Preliminaries on Fields

Zoé Chatzidakis* (CNRS - Université Paris 7)

Contents

1 Review on fields

We review briefly well-know results in field theory. The notions and results specific to positive characteristic (p-bases, p-independence, etc...) can be found in Bourbaki [2]. The other unreferenced results come from Chapter III of Lang's book [38]. We assume a good knowledge of Galois theory.

1.1. Notation. Let A be a field. Then A^{alg} denotes the (field-theoretic algebraic) closure of A, and A^s the separable closure of A (i.e., the elements of A^{alg} which are separably algebraic over A). We denote by $G(A)$ the absolute Galois group of A, i.e., $G(A) = \mathcal{G}al(A^s/A)$. We often identify $G(A)$ with $Aut(A^{alg}/A)$.

If A and B are subfields of some larger field Ω, we denote by $A[B]$ or $B[A]$ the subring of Ω generated by A and B, and by AB the quotient field of $A[B]$.

*partially supported by MRTN-CT-2004-512234 and by ANR-06-BLAN-0183

If the characteristic of A is $p > 0$, then the map $x \mapsto x^p$ defines a monomorphism $A \to A$; the image of A under this homomorphism is denoted by A^p. We also define $A^{1/p} = \{a \in A^{alg} \mid a^p \in A\}$ and $A^{1/p^\infty} = \{a \in A^{alg} \mid a^{p^n} \in A \text{ for some } n \in \mathbb{N}\}$.

A field K is *perfect* if it is of characteristic 0, or if it is of characteristic $p > 0$, and $K^p = K$. The *perfect hull* of K is K^{1/p^∞}.

In what follows we will work within models of a complete theory T of fields, and if A is a subfield of a model F of T, then $acl(A)$ will denote the (model-theoretic) algebraic closure of A in F and $dcl(A)$ the (model-theoretic) definable closure of A in F.

1.2. Linear disjointness. We refer to Chapter III of Lang [38] for the proofs and details. Unless otherwise stated, we work inside some large algebraically closed field Ω, and K, L, M, E are subfields of Ω.

Assume that $K \subseteq L, M$. We say that L is *linearly disjoint from M over K* if every finite set of elements of L that is linearly independent over K remains linearly independent over M in the field composite LM.

Even though the definition is asymmetric, the property is symmetric: L is linearly disjoint from M over K if and only if M is linearly disjoint from L over K. Thus we will also say: L and M are *linearly disjoint over K*.

The following are equivalent:

(1) L and M are linearly disjoint over K.

(2) The canonical map $L \otimes_K M \to L[M]$ is an isomorphism.

(3) If $B \subset L$ is a basis of the K-vector space L, then B is a basis of the M-vector space $L[M]$.

1.3. Let $K \subseteq L, M$, and assume that L is algebraic over K. Then L and M are linearly disjoint over K if and only if $[K(a) : K] = [M(a) : M]$ for every finite tuple a from L. Assume that L is a finite Galois extension of K, linearly disjoint from M over K. Then $[L : K] = [ML : M]$ implies that $\mathcal{G}al(LM/M)$ is canonically isomorphic to $\mathcal{G}al(L/K)$ via the restriction map.

This has the following consequences:

(1) If L is a Galois extension of K, then L and M are linearly disjoint over K if and only if $L \cap M = K$, if and only if the restriction map : $\mathcal{G}al(LM/M) \to \mathcal{G}al(L/K)$ is an isomorphism (of profinite groups).

(2) If L and M are linearly disjoint over K and are Galois extensions of K, then $\mathcal{G}al(LM/K)$ is canonically isomorphic to $\mathcal{G}al(L/K) \times \mathcal{G}al(M/K)$.

(3) Note that (1) can fail when L is not Galois: consider e.g., $a \neq b \in \mathbb{Q}^{alg}$ such that $a^3 = b^3 = 2$; then $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$, and $[\mathbb{Q}(a, b) : \mathbb{Q}(a)] = 2 < [\mathbb{Q}(b) : \mathbb{Q}]$, which shows that $\mathbb{Q}(a)$ and $\mathbb{Q}(b)$ are not linearly disjoint over $\mathbb{Q}$.

1.4. Let $K \subseteq L, M$, and assume that E is a subfield of L containing K. Then L and M are linearly disjoint over K if and only if E and M are linearly disjoint over K and L and EM are linearly disjoint over E.

1.5. Let $K \subseteq L$, and let $u_1, \ldots, u_n$ be a tuple of elements of Ω which are algebraically independent over L. Then $K(u_1, \ldots, u_n)$ and L are linearly disjoint over K.

1.6. Let $\{L_i \mid i \in I\}$ be a family of extensions of K contained in Ω. We say that $\{L_i \mid i \in I\}$ is *linearly disjoint* over K, if for every $i \in I$, the field L_i and the field composite of $\{L_j \mid j \in I,\ j \neq i\}$ are linearly disjoint over K. Note that, by 1.4, if $<$ is a linear ordering on I, this is equivalent to: for every i, the field L_i and the field composite of $\{L_j \mid j < i\}$ are linearly disjoint over K.

1.7. Algebraic independence or freeness. Let $K \subseteq L, M$ be fields. We say that L and M are *free over* K, or that L and M are *algebraically independent over* K, if every finite set of elements of L which is algebraically independent over K remains algebraically independent over M. Again, this notion is symmetric.

If L and M are linearly disjoint over K, then L and M are algebraically independent over K. The converse is not true: if L is algebraic over K, then L is algebraically independent over K from any extension of K.

1.8. Separable extensions. Let $K \subseteq L$ be fields of characteristic $p > 0$. We say that L is a *separable extension* of K if the fields L and $K^{1/p}$ are linearly disjoint over K. If L is algebraic over K, this is equivalent to $L \subseteq K^s$, and in that case we have $KL^p = L$.

Remark. One extends the definition to the characteristic 0 case as follows: if $char(K) = 0$, then *any* field extension of K is *separable over* K.

1.9. The following conditions are equivalent:

(1) L is a separable extension of K.

(2) L and K^{1/p^∞} are linearly disjoint over K.

(3) Whenever u is a finite tuple from L, then $K(u)$ has a transcendence basis $\{t_1, \ldots, t_m\}$ over K, such that $K(u)$ is separably algebraic over $K(t_1, \ldots, t_m)$. Such a transcendence basis is called a *separating transcendence basis*.

(4) L^p and K are linearly disjoint over K^p.

1.10. Let $K \subseteq L \subseteq M$. If M is separable over L and L is separable over K then M is separable over K.

If M is separable over K, then L is separable over K, but M is not necessarily separable over L (e.g.: $K \subset K(t) \subset K(t^{1/p})$).

If M has a separating transcendence basis over K, then M is separable over K. The converse holds if M is a finitely generated field extension of K, but does not always hold in the general case. If the characteristic is $p > 0$, then $K(t^{p^{-n}} \mid n \in \mathbb{N})$ is a separable extension of K (since any finitely generated subextension is separable over K), but it does not have a separating transcendence basis over K.

1.11. Assume that L is a separable extension of K and that M is an extension of K algebraically independent from L over K. Then LM is a separable extension of M.

Assume that L and M are separable extensions of K, which are algebraically independent over K. Then LM is a separable extension of L and of M (and also of K).

1.12. Regular extensions. Let $K \subseteq L$. We say that L is a *regular extension of* K if the fields L and K^{alg} are linearly disjoint over K. In that case, the restriction map : $G(L) \to G(K)$ is onto.

The following conditions are equivalent:

(1) L is a regular extension of K.

(2) L is a separable extension of K, and L and K^s are linearly disjoint over K.

(3) L is a separable extension of K, and $L \cap K^s = K$.

(4) L is a separable extension of K, and the restriction map : $G(L) \to G(K)$ is onto.

1.13. Properties of regular extensions. Let $K \subseteq L, M$.

(1) If L is a regular extension of K and M is a regular extension of L, then M is a regular extension of K.

(2) If M is regular over K and $L \subseteq M$, then L is regular over K.

(3) Assume that L and M are linearly disjoint over K. Then L is regular over K if and only if LM is regular over M.

(4) If L and M are algebraically independent over K and L is a regular extension of K, then L and M are linearly disjoint over K. Thus LM is a regular extension of M.

(5) If L and M are regular extensions of K, and algebraically independent over K, then LM is a regular extension of L, M and K.

1.14. A particular case: algebraic closure of a set within a model.

Let $A \subseteq K$, and consider the algebraic closure $acl(A)$ of A in the model K. Then $acl(A)$ is a field and K is a regular extension of $acl(A)$.

