{m+N,m'}),$$

therefore

$$\dim(C_{m,m'}) \geq \dim(A_{m+N,m'})+\dim(B_{m+N,m'})+\dim(E_{m,m'})-2\dim(E_{m+N,m'}).$$

Substituting in this we obtain

$$0 \geq f(n+m) + \ell Y.f(n+m+m') + \ell Z.f(m) - \ell Z.f(m+N) - f(n+m+N).$$

On the second side of this inequality, m' occurs only in the second term, and we can choose it arbitrarily big. How do all these terms behave when one of m and m' goes to the infinity ?

1. If f is bounded on $\mathbb{N}$ (P is then said to be <u>thin</u>, thin types play a main role in the proof of Hrushovski, see the next section), all terms $f(m + ...)$ become equal for m big enough, which forces $\ell Y = 0$.
2. If $f(s) \to \infty$ for $s \to \infty$, let us fix m and let m' tend to ∞. Again ℓY must equal 0.

II. We consider now the case where X_{i_1} is independent modulo A, but (X_{i_1}, X_{i_2}) is not. Let $X \subseteq \{X_1, ..., X_k\}$ be a maximal independent subset modulo C.

Claim: Then X_{i_1} and X_{i_2} are algebraic over C, and either $X\frown X_{i_1}$ or $X\frown X_{i_2}$ is independent modulo A.

Proof: From $A \not\subseteq B$ follows $C \subset A$, therefore $I(A) \subset I(C)$, but also

$$(**) \qquad I(A) \cap K[X_\infty, X_{i_1,\infty}, X_{i_2,\infty}] \subset I(C) \cap K[X_\infty, X_{i_1,\infty}, X_{i_2,\infty}]$$

(if one of the variables X_{i_1} or X_{i_2} belongs to X, we do not repeat it in the polynomial ring above). Indeed, since the polynomials $X_{i_1,j} - X_{i_2,j}, j \in p^\infty$, all are in $I(C) \cap K[X_\infty, X_{i_1,\infty}, X_{i_2,\infty}]$ and, together with $\sum_{i=1}^k I_i^0$, generate $I(B)$, the equality

$$I(A) \cap K[X_\infty, X_{i_1,\infty}, X_{i_2,\infty}] = I(C) \cap K[X_\infty, X_{i_1,\infty}, X_{i_2,\infty}]$$

would imply $I(A) \supseteq I(B)$, whence $A \subseteq B$. Now X is independent modulo C and X_{i_1} and X_{i_2} are dependent modulo A. Then the conclusion of the claim follows from the strict inclusion $(**)$. □

Thus we are allowed as in the first case to reorder and rename $X_1, ..., X_k$ as X, U, V, Y, Z (X, Y, Z are tuples, U and V variables) such that
- X is independent maximal modulo C,
- (X, U, Y) is independent maximal modulo A, and
- the equation defining B is $U = V$.

We choose $n \in \mathbb{N}$ such that
- modulo $I(A)$, Z and V are algebraic over $K(X_{\leq n}, U_{\leq n}, Y_{\leq n})$ of same degree as over $K(X_\infty, U_\infty, Y_\infty)$,
- modulo $I(C)$, U, V, Y and Z are algebraic over $K(X_{\leq n})$ of same degree as over $K(X_\infty)$.

We define

$$M_{m,m'} := K[X_{\leq 2n+m+m'}, U_{\leq n+m+m'}, V_{\leq m}, Y_{\leq n+m+m'}, Z_{\leq m}],$$

and the varieties naturally associated $A_{m,m'}, B_{m,m'}, C_{m,m'}$ and $E_{m,m'}$, and analogously to the first case, the integer N and the subvariety D of $E_{m+N,m'}$. Then

$$\dim(A_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y + 1).f(n+m+m')$$

$$\dim(B_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y + 1).f(n+m+m') + \ell Z.f(m)$$

$$\dim(C_{m,m'}) = \ell X.f(2n+m+m')$$

$$\dim(E_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y + 1).f(n+m+m') + (\ell Z + 1).f(m).$$

The necessary inequality becomes

$$0 \geq -(\ell Z + 2).f(m+N) + (\ell Y + 1).f(n+m+m') + (\ell Z + 1).f(m),$$

which forces P to be thin and then ℓY to be zero.