Proof. Any element of K which is separably algebraic over $acl(A)$ is clearly in $acl(A)$, which implies $K \cap acl(A)^s = acl(A)$. By 1.12(2) it suffices to show that K is a separable extension of $acl(A)$. If $char(K) = 0$ then K is a separable extension of any subfield, and we are done. Otherwise, the λ-functions of K are definable in K (see 1.17 for the definition). Thus $acl(A)$ is closed under the λ-functions of K, which implies that K is a separable extension of $acl(A)$ by 1.18(7).

The same argument gives: if $A \subseteq K$, then K is a separable extension of $dcl(A)$ (the definable closure of A within K).

1.15. Definition. We say that the field F is *bounded* if F has finitely many separably algebraic extensions of degree n for all $n > 1$.

Lemma. Assume that F is bounded, and let F^* be an elementary extension of F (in a language containing the language of fields). Then the restriction map : $G(F^*) \to G(F)$ is an isomorphism.
Proof. Equivalently, we need to show that the separable closure of F^* is F^*F^s. Fix $n > 1$, and let $L_1, \ldots, L_N$ be the separable extensions of F of degree n. Since $F \prec F^*$, the extensions L_iF^* have degree n over F^* and are distinct. On the other hand, the phrase: "F has exactly N separable extensions of degree n" is expressible by a first-order sentence of the language of fields, and is therefore satisfied by F^*. Hence $L_1F^*, \ldots, L_NF^*$ are precisely the extensions of F^* of degree n. Thus, for every $n \in \mathbb{N}$, any separable extension of F^* of degree n over F^* is contained in F^*F^s. This proves our assertion.

1.16. p-bases, p-independence. Let F be a field of characteristic $p > 0$. Then F^p is a subfield of F, isomorphic to F via the map $x \mapsto x^p$. Thus F is naturally an F^p-vector space. We say that $B \subseteq F$ is *p-independent in F* if the set M of all monomials in B of the form $b_1^{i(1)} \cdots b_n^{i(n)}$ with $b_1, \ldots, b_n \in B$ and $0 \leq i(1), \ldots, i(n) \leq p-1$, is independent in the F^p-vector space F. If furthermore M is a basis of the F^p-vector space F, then we call B a *p-basis of F*. Note that B is a p-basis of F if and only if B is a maximal p-independent subset of F (and then $F = F^p[B]$).

Any p-independent subset of F extends to a p-basis of F, and any two p-bases of F have the same cardinality. The size of a p-basis of F is called the *degree of imperfection* of F. The following are easy consequences of the definition:

(1) Let $B \subset F$. Then B is p-independent in F if and only if for every $b \in B$, $b \notin F^p[B \setminus \{b\}]$.

(2) Let $B \subset F$ be p-independent in F. Then B is a p-basis of F if and only if $F^p[B] = F$.

If E is a subfield of F, we say that B is a *p-basis of F over E* if the set M of all monomials in B of the form $b_1^{i(1)} \cdots b_n^{i(n)}$ with $b_1, \ldots, b_n \in B$ and $0 \leq i(1), \ldots, i(n) \leq p-1$, is a basis of the EF^p-vector space F. Then $F = EF^p[B]$. Observe that a p-basis of F over E is also a p-basis of F^s over E and over E^s.

The size of a p-basis of F over E (by convention, an element of $\mathbb{N} \cup \{\infty\}$) is called the *degree of imperfection of F over E*. For properties of p-bases, see 1.19 below.

1.17. The λ-functions. Let F be a field of characteristic $p > 0$. For each n fix an enumeration $m_{i,n}(\bar{x})$ of the monomials $x_1^{i(1)} \cdots x_n^{i(n)}$ with $0 \leq i(1), \ldots, i(n) \leq p-1$. Define the $(n+1)$-ary functions $\lambda_{i,n} : F^n \times F \to F$ as follows:
If the n-tuple $\bar{a}$ is not p-independent, or if the $(n+1)$-tuple $(\bar{a}, b)$ is p-independent, then $\lambda_{i,n}(\bar{a}, b) = 0$. Otherwise, the $\lambda_{i,n}(\bar{a}, b)$ satisfy

$$b = \sum_{i=0}^{p^n-1} \lambda_{i,n}(\bar{a}, b)^p m_{i,n}(\bar{a}).$$

Note that these functions depend on the field F, and that the above properties define them uniquely. They are first-order definable in the field F. We will refer to them as: the *λ-functions defined on F*".

1.18. The following conditions are equivalent:

(1) L is a separable extension of K.

(2) L and K^{1/p^∞} are linearly disjoint over K.

(3) Whenever u is a finite tuple from L, then $K(u)$ has a transcendence basis $\{t_1, \ldots, t_m\}$ over K, such that $K(u)$ is separably algebraic over $K(t_1, \ldots, t_m)$. Such a transcendence basis is called a *separating transcendence basis*.

(4) L^p and K are linearly disjoint over K^p.

(5) Any p-basis of K remains p-independent in L.

(5') Any p-basis of K is contained in a p-basis of L.

(6) Some p-basis of K remains p-independent in L.

(6') Some p-basis of K is contained in a p-basis of L.

(7) K is closed under the λ-functions of L.

Remark. One extends the definition to the characteristic 0 case as follows: if $char(K) = 0$, then *any* field extension of K is *separable over* K.

Proof of (1) implies (7). This follows easily from the definition of the λ-functions of L, but we will give the proof. Here the λ-functions are those of L. Assume that L is not a separable extension of K. Choose a tuple $(a_1, \ldots, a_n) \in K^n$ which is p-independent in K but not p-independent in L, with n minimal such. Then $a_1, \ldots, a_{n-1}$ are p-independent in L, and $a_n \in L^p[a_1, \ldots, a_{n-1}]$, $a_n \notin K^p[a_1, \ldots, a_{n-1}]$. Hence $\lambda_{i,n-1}(a_1, \ldots, a_{n-1}; a_n) \in L \setminus K$ for some i. This shows one direction. For the other assume that for some $a_1, \ldots, a_n \in K$ and some i the element $\lambda_{i,n-1}(a_1, \ldots, a_{n-1}; a_n)$ is not in K. Note that the $\lambda_j(a_1, \ldots, a_{n-1}; a_n)$ are (the unique) solutions in L of the equation

$$(*) \qquad \sum_j X_j^p m_{j,n-1}(a_1, \ldots, a_{n-1}) = a_n.$$

From $\lambda_{i,n-1}(a_1, \ldots, a_{n-1}; a_n) \notin K$, we obtain first that $\{a_1, \ldots, a_{n-1}\}$ is p-independent in L, and then that $\{a_1, \ldots, a_n\}$ is p-independent in K: if not, there would be elements b_j in K satisfying $(*)$ in K, and we would have $b_j = \lambda_{j,n-1}(a_1, \ldots, a_{n-1}; a_n) \in K$ for all j. Thus $a_1, \ldots, a_n$ is p-independent in K but not in L.

1.19. Properties of p-bases. Let K be a field of characteristic $p > 0$ and L a separable extension of K. The following facts are easy consequences of the definitions:

(1) If B is a p-basis of L over K, then the elements of B are algebraically independent over K.

(2) Assume that L is finitely generated over K. Then the degree of imperfection of L over K equals the transcendence degree of L over K. Any p-basis of L over K is a (separating) transcendence basis of L over K.

(3) A subset B of L is p-independent over K if and only if for every element $b \in B$, $b \notin KL^p[B \setminus \{b\}]$.

(4) A subset B of L which is p-independent over K is a p-basis of L over K if and only if $L = KL^p[B]$.

(5) Assume that B_0 is a p-basis of K and B_1 is a p-basis of L over K. Then $B_0 \cup B_1$ is a p-basis of L.

1.20. p-independent extensions. Assume that L and M are separable extensions of K and $char(K) = p > 0$. We say that L and M are *p-independent over K*, if any subset of L which is p-independent over K remains p-independent over M (in the field LM).

Choose a p-basis B_0 of K, and extend it to p-bases B_1 of L and B_2 of M. The following are equivalent:

(1)L and M are p-independent over K.

(2)$B_1 \cup B_2$ is a p-basis of LM.

(3)$(B_1 \setminus B_0) \cup (B_2 \setminus B_0)$ is p-independent over K in the field LM.

Remark. Note that if L and M are linearly disjoint over K, then they are p-independent over K: assume that $B = B_1 \setminus B_0$ is not p-independent over M in LM. Then some non-trivial M-linear combination of elements of $L^p[B]$ is 0. By linear disjointness, some non-trivial K-linear combination of these elements equals 0, which contradicts our assumption on B.