III. The case where both X_{i_1} and X_{i_2} are algebraic modulo A is prohibited since this would imply that $a \in A \Rightarrow a_{i_1} = a_{i_2}$, therefore $A \subseteq B$.

IV. There remains to be considered the case where X_{i_1} and X_{i_2} are independent modulo A and become both algebraic modulo C. We introduce $X \subseteq \{X_1, ..., X_k\}$ maximal independent modulo C and consider as in the second case

$$K[X_\infty, X_{i_1,\infty}, X_{i_2,\infty}]$$

(without repetition) and the trace over this ring of the strict inclusion $I(A) \subset I(C)$. The same argument proves that either $X\frown X_{i_1}$ or $X\frown X_{i_2}$ is independent modulo A.

Let us prove that $X\frown X_{i_1}\frown X_{i_2}$ can not be independent modulo A. In this case, define $U := X_{i_1}$, $V := X_{i_2}$, Y such that X, U, V, Y are maximal independent modulo A, and Z the other variables. We consider as previously $n \in \mathbb{N}$ and

$$M_{m,m'} := K[X_{\leq 2n+m+m'}, U_{\leq n+m+m'}, V_{\leq n+m}, Y_{\leq n+m+m'}, Z_{\leq m}],$$

the varieties $A_{m,m'}, B_{m,m'}, C_{m,m'}$ and $E_{m,m'}$, the integer N and the variety D. Then

$$\dim(A_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y+1).f(n+m+m') + f(n+m)$$

$$\dim(B_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y+1).f(n+m+m') + \ell Z.f(m)$$

$$\dim(C_{m,m'}) = \ell X.f(2n+m+m')$$

$$\dim(E_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y+1).f(n+m+m') + f(n+m) + \ell Z.f(m),$$

and the inequality becomes

$$0 \geq -\ell Z.f(m+N) - f(n+m+N) + (\ell Y+1).f(n+m+m') + f(n+m) + \ell Z.f(m),$$

which is seen first implying that P is thin and then being impossible.

So we are in the case where

- (X, U, Y) is maximal independent modulo A, and V, Z are the other variables, and
- X is maximal independent modulo C.

Taking

$$M_{m,m'} := K[X_{\leq 2n+m+m'}, U_{\leq n+m+m'}, Y_{\leq n+m+m'}, V_{\leq m}, Z_{\leq m}],$$

we get

$$\dim(A_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y+1).f(n+m+m')$$

$$\dim(B_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y+1).f(n+m+m') + \ell Z.f(m)$$

$$\dim(C_{m,m'}) = \ell X.f(2n+m+m')$$

$$\dim(E_{m,m'}) = \ell X.f(2n+m+m') + (\ell Y+1).f(n+m+m') + (\ell Z+1).f(m),$$

and the inequality

$$0 \geq -(\ell Z + 2).f(m + N) + (\ell Y + 1).f(n + m + m') + (\ell Z + 1).f(m),$$

implies that P is thin and ℓY zero. □

Theorem 5.9 *Minimal types are Zariski.*

Proof: Condition i) is Proposition 5.7, ii) is Corollary 5.5 and iii) is Proposition 5.8. □

6 Thin types

Let $K \models T_{p,\nu}$.

Definition: A type $P \in S_1(K)$ is thin if the transcendence degree $tr(K\langle P\rangle, K)$ is finite. In this case, we define $RT(P) := tr(K\langle P\rangle, K)$. Otherwise $RT(P) = \infty$.

Proposition 6.1 1. *RT is a rank.*
2. *A thin type P is ranked and $RU(P) \leq RT(P)$.*

Proof: 1. follows from the characterization of forking we gave in section 2.
2. is proved by induction on $RT(P)$. For x realizing P and $L \succeq K$, $t(x, L)$ forks over K iff L and $K\langle x\rangle$ are not linearly disjoint over K iff $tr(L\langle x\rangle, L) < tr(K\langle x\rangle, K)$. □

Examples: 1. For $L \succeq K$ and P the type over K of an element of $L^{p^\infty} \setminus K$, $RU(P) = RT(P) = 1$.
2. If x and y are two independent realizations of the previous P and $z = x^p + by^p$ (b an element in the p-basis of K), then $RU(x, K) = RT(x, K) = 2$.
3. In [CCSSW], some types with $RU = 1$ and $RT = 2$ are described, and in [CWo], some minimal non thin types are constructed.