1.21. Derivations. Let $R \subset S$ be commutative rings. Recall that an R-derivation on S is an additive map $\delta : S \to S$ which vanishes on R and satisfies $\delta(xy) = \delta(x)y + x\delta(y)$. Let $A \subseteq \Omega$ be a finite set, and assume that every k-derivation on $k(A)$ vanishes on $k(A)$. Then $k(A)$ is separably algebraic over k, see [37]?? Proposition X.7.2. We will use the following easy consequence of this:

Lemma. Let A, B be finite subsets of Ω.

(1) $A \subseteq k(A^p)$ if and only if A is separably algebraic over k.

(2) Assume that A is separably algebraic over $k(B^p)$ and that B is separably algebraic over $k(A)$. Then (A, B) is separably algebraic over k.

Proof. (1) If a is separably algebraic over k then $a \in k(a^p)$, and this gives the right-to-left implication. Conversely, assume that $A \subset k(A^p)$ and let D be a k-derivation on $k(A)$. Then D vanishes on $k(A^p)$, and therefore vanishes on A. Hence A is separably algebraic over k.

(2) Let D be a k-derivation on $k(A,B)$. Then D vanishes on $k(B^p)$ and therefore vanishes on A since A is separably algebraic over $k(B^p)$. This implies that D vanishes on B, and therefore that (A,B) is separably algebraic over k.

1.22. Basic λ-terms. We work in a large field K, with p-basis B. We first suppose that $B=\{b_1,\dots,b_e\}$. We let $I=I(B)=\{1,\dots,p^e\}$, $\lambda_i(B;-)=\lambda_{i,e}(b_1,\dots,b_e;-)$ and $m_i(B)=m_{i,e}(b_1,\dots,b_e)$. If $\mu\in I^n$, we define by induction on n the function $\lambda_\mu(B;-)$ and the p^n-monomial $m_\mu(B)$ as follows: if $n=0$, then $\lambda_\mu(B;x)=x$, $m_\mu(B)=1$; if $n\geq 1$, write $\mu=\nu^\frown i$, where $\nu\in I^{n-1}$, $i\in I$, and define

$$\lambda_\mu(B;x)=\lambda_i(B;\lambda_\nu(B;x)),\qquad m_\mu(B)=m_i(B)^{p^{n-1}}m_\nu(B).$$

Then we have, for any $a\in K$ and $n\in\mathbb{N}$:

$$a=\sum_{\mu\in I^n}\lambda_\mu(B;a)^{p^n}m_\mu(B).$$

If $\mu\in I^n$, we call λ_μ a *λ-term of level n*. Note that all basic λ-terms are terms of the language $\mathcal{L}_\lambda(b_1,\dots,b_e)$. We let $I^{<\omega}=\bigcup_{n\in\mathbb{N}}I^n$.

If $B\subseteq K$ is infinite, then by abuse of notation, we will denote by $(\lambda_\mu(B;x)\mid\mu\in I^n)$ the set of all terms $\lambda_\mu(b_1,\dots,b_e;x)$ where $e\in\mathbb{N}$, $b_1,\dots,b_e\in B$, and $\mu\in I(\{b_1,\dots,b_e\})^n$. Note that for a given element $c\in K$, the set $\{\lambda_\mu(B;c)\mid\mu\in I^n\}$ is finite, and that $c\in\mathbb{F}_p[\lambda_\mu(B;c)\mid\mu\in I^n]^{p^n}[B]$.

Lemma. Let $k\subseteq L\subseteq K$, assume that B is a p-basis of k and of K. Let C be a p-basis of L over k, and let $k\langle C\rangle=k(\lambda_\mu(B;c)\mid c\in C,\mu\in I^{<\omega})$, the λ-functions being those of K.

(1) If $c\in L^{p^n}(B)$, then $\lambda_\mu(B;c)\in L$ for every $\mu\in I^n$.

(2) $Lk\langle C\rangle$ is closed under the λ-functions of K. If $a\in L$ and $\nu\in I^n$, then $\lambda_\nu(B;a)\in L[\lambda_\mu(B;c)\mid c\in C,\mu\in I^n]$.

(3) If D is another p-basis of K and $a\in L$, $\nu\in I^n$, then $\lambda_\nu(B;a)\in\mathbb{F}_p[\lambda_\mu(D;a),\lambda_\mu(B;d)\mid d\in D,\mu\in I^n]$. If $D\subset k$, then $\lambda_\nu(B;a)\in k[\lambda_\mu(D;a)\mid\mu\in I^n]$.

Proof. (1) As $B\subset L$, we have $L^{p^n}(B)=L^{p^n}[B]$, and $c\in L^{p^n}[B_0]$ for some finite subset B_0 of B, so that we may assume that B is finite. Then $c=\sum_{j\in I}c_j^p m_j(B)$ for some $c_j\in L^{p^{n-1}}$. Thus $c_j=\lambda_j(B;c)\in L^{p^{n-1}}$. Since $\lambda_\mu=\lambda_\nu\circ\lambda_j$ for some $\nu\in I^{n-1}$ and $j\in I$, an induction on n gives us that $\lambda_\mu(B;c_j)\in L$.

(2) By assumption, $B\cup C$ is a p-basis of L; hence $L=L^{p^n}[B,C]$ for every $n\geq 0$. By definition of the λ-functions, we also have that $c\in(\mathbb{F}_p[\lambda_\mu(B;c)\mid\mu\in I^n])^{p^n}[B]$ for any $c\in K$. Hence $L=(L[\lambda_\mu(B;c)\mid c\in C,\mu\in I^n])^{p^n}[B]$, and (1) gives that $\lambda_\nu(B;a)\in L[\lambda_\mu(B;c)\mid c\in C,\mu\in I^n]$. Hence $Lk\langle C\rangle$ is closed under the λ-functions of K.

(3) By assumption, $K=K^{p^n}[D]=K^{p^n}[B]$. If $a\in L$, then $a\in(\mathbb{F}_p[\lambda_\mu(D;a)\mid\mu\in I^n])^{p^n}[D]$, and if $d\in D$ then $d\in(\mathbb{F}_p[\lambda_\mu(B;d)\mid\mu\in I^n])^{p^n}[B]$. Thus $a\in\mathbb{F}_p[\lambda_\mu(D;a),\lambda_\mu(B;d)\mid\mu\in I^n,d\in D]^{p^n}[B]$, and (1) gives the first assertion. The second assertion follows from the fact that $D\subset k$ and that k is closed under the λ-functions of K.

1.23. λ-polynomial rings over k when k has finite degree of imperfection.

Let B be a p-basis of k of finite size e. Then the set I defined above has size p^e. We define $k\langle X\rangle_{\leq n,B}$ to be the quotient of the polynomial ring $k[X_\mu \mid \mu \in I^{\leq n}]$ by the ideal generated by the polynomials

$$X_\mu - \sum_{i\in I} X^p_{\mu^\frown i} m_i(B)$$

for $\mu \in I^{\leq n-1}$, and we let $k\langle X\rangle_B = \bigcup_n k\langle X\rangle_{\leq n,B}$. If we consider only one p-basis B, then we will omit B from the notation. We define $k\langle X_1,\ldots,X_n\rangle_{\leq n,B}$ and $k\langle X_1,\ldots,X_n\rangle_B$ analogously.

Then B is a p-basis of (the field of fractions of) $k\langle X_1,\ldots,X_n\rangle_B$. If B is a p-basis of an extension K of k and $a_1,\ldots,a_n \in K$, then there is a unique k-morphism $k\langle X_1,\ldots,X_n\rangle_B \to K$ which sends X_i to a_i. Note also that $k\langle X_1,\ldots,X_n\rangle_B$ is generated as a ring by the elements $\lambda_\mu(B;X_i), i = 1,\ldots,n, \mu \in I(B)^{<\omega}$.

If C is another p-basis of k, then there is a natural $k[X_1,\ldots,X_n]$-isomorphism

$$k\langle X_1,\ldots,X_n\rangle_B \to k\langle X_1,\ldots,X_n\rangle_C.$$

This follows from the previous observation, and the fact that by Lemma 1.12(3), we have

$$k\langle X_1,\ldots,X_n\rangle_{\leq m,C} \subseteq k\langle X_1,\ldots,X_n\rangle_{\leq m,B}$$

and

$$k\langle X_1,\ldots,X_n\rangle_{\leq m,B} \subseteq k\langle X_1,\ldots,X_n\rangle_{\leq m,C}$$

for every $m \in \mathbb{N}$.

1.24. Lemma. Let K be a separable extension of k, with p-basis B over k, and let $C \subset k$ be p-independent. Consider the fields $k_1 = k(c^{1/p} \mid c \in C)$ and $k_2 = k(c^{1/p^n} \mid c \in C, n \in \mathbb{N})$. Then B is a p-basis of k_1K over k_1 and of k_2K over k_2.

Proof. Clearly $k_1K = k_1K^p[B]$ and $k_2K = k_2K^p[B]$, so we only need to show that B is p-independent over k_1 in k_1K and over k_2 in k_2K. Since K is a separable extension of k, the fields $k^{p^{-\infty}}$ and K are linearly disjoint over k. Hence K is linearly disjoint from k_1 and from k_2 over k. This implies that k_1K^p and K are linearly disjoint over kK^p: hence linearly independent elements of the kK^p-vector space K stay linearly independent in the k_1K^p-vector space k_1K. This shows that B stays p-independent over k_1 in k_1K. The proof for k_2K is similar.

1.25. Separably closed fields.

For each $e \in \mathbb{N} \cup \{\infty\}$, the theory expressing that K is a separably closed field of degree of imperfection e, is a complete theory (Ershov [E]), which we denote by SCF_e, and is stable (Wood [W]). If K is separably closed and $\{b_1,\ldots,b_e\}$ is a p-basis of K, then $\mathrm{SCF}_{e,b} = Th(K,b_1,\ldots,b_e)$ is model complete in the language $\mathcal{L}(b_1,\ldots,b_e)$.

Consider the language $\mathcal{L}_\lambda = \mathcal{L} \cup \{\lambda_{i,n} \mid n \in \mathbb{N},\ 1 \leq i \leq p^n\}$, and let T_λ be the $\mathcal{L}_\lambda$-theory obtained by adjoining to the theory of fields axioms expressing the defining properties of the functions $\lambda_{i,n}$ defined above. Let $\mathrm{SCF}_{e,\lambda} = \mathrm{SCF}_e \cup T_\lambda$. Then $\mathrm{SCF}_{e,\lambda}$ is complete and eliminates quantifiers but does not eliminate imaginaries (Delon [D]).

1.26. Separably closed fields of finite degree of imperfection.
Fix a separably closed field K. When the degree of imperfection of K is finite, one may fix a p-basis $\{b_1, \ldots, b_e\}$ of K, and only consider the unary functions $\lambda_i(x) := \lambda_{i,e}(b_1, \ldots, b_e; x)$. Then $Th(K)$ eliminates quantifiers and imaginaries in the language $\mathcal{L}_\lambda(b_1, \ldots, b_e) = \mathcal{L} \cup \{b_1, \ldots, b_e, \lambda_i : 1 \leq i \leq p^e\}$ (Delon [15]).

2 Preliminaries in algebraic geometry: definitions and main facts

2.1. Algebraic sets, (affine) varieties and regular extensions. Details can be found in Chapter III of [38]. Let K be a field, Ω a large algebraically closed field containing K.

Let n be an integer. The set Ω^n is called the affine space of dimension n (over Ω); it is also sometimes denoted by $\mathbb{A}^n$, or by $\mathbb{A}^n(\Omega)$. A subset V of Ω^n is called *an algebraic set*, or a *Zariski closed set*, if $V = \{a \in \Omega^n \mid f_1(a) = \ldots = f_m(a) = 0\}$ for some polynomials $f_i(X) \in \Omega[X]$, $X = (X_1, \ldots, X_n)$. We denote by $V(K)$ the set $V \cap K^n$.

If the polynomials $f_1(X), \ldots, f_m(X) \in K[X]$, then we say that V is *definable over* K, or that V is a *K-closed set*. The set V is *K-irreducible* if it is not the proper union of two proper K-closed sets. The set V is called *irreducible* (or *absolutely irreducible*, or a *variety*) if it is Ω-irreducible.

If V is defined over K, then V is irreducible if and only if it is K^s-irreducible. Every algebraic set V decomposes into a finite union of irreducible closed sets, say $V_1, \ldots, V_m$, and this decomposition is unique up to a permutation, if one assumes that $V_i \subseteq V_j$ implies that $i = j$. The sets V_i are called the *irreducible components* of V.

To an algebraic set V we associate the ideal $I(V) = \{f(X) \in \Omega[X] \mid f(a) = 0 \text{ for all } a \in V\}$.

We say that V is *defined over* K if and only if $I(V)$ is generated by $I(V) \cap K[X]$. For every algebraic set V, there is a unique smallest field over which V is defined, called the *field of definition of* V.

2.2. Note: if V is defined over K, then it is definable over K. The converse is not true in general, but we have: if V is definable over K then V is defined over K^{1/p^∞}. Thus the notions of defined and definable agree when the characteristic is 0.

Assume that V is definable over K. Then V is K-irreducible if and only if $I(V) \cap K[X]$ is a prime ideal.

Assume that V is K-irreducible. Then the irreducible components of V are defined over K^{alg}, and are permuted transitively by $Aut(K^{alg}/K)$. Moreover, V is irreducible and defined over K if and only if the field of quotients of $K[V] =_{\text{def}} K[X]/I(V) \cap K[X]$ is a regular extension of K.

2.3. The topology on K^n whose closed sets are the algebraic sets, is called the *Zariski topology*. If $S \subseteq K^n$, there is a smallest algebraic set containing S: it is called the *Zariski closure* of S and denoted by $\bar{S}$.

The topology induced on K^n by the Zariski topology on Ω^n coincides with the Zariski topology on K^n.

2.4. For $S \subseteq \Omega^n$ we define

$$I(S) = \{f \in \Omega[X_1, \ldots, X_n] \mid f(a) = 0 \text{ for all } a \in S\}.$$

Then $\bar{S}$ is precisely the set of zeros of $I(S)$. Observe that because $\Omega[X_1, \ldots, , X_n]$ is noetherian, every descending chain of closed sets is finite.

2.5. For an algebraic set V, we define the *affine coordinate ring* of V to be

$$\Omega[V] :=_{\text{def}} K[X_1, \ldots, X_n]/I(V).$$

If V is a variety, then $\Omega[V]$ is an integral domain and its quotient field, $\Omega(V)$, is called the *function field* of V.

If V is F-closed, we define $F[V] = F[X_1, \ldots, X_n]/(I(V) \cap F[X_1, \ldots, X_n])$. If V is F-irreducible, $F(V)$ is the quotient field of $F[V]$. Then

V is a variety if and only if F is relatively separably closed in $F(V)$.

V is a variety defined over F if and only if $F(V)$ is a regular extension of F.

If V and W are varieties, then so is their cartesian product $V \times W$, and $\Omega[V \times W] = \Omega[V] \bigotimes_{\Omega} \Omega[W]$. If V and W are F-closed and F-irreducible, then $V \times W$ may be F-reducible. This happens if $F[V] \cap F^s$ and $F[W] \cap F^s$ are not linearly disjoint over F.

2.6. For a variety V, we define $dim(V)$ to be the transcendence degree of $K(V)$ over K (or equivalently of $F(V)$ over F if V is defined over F). A point $a \in V$ is called *generic over* F if the transcendence degree of $F(a)$ over F equals $dim(V)$. Note that if a is generic, then $F(a) \simeq_F F(V)$. If K has infinite transcendence degree, then it contains generic points of any variety (over its field of definition).

For an algebraic set V, we define $dim(V)$ to be the supremum of the dimensions of the irreducible components of V. For $S \subseteq K^n$, we define $dim(S) = dim(\bar{S})$.

2.7. Let $a \in \Omega^n$; we define $I(a/K)$ to be the ideal consisting of all polynomials $f \in K[X_1, \ldots, X_n]$ such that $f(a) = 0$; then $I(a/K)$ is a prime ideal. If $V \subseteq \Omega^n$ is the associated algebraic set, it is then K-irreducible and $K(a) \simeq_K K(V)$; we call V the (algebraic) *locus* of a over K. Thus V is a variety if and only if K is relatively separably closed inside $K(a)$. Observe that by definition a is a generic point of V over K.

2.8. Let a, V be as above. The model-theoretic interpretation, in the sense of the theory ACF, is:

The Morley rank and U-rank of $tp(a/K)$ both equal $dim(V)$. The type $tp(a/K)$ is stationary if and only if V is a variety. If V is not a variety, then the multiplicity of $tp(a/K)$ equals the number of irreducible components of V. In terms of field extensions: $tp(a/K)$ is stationary if and only if K is relatively separably closed in $K(a)$; the multiplicity of $tp(a/K)$ equals $[K^s \cap K(a) : K]$.