Thin types arise naturally in the context of algebraic groups over separably closed fields as was shown in [Hr 96, Lemma 2.15]:

Proposition 6.2 *Let $\underline{G}$ be an Abelian algebraic group defined over $K \models T_{p,\nu}$, $G := \underline{G}(K)$, $A := \cap p^n G$. Then generic types of A are thin.*

Claim (Weil, [We 48]): Let U be a variety defined over a field F of characteristic p, $M \in U$ generic over F and f a rational map $f : U^{p^n} \ldots \to F$, where n is an arbitrary integer, f defined with coefficients from F, defined at $(M, \ldots, M) \in U^{p^n}$

and symmetrical, which means that $f(M_1, ..., M_{p^n}) = f(M_{\sigma(1)}, ..., M_{\sigma(p^n)})$ for any permutation σ of $\{1, ..., p^n\}$. Then there is a rational map $g : U... \to F$ defined over $F^{p^{-n}}$, defined at M and such that $f(M, ..., M) = g(M)^{p^n}$.

The proof of this claim uses derivations, see [We 48, I.6, Lemma 4].

Proof of Proposition 6.2 : Let k be the dimension of $\underline{G}$, $G := \underline{G}(K)$, the group of K-rational points of $\underline{G}$, and $A := \bigcap_{n \in \mathbb{N}} p^n G$. Then A is a group, its domain is $\wedge$-definable in the separably closed field K and its law is rational over this field. The Zariski closure $\overline{A}$ of A is a variety with a rational map (the addition of A) generically defined on it. We apply the previous claim to it and to the map $f(x_1, ..., x_{p^n}) = \sum_1^{p^n} x_i$, where the $\sum$ refers to the addition in A. Each generic point a of $\overline{A}$ belongs to A, hence, for each integer n, a is of the form $p^n b_n$, for some $b_n \in A$, i.e. $a = f(b_n, ..., b_n)$. By the claim, $a \in K(b_n^{p^n})$, hence $a_{\leq n} \subseteq K(b_n)$. Now $tr(K\langle a \rangle, K) = tr(K(a_\infty), K) = sup\{tr(K(a_{\leq n}), K); n \in \omega\} \leq tr(K(b_n), K) \leq k$. □

References

[Bour] N. Bourbaki, XI, Algèbre, chapitre 5, *Corps commutatifs*, Hermann, Paris 1959.

[Bous] E. Bouscaren, *Proof of the Mordell-Lang conjecture for function fields*, this volume.

[ChKe] C. Chang and J. Keisler, *Model Theory*, North-Holland, Amsterdam 1973.

[CCSSW] Z. Chatzidakis, G. Cherlin, S. Shelah, G. Srour and C. Wood, *Orthogonality of types in separably closed fields*, in Classification Theory (Proceedings of Chicago, 1985), LNM 1292, Springer, 1987.

[CWo] Z. Chatzidakis and C. Wood, manuscript, 1996.

[De 88] F. Delon, *Idéaux et types sur les corps séparablement clos*, Supplément au Bulletin de la SMF, Mémoire 33, Tome 116 (1988).

[Er] Y. Ershov, *Fields with a solvable theory*, Sov. Math. Dokl. 8 (1967), 575-576.

[Hr 90] E. Hrushovski, *Unidimensional theories are superstable*, APAL 50 (1990), 117-138.

[Hr 96] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J.AMS 9 (1996), 667-690.

[Lan 58] S. Lang, *Introduction to algebraic Geometry*, Interscience Tracts in pure and applied Mathematics, Interscience Publishers, New York 1958.

[Lanl 65] S. Lang, Algebra, Addison-Wesley, 1965.

[Mar] D. Marker, *Zariski geometries*, this volume.

[Me 94] M. Messmer, *Groups and fields interpretable in separably closed fields*, TAMS 344 (1994), 361-377.

[Me 96] M. Messmer, *Some model theory of separably closed fields*, in Model Theory of Fields, Lecture Notes in Logic 5, Springer, 1996.

[Pil] A. Pillay, *Model theory of algebraically closed fields*, this volume.

[We 48] A. Weil, *Courbes algébriques et variétés abéliennes*, Hermann, Paris, 1948.

[Wo 79] C. Wood, *Notes on the stability of separably closed fields*, JSL 44 (1979), 412-416.

[Zie] M. Ziegler, *Introduction to stability theory and Morley rank*, this volume.