We define the canonical base of $tp(a/K)$, denoted by $Cb(a/K)$, to be the perfect hull of the field of definition of V; it is definably closed in the sense of ACF, and is contained in the perfect hull of K. It is the smallest definably closed subset of K over which a has same rank and multiplicity as over K. Note that we do not require $tp(a/K)$ to be stationary, for more details on canonical bases of non-stationary types see [3]. By abuse of notation we will write $b = Cb(a/K)$ whenever b is a tuple such that $dcl(b) = Cb(a/K)$.

Observe that, if $tp(a/K)$ is not stationary, then $Cb(a/K^{alg})$ is contained in the definable closure of $K(a) \cap K^s$, and $tp(a/K(a) \cap K^s) \vdash tp(a/K^{alg})$.

2.9. Let $V \subseteq \Omega^n$, $W \subseteq \Omega^m$ be varieties. A *morphism* from V to W is a map $f = (f_1, \ldots, f_m)$ defined on V and taking its values in W, where each $f_i \in \Omega[V]$. It induces a dual map $f^* : \Omega[W] \to \Omega[V]$, $g \mapsto g \circ f$, which is an inclusion of Ω-algebras if $f(V)$ is Zariski dense in W. A morphism is continuous (for the Zariski topology).

If f is bijective and f^{-1} is also a morphism, then f is called an *isomorphism*. There are bijective morphisms which are not isomorphisms, for instance in characteristic $p > 0$, the morphism $x \mapsto x^p$. If f is an isomorphism then f^* is an isomorphism, and conversely.

A *rational map* from V to W is a map $f = (f_1, \ldots, f_m)$ defined on some open subset of V and taking its values in W, and where each $f_i \in K(V)$. It induces a dual map $f^* : \Omega(W) \to \Omega(V)$, $g \mapsto g \circ f$, which is an inclusion of K-algebras if $f(V)$ is Zariski dense in W. A rational map is continuous.

We say that f is *birational* if there is a rational map $g : W \to V$ such that $f \circ g$ is the identity. If f is birational then f^* is an isomorphism, and conversely. Two varieties are birationally equivalent if there is a birational map between them.

2.10. A constructible set in Ω^n is a boolean combination of Zariski closed sets; it can be written as a finite union of sets of the form $V \cap U$, where V is a variety, and U a basic open set, i.e. of the form $\{a \in \Omega^n \mid g(a) \neq 0\}$ for some polynomial g over Ω.

By quantifier-elimination of the theory ACF, every definable subset of Ω^n is constructible.

2.11. Abstract varieties. So far we have talked only of affine algebraic sets and varieties. There is a more general notion of variety, whose definition encompasses both affine varieties and projective varieties. Below, we will list the definitions pertaining to abstract varieties and some of their properties.

(1) An abstract variety $(V, U_i, V_i, \varphi_i)_{i \in I}$, I a finite set of indices, is given by a set $V = \bigcup_{i \in I} U_i$, affine varieties V_i, $i \in I$, and bijections $\varphi_i : U_i \to V_i$ such that for $i \neq j$, $f_{ij} = \varphi_j \varphi_i^{-1} : V_i \to V_j$ is a rational map, defined on the open subset $\varphi_i(U_i \cap U_j)$ of V_i.

(2) The topology on V is then defined in the following manner: a subset W of V is open if and only if $\varphi_i(W \cap U_i)$ is open (for the Zariski topology) in V_i for all $i \in I$. Our assumption on the sets $\varphi_i(U_i \cap U_j)$ implies that each U_i is open in V. This topology is called the Zariski topology.

(3) If all the varieties V_i and rational maps f_{ij} are defined over the field F, we say that V is defined over F. Note that the abstract variety is actually uniquely determined by the data $(V_i, f_{ij})_{i,j \in I}$.

(4) Observe that all varieties V_i have the same dimension, since each map f_{ij} is birational (with inverse f_{ji}) and therefore $F(V_i) \simeq F(V_j)$.

A point $a \in V$ is a generic point of V if $\varphi_i(a)$ is a generic point of V_i for all $i \in I$ (or, equivalently, for some $i \in I$, since one has: if $b = \varphi_i(a)$ is generic, then so is $f_{ij}(b)$).

For $a \in V$, one can define $F(a)$ to be the field $F(\varphi_i(a))$ for some $i \in I$ such that $a \in U_i$. Note that this definition is independent of the choice of i (up to an F-automorphism).

(5) A subvariety of V is an irreducible closed subset W of V. Equivalently, W is a subvariety of V if $\varphi_i(W \cap U_i)$ is a subvariety of V_i for each i. A point $b \in W$ is a generic of W if $\varphi_i(b)$ is a generic of $\varphi_i(W \cap U_i)$ for each i.

(6) Let $S \subseteq V$ be a set. We denote by $\bar{S}$ the closure of S for the topology on V. Then $\bar{S} = \bigcup_{i \in I} \varphi_i^{-1}(\overline{\varphi_i(S \cap U_i)})$.

(7) Let $(V, U_i, V_i, \varphi_i)_{i \in I}$ and $(W, S_j, W_j, \psi_j)_{j \in J}$ be two abstract varieties. A rational map $\theta : V \to W$ is a map with domain an open subset of V, and such that for $i \in I$ and $j \in J$ the maps $\theta_{ij} = \psi_j \theta \varphi_i^{-1} : V_i \to W_j$ are rational maps. Note that θ is continuous for the topology.

(8) If $(V, U_i, V_i, \varphi_i)_{i \in I}$ and $(W, S_j, W_j, \psi_j)_{j \in J}$ are abstract varieties, then their product is also an abstract variety, given by $(V \times W, U_i \times S_j, V_i \times W_j, \varphi_i \times \psi_j)_{i \in I, j \in J}$.

2.12. Example: projective varieties. Consider the projective space of dimension n, $\mathbb{P}^n$. It is the set of lines in affine $(n+1)$-space, and can be described as follows: let $S = K^{n+1} \setminus \{0\}$, and define an equivalence relation on S by: $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if $\lambda x_0 = y_0, \ldots, \lambda x_n = y_n$ for some $\lambda \in K$. Then $\mathbb{P}^n = S/\sim$. The representative of the equivalence class of $(x_0, \ldots, x_n)$ is often denoted by $(x_0 : \cdots : x_n)$.

One defines (projective) algebraic sets as in the affine case, except that one has to be careful to only consider zero-sets of sets of homogeneous polynomials. We will now show that $\mathbb{P}^n$ has a natural structure of abstract variety, and that the closed sets are precisely finite unions of algebraic sets. For $i = 0, \ldots, m$, consider the hyperplane H_i of $\mathbb{P}^n$ defined by the equation $x_i = 0$, and let $U_i = \mathbb{P}^n \setminus H_i$. There is a natural bijection $\varphi_i : U_i \to K^n = V_i$ given by

$$(x_0 : \cdots : x_n) \mapsto \Big(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i} \ldots, \frac{x_n}{x_i}\Big).$$

Then the maps $\varphi_j \varphi_i^{-1} : V_i \to V_j$ are rational maps. Hence $(\mathbb{P}^n, U_i, V_i, \varphi_i)_{0 \leq i \leq n}$ is an abstract variety. One also verifies that algebraic sets are closed, and conversely that an irreducible closed set is an algebraic set (look at the polynomials vanishing at a generic point of the closed set).

2.13. Algebraic groups. Recall that a connected algebraic group is a group G, with a structure of abstract variety on G, and such that multiplication: $G \times G \to G$ and inverse: $G \to G$ are rational maps which are everywhere defined (on $G \times G$ and G). If the underlying variety is affine, we say that G is an affine algebraic group.

One can extend this definition to non-connected algebraic groups by defining an "abstract algebraic set": it is a union of sets U_i, each of them in bijection with some algebraic affine set V_i via a map φ_i, with the maps $\varphi_j \varphi_i^{-1}$ defined on an open subset of V_i, and given locally by rational maps.

Then, an algebraic group G is an abstract algebraic set, such that multiplication and inverse are everywhere defined and given locally by rational functions. In particular, closed subgroups of algebraic groups are algebraic groups. See [44] for a precise definition, and [24] for a detailed definition in the affine case and for related results. We conclude this section with two easy results on algebraic groups.

2.14. Let G be an algebraic group defined over F, let S be a subset of G such that:

(i) S contains all the generics of $\bar{S}$ over F.

(ii) If $a, b \in S$ are generic and independent over F then $ab \in S$ and $a^{-1} \in S$.

Then $\bar{S}$ is a subgroup of G.

Proof. By assumption and since the map $a \mapsto a^{-1}$ is continuous, S^{-1} is a dense subset of the closed set $(\bar{S})^{-1}$ which contains all the generics of S. This implies that $(\bar{S})^{-1} = \overline{S^{-1}} \supseteq \bar{S}$, from which one deduces that $\bar{S} = \bar{S}^{-1}$.

Let $a \in S$ be generic; then the set $S(a) = \{b \in \bar{S} \mid ab \in \bar{S}\}$ is closed and contains all the generic elements of $\bar{S}$ which are independent from a over F; thus $S(a) = \bar{S}$, and $a\bar{S} = \bar{S}$; similarly, the set $\{a \in \bar{S} \mid a\bar{S} = \bar{S}\}$ is closed, contains all the generic elements of $\bar{S}$ and therefore equals $\bar{S}$; thus $\bar{S}\bar{S} = \bar{S} = \bar{S}^{-1}$, which proves the result.

2.15. Let G be an algebraic group defined over F, let $a \in G$ and b be a generic of G, independent from a over F. Then ab is also a generic of G, and is independent from a over F.

Proof. This is a simple argument using transcendence degrees. Let $n = dim(G)$. Then $F(a, b) = F(a, ab)$ has transcendence degree n over $F(a)$. Hence

$$n = tr.deg(F(a, ab)/F(a)) \leq tr.deg(F(ab)/F) \leq n,$$

which shows that ab is a generic of G, independent from a over F.

3 Preliminaries on finite and pseudo-finite fields

3.1. Definitions. (1) A field F is *pseudo-algebraically closed* (abbreviated by PAC) if every affine variety defined over F has an F-rational point.

(2) A field F is *pseudo-finite* if it is PAC, perfect, and has precisely one algebraic extension of degree n for every $n \in \mathbb{N}$.

3.2. Let m, n, d be positive integers; there exists an integer e such that, for any field F, if $f_1, \ldots, f_m, f$ are polynomials in n variables over F of total degree $\leq d$ then:

(1) if $f \in I = (f_1, \ldots, f_m)$, then $f = \sum_{i=1}^{m} g_i f_i$ for polynomials g_i of total degree $\leq e$.

(2) if I is not prime, then there are some polynomials g and h of total degree $\leq e$ such that $gh \in I$ but $g, h \notin I$.

The proof can be found e.g. in [17]; from this it follows that "$f_1, \ldots, f_m$ generate a prime ideal in $F[X_1, \ldots, X_n]$" is a first-order property of the coefficients of $f_1, \ldots, f_m$. Moreover, since

ACF eliminates quantifiers, there is a quantifier-free formula which defines in all fields F (the coefficients of) the polynomials $f_1, \ldots, f_m$ in n variables and of total degree $\leq d$ whose zero-set is a variety (i.e., such that $f_1, \ldots, f_m$ generate a prime ideal in $F^{alg}[X_1, \ldots, X_n]$). Thus one can talk about varieties in a first-order way.

Observe also that the statement "F has one extension of degree n" can be formulated by translating in a first-order way: there are $c_1, \ldots, c_n$ such that $f(X) = X^n + c_1X^{n-1} + \cdots + c_n$ is irreducible, and for all $d_1, \ldots, d_n$ such that $g(X) = X^n + d_1X^{n-1} + \cdots + d_n$ is irreducible, the field obtained by adjoining to F a root of $f(X)$ contains a root of $g(X)$.

From these we deduce that being pseudo-finite is a first-order property in the language $\mathcal{L}$, and we denote by Psf the theory of all pseudo-finite fields. It is immediate that every finite field is perfect and has one extension of degree n for each $n \in \mathbb{N}$ (the unique extension of $\mathbb{F}_q$ of degree n is $\mathbb{F}_{q^n}$); it also follows from the Lang-Weil theorem that every non-principal ultraproduct of finite fields is PAC. J. Ax [1] showed that pseudo-finite fields are precisely the infinite models of the theory T_f of all finite fields. The fact that every infinite model of the theory of finite fields is a model of Psf follows easily from the Lang-Weil estimates on the number of points in finite fields of varieties; the reverse direction is given by 3.7.

We list below the main properties of the theory Psf; the proofs can be found in [1], [7] and [22]. Let F, F_1 and F_2 be pseudo-finite fields.

3.3. Let E be a subfield of F_1 and F_2. Then

$$F_1 \equiv_E F_2 \quad \Longleftrightarrow \quad (F_1 \cap E^{alg}) \simeq_E (F_2 \cap E^{alg}).$$

3.4. Taking for E the prime field, one obtains invariants for the elementary theories of pseudo-finite fields:

$$F_1 \equiv F_2 \quad \Longleftrightarrow \quad Abs(F_1) \simeq Abs(F_2),$$

where $Abs(F_1)$ is the subfield of F_1 of elements algebraic over the prime field.

3.5. Assume that $F_1 \subseteq F_2$; then, taking $E = F_1$:

$$F_1 \prec F_2 \quad \Longleftrightarrow \quad F_1^{alg} \cap F_2 = F_1.$$

3.6. Another application of 3.3 is the following: let E be a subfield of F, and $a, b \in F$; then $tp(a/E) = tp(b/E)$ if and only if there is an E-isomorphism f between $(E(a)^{alg} \cap F)$ and $(E(b)^{alg} \cap F)$ which sends a to b.

From this one then deduces: let $\varphi(x)$ be a formula (x a tuple of variables); there is a formula $\psi(x)$, boolean combination of sentences of the form $(\exists t\ f(x,t) = 0)$, where $f(x,t) \in \mathbb{Z}[x,t]$, t a single variable, such that

$$\text{Psf} \vdash \varphi(x) \leftrightarrow \psi(x).$$

3.7. Let E be a perfect field, and assume that E has at most one algebraic extension of each degree. Then there is a field F isomorphic to an ultraproduct of finite fields, such that

$$F \cap E^{alg} = E.$$

Moreover if E is of characteristic 0, F can be chosen isomorphic to an ultraproduct of prime fields $\mathbb{F}_p$.

This shows that Psf is precisely the theory of all infinite models of T_f, and that the pseudo-finite fields of characteristic 0 are exactly the infinite models of $Th(\mathbb{F}_p \mid p \text{ a prime })$.

3.8. As an illustration of techniques of proofs, we will show that the algebraic-geometric and model-theoretic notions of algebraic closure coincide:
Let E be a subfield of the pseudo-finite field F, relatively algebraically closed inside F, and let $a \in F$, $a \notin E$; then $tp(a/E)$ is not algebraic. *Proof.* Choose a field F' isomorphic to F over E, and linearly disjoint from F over E; because F and F' are linearly disjoint over E, the ring $F^{alg} \bigotimes_{E^{alg}} F'^{alg}$ is an integral domain; choose (topological) generators σ of $Aut(F^{alg}/F)$ and σ' of $Aut(F'^{alg}/F')$ such that σ and σ' have the same restriction to E^{alg}; define τ on the quotient field M of $F^{alg} \bigotimes_{E^{alg}} F'^{alg}$ by setting $\tau(b \otimes c) = \sigma(b) \otimes \sigma'(c)$ for $b \in F^{alg}$, $c \in F'^{alg}$, and extending in the obvious manner. Lift τ to an automorphism τ_1 of M^{alg}, and let $M_1 \subseteq M^{alg}$ be the subfield of M^{alg} fixed by τ_1; then $Aut(M_1^{alg}/M_1)$ is by definition generated by τ_1, and F and F' are relatively algebraically closed in M_1, since τ_1 extends σ and σ'. By 3.7, there is a pseudo-finite field L containing M_1 and such that M_1 is relatively algebraically closed in L. By 3.5, L is an elementary extension of both F and F', and therefore contains a realisation of $tp(a/E)$ not in F. Hence $tp(a/E)$ is not algebraic.

3.9. We now give a sharper description of definable sets.

Let $\varphi(x, y)$ be a formula, $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_n)$, let $a \in F^m$ and let $S = \varphi(a, F^n) = \{b \in F^n \mid F \models \varphi(a, b)\}$; there is a positive integer e, an algebraic set V defined over F, and a projection map (on the first n coordinates) π from $V(F)$ onto S, with fibers $\pi^{-1}(y)$ of size $\leq e$ for $y \in S$.

3.10. Using the Lang-Weil estimates on the number of rational points of varieties in finite fields, the above description of definable sets, and some counting arguments, one then obtains similar estimates for definable subsets of finite fields:
Theorem. Let $\varphi(x, y)$ be a formula in $\mathcal{L}$, with $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_n)$. There is a positive constant C, and a finite set D of pairs (d, μ) with $d \in \{0, 1, \ldots, n\}$ and μ a positive rational number, or $(d, \mu) = (0, 0)$, such that for each finite field $\mathbb{F}_q$ and tuple $a \in \mathbb{F}_q^m$,

$$(*) \qquad |card(\varphi(a, \mathbb{F}_q^n)) - \mu q^d| \leq C q^{d-(1/2)}$$

for some $(d, \mu) \in D$.

Furthermore, for each $(d, \mu) \in D$ there is a formula $\varphi_{(d,\mu)}(x)$, which defines in each finite field $\mathbb{F}_q$ the set of tuples a such that $(*)$ holds.

Let a be an m-tuple from the pseudo-finite field F. Then there is a unique pair $(d, \mu) \in D$ such that $F \models \varphi_{(d,\mu)}(a)$; one verifies that $d = dim(\varphi(a, F^n))$. The number μ can be used to define

a measure m_S on the definable subsets of $S = \varphi(a, F^n)$: for T a definable subset of S with associated pair (e, ν), define:

$$m_S(T) = \begin{cases} 0 & \text{if } e < d, \\ \nu/\mu & \text{if } e = d. \end{cases}$$

Since the definition of m_S originates from counting points in finite sets, m_S is clearly a finitely additive probability measure, defined on the definable subsets of S, taking only rational values, and invariant under definable bijection.

From these considerations, one obtains easily the following results:

3.11. (Finiteness of the S_1-rank) Let $S \subseteq F^n$ be definable, with $dim(S) = d$; let $\varphi(x, y)$ be a formula, and $(a_i)_{i \in I}$ a sequence such that $dim(S \cap \varphi(a_i, F^n)) = d$ for all i, and $dim(S \cap \varphi(a_i, F^n) \cap \varphi(a_j, F^n)) < d$ for all $i \neq j$; then I is finite.
Proof. By 3.10 there is a positive rational number $r \leq 1$ such that for any $a \in F^m$, $m_S(\varphi(a, F^n)) > 0$ implies $m_S(\varphi(a, F^n)) > r$; from the additivity of m_S, we obtain that I has less than $(1/r)$ elements.

3.12. We will denote the second coordinate of the pair associated to a definable set S by $\mu(S)$; then one has:

(a) For a variety V defined over F, $\mu(V(F)) = 1$ (This is the Lang-Weil Theorem).

(b) For disjoint definable subsets S and T of F^n,

$$\mu(S \cup T) = \begin{cases} \mu(S) + \mu(T) & \text{if } dim(S) = dim(T), \\ \mu(S) & \text{if } dim(S) > dim(T), \\ \mu(T) & \text{if } dim(S) < dim(T). \end{cases}$$

(c) If $f : S \to T$ is definable, and $dim(f^{-1}(a)) = d$ for each $a \in T$, then $dim(S) = dim(T) + d$. If moreover $\mu(f^{-1}(a)) = m$ for every $a \in T$, then $\mu(S) = m\mu(T)$.

3.13. (not the strict order-property) Let $\varphi(x, y)$ be a formula; then every sequence of tuples $a_i \in F$ such that the sets $\varphi(a_i, F^n)$ form a strictly increasing chain, is of bounded length.

We should mention that pseudo-finite fields are unstable: indeed Duret showed they have the independence property [18].

3.14. Adjoin to the language new constant symbols $c_{i,n}$ for $0 \leq i < n \in \mathbb{N}$ to obtain the language $\mathcal{L}_c$, and consider the extension Psf_c obtained by adding to Psf axioms expressing that the polynomials $X^n + c_{n-1,n}X^{n-1} + \cdots + c_{0,n}$ are irreducible for each n. Every pseudo-finite field then expands (non-uniquely) to a model of Psf_c; also, Psf_c is model-complete, since whenever $(F_1, c) \subseteq (F_2, c)$ are models of Psf_c then F_1 is relatively algebraically closed in F_2.

F admits elimination of imaginaries in the language $\mathcal{L}_c$. Thus every group G interpretable in F is F-definably isomorphic to a group defined in F.

3.15. Let G be a group definable in F; then there is a connected algebraic group H defined over F, definable subgroups of finite index G_0 of G and H_0 of $H(F)$, and a surjective isomorphism $f : G_0 \to H_0$, defined over F and with finite central kernel.

3.16. If V is a variety defined over F, then the set $V(F)$ is Zariski dense in V, that is, its Zariski closure equals V (actually, this holds in arbitrary PAC-fields).

Indeed, for $0 \neq g(x) \in F[V]$, the algebraic set $V' = \{(a, b) \mid a \in V,\ bg(a) = 1\}$ is clearly a variety, so it has an F-rational point. This shows that $V(F)$ intersects every open set of Ω^n defined over F. If W is a proper closed subset of V defined over F^{alg}, then the union of the conjugates of W over F is defined over F, which shows that $V(F)$ is dense in $V(F^{alg})$. Because $V(F^{alg})$ is dense in V, we deduce that $V(F)$ is dense in V.

4 PAC fields

4.1. Pseudo-algebraically closed fields. A field F is *pseudo-algebraically closed* (PAC) if every (absolutely irreducible) variety V defined over F has an F-rational point, i.e., a point with all its coordinates in F.

4.2. Properties of PAC fields. Let E and F be fields, with F PAC.

(1) (10.7 in [22]) An algebraic extension of a PAC field is also PAC.

(2) Let E be a regular field extension of F. Then F has an elementary extension F^* containing E. If the degree of imperfection of F is infinite and B is a p-independent subset of E containing a p-basis of F, then F^* can be chosen so that B is a p-basis of F^*. This is an immediate consequence of the definition of PAC and of 2.2.

(3) ((4.5) in [10]) If $E \subseteq F$, then $acl(E)$ is obtained by closing E under the λ-functions of F and taking the relative (field-theoretic) algebraic closure in F.

4.3. Definitions.

(1) Recall that a profinite group G is projective if every diagram

$$(*) \qquad \begin{array}{ccc} & & G \\ & & \downarrow \\ B & \longrightarrow & A \end{array}$$

where the maps are continuous epimorphisms, can be completed by a continuous homomorphism (not necessarily onto!) $G \to B$ making the diagram commutative. If G is projective, H is a profinite group and $f : H \to G$ is a continuous epimorphism, then H has a closed subgroup G_1 such that f restricts to a homeomorphism from G_1 onto G, see Remark 20.11 in [22].

(2) A field F is *ω-free* if it has a countable elementary substructure F_0 with $G(F_0) \simeq \hat{F}_\omega$, the free profinite group on countably many generators.

(3) A field F is *Frobenius*, if it is PAC and its absolute Galois group $G(F)$ has the so-called embedding property (or Iwasawa property), i.e.: every diagram

$$(*) \qquad \begin{array}{ccc} & & G(F) \\ & & \downarrow \\ B & \longrightarrow & A \end{array}$$

where the maps are continuous epimorphisms and B is isomorphic to a finite (continuous) quotient of $G(F)$, can be completed by a continuous epimorphism $G(F) \to B$ making the diagram commutative. The class of Frobenius fields is elementary, see §5. Since $\hat{F}_\omega$ satisfies the above property, ω-free PAC fields are Frobenius.

4.4. If F is PAC, then $G(F)$ is projective (10.17 in [22]), and any algebraic extension of F is PAC (10.7 in [22]).

4.5. Properties of ω-free PAC fields and Frobenius fields. Let E, F, F' and L be fields, with F and F' Frobenius fields.

(1) Assume that F and F' have the same degree of imperfection, and are separable extensions of L. Then $F \equiv_L F'$ if and only if $F \cap L^s \simeq_L F' \cap L^s$.

(2) Assume that F and F' have the same degree of imperfection, and that F' is a separable extension of F. Then $F \prec F' \iff F' \cap F^s = F$.

(3) (18.2 in [22]) Let $L = acl(L) \subseteq F$, and assume that F is sufficiently saturated. Let E be a regular extension of L, with $[E : E^p] \leq [F : F^p]$, and assume that every finite (continuous) quotient of $G(E)$ is also a finite quotient of $G(F)$. Then there is an L-isomorphic copy E' of E in F, such that F is a regular extension of E'.

Proof. For (1), see 5.12, and (2) is a direct consequence of (1). For (3), assume that F is $|E|^+$-saturated. We now use the terminology of section 5, see in particule 5.11: our assumption on the finite quotients means that $Im(G(E)) \subset Im(G(F))$. The inclusions $L \subseteq E$ and $L \subseteq F$ gives us embeddings $SG(L) \subset SG(E)$ and $SG(L) \subset SG(F)$. By the embedding property and the $|E|^+$-saturation of $SG(F)$, there is an $SG(L)$-embedding $\varphi : SG(E) \to SG(F)$. Dualising, this gives us a group epimorphism $\Phi : G(F) \to G(E)$, which commutes with the restriction maps onto $G(L)$. We now get the result by the embedding lemma (18.2 of [22]).

4.6. Consequences. Let F be a Frobenius field, sufficiently saturated. 4.5(1) allows us to describe the types in a simple manner: If a, b are tuples in F, and $E \subseteq F$, then $tp(a/E) = tp(b/E)$ if and only if there is an isomorphism φ between $acl(Ea)$ and $acl(Eb)$, which sends a to b and is the identity on E. One direction is clear. For the other, extend φ to an isomorphism of F with some field F'. Then F' is also Frobenius. Since F is a regular extension of $acl(Ea)$,

F' is a regular extension of $acl(Eb)$. Then 4.5(1) gives us that $F' \equiv_{acl(Eb)} F$, i.e., b realises the same type over E in F and in F'. Since φ is the identity on E, sends a to b and F to F', this implies that $tp(a/E) = tp(b/E)$.

4.7. Lemma . Let F be a Frobenius field, and assume that F is sufficiently saturated and that $L = acl(L) \subseteq F$. Let E be a regular extension of L, and assume that every finite quotient of $G(E)$ appears as a finite quotient of $G(F)$. Then there is an L-isomorphic copy E' of E in F such that $F \cap E'^s = E'$.

Proof. If the characteristic is 0, or if the characteristic is $p > 0$ and $[E : E^p] \leq [F : F^p]$, then this is 4.5(3). Hence, we may assume that the characteristic is $p > 0$ and that the degree of imperfection of F is finite and smaller than the degree of imperfection of E. Let C be a p-basis of E over L, and consider the extension $M = E(c^{1/p^n} \mid c \in C, n \in \mathbb{N})$. We claim that this is a regular extension of L. Indeed, without loss of generality, we may assume that E is finitely generated over L; then C is a separating transcendence basis of E over L, and for every $n \in \mathbb{N}$, the extension $E(c^{1/p^n} \mid c \in C)$ is separably algebraic over $L(c^{1/p^n} \mid c \in C)$. This shows that M is a separable extension of L. As E is regular over L and M is purely inseparable over E, this implies that $M \cap L^s = L$, and therefore that M is a regular extension of L. By construction, $[M : M^p] = [L : L^p] \leq [F : F^p]$, so that 4.5(3) applies and give the result.

5 Results of Cherlin, Van den Dries and Macintyre on PAC fields

In this section we give a proof of a result of Cherlin, Van Den Dries and Macintyre, which was announced in [11], but was never published in spite of the existence of two manuscripts [12] and [13]. The proof we give does not differ much from theirs, but of course, all mistakes are of my doing. I give references to the parts of their proof which have been published.

We first recall the definition of the inverse system of an absolute Galois group. This concept was introduced in [12], see also [11] and [13].

5.1. The inverse system of a profinite group. Recall that a profinite group is a compact Hausdorff, totally disconnected topological group. Equivalently, it is the inverse limit of an inverse system of finite groups with the discrete topology. We refer to [49] or to [22] for the basic properties of profinite groups. We will use an ω-sorted language, with sorts indexed by the positive integers, and we refer to the book by Kreisel and Krivine [36] for properties of many-sorted logics. They behave very much like ordinary first-order logic, except that all variables and constants have a prescribed sort. Eg, if x is of sort n, then the quantifier $\forall x$ ranges over all elements of sort n. Traditionally, the universes of distinct sorts are disjoint, however one can easily bypass this restriction by introducing functions which identify elements of distinct sorts. This is what we will do implicitly in our case. In particular, in the terminology of [36], the relations introduced below should be infinite collections of relations. We leave the reader to make the appropriate adjustments to the terminology of [36].

Let G be a profinite group. Consider the set $SG = \bigcup G/N$, where N ranges over the set $\mathcal{N}(G)$ of all open normal sugroups of G; if $N \subseteq M$ are in $\mathcal{N}(G)$, denote by $\pi_{N,M}$ the natural epimorphism $G/N \to G/M$. We denote the elements of G/N by gN, $g \in G$. Consider the ω-sorted language $\mathcal{L}_G = \{\leq, C, P\}$ where $\leq$ and C are binary relations, P is a ternary relation, and the sorts are indexed by the positive integers.

We define an $\mathcal{L}_G$-structure on SG as follows:

— gN is of sort n if and only if $[G : N] \leq n$. Note that we do not assume that the sorts are disjoint.

— $gN \leq hM$ if and only if $N \subseteq M$.

— $C(gN, hM)$ if and only if $N \subseteq M$ and $gM = hM$.

— $P(g_1N_1, g_2N_2, g_3N_3)$ if and only if $N_1 = N_2 = N_3$ and $g_1g_2N_1 = g_3N_1$.

Note that the $\mathcal{L}_G$-structure SG encodes precisely the inverse system $\{G/N, \pi_{N,M} \mid N, M \in \mathcal{N}(G), N \subseteq M\}$, and therefore determines G uniquely, since $G = \lim_{\leftarrow} G/N$. We call the $\mathcal{L}_G$ structure SG the **complete system associated to** G. The class of $\mathcal{L}_G$-structures of the form SG for some profinite group G is axiomatised by the following scheme of axioms T_G:

(1) $\leq$ is transitive and reflexive, with a unique largest element which is of sort 1. The elements of sort n are exactly the elements having at most n elements in their $\sim$-equivalence class, where $\sim$ is the equivalence relation defined by: $x \sim y \iff x \leq y$ and $y \leq x$. We will denote by $[x]_\sim$ the $\sim$-equivalence class of x.

(2) $S/\sim$ is a modular lattice (with respect to the partial ordering $\leq$). For the axiom stating the existence of the infimum, note that $[G : N \cap M] \leq [G : N][G : M]$.

(3) $P(x, y, z) \to (x \sim y \wedge y \sim z)$, $C(x, y) \to x \leq y$.

(4) P defines on each $\sim$-equivalence class the graph of a group multiplication.

(5) If $x \leq y$, then the intersection of C with the product $[x]_\sim \times [y]_\sim$ is the graph of a group epimorphism $\pi_{x,y}$ from $[x]_\sim$ to $[y]_\sim$. These epimorphisms from a compatible system: $\pi_{xx} = id$, $\pi_{yz}\pi_{xy} = \pi_{xz}$ if $x \leq y \leq z$.

(6) If N is a normal subgroup of $[x]_\sim$, then there is a unique y such that $C(x, y)$ and $\{xz^{-1} \mid z \sim x \wedge C(z, y)\} = N$.

If $S \models T_G$, one then defines a profinite group $G(S)$ as the inverse limit of the system of finite groups and epimorphisms $\{[\alpha]_\sim, \pi_{\alpha\beta} \mid \alpha, \beta \in S,\ \alpha \leq \beta\}$. Unravelling the definitions and using the isomorphism $G \simeq \lim_{\leftarrow}\{G/N, \pi_N, M \mid N \subseteq M \in \mathcal{N}(G)\}$, one checks easily that if G is a profinite group then $G(SG)$ is naturally isomorphic to G.

If $S \models T_G$, then $G(S)$ can be identified with the closed subgroup of $\prod_{\alpha \in S/\sim}[\alpha]_\sim$ consisting of those sequences (g_α) satisfying $\pi_{\alpha,\beta}(g_\alpha) = g_\beta$ for $\alpha \leq \beta \in S$. (Here $\prod_{\alpha \in S/\sim}[\alpha]_\sim$ is equipped with the product topology. Also, to simplify notation we write g_α instead of $g_{[\alpha]_\sim}$.)

We will define an embedding i of S into $SG(S)$, and show that i is onto. Let $\gamma \in S$. Since the maps $\pi_{\alpha,\beta}$ are epimorphisms and compatible, there is an element $(g_\alpha)_\alpha \in G(S)$ such that

$g_\gamma = \gamma$. For $\beta \in S$, let $N_\beta = G(S) \cap M_\beta$, where M_β is the kernel of the natural projection $\prod_\alpha [\alpha]_\sim \to [\beta]_\sim$. Then N_β is an open normal subgroup of $G(S)$, and we define $i(\gamma) = (g_\alpha)N_\gamma$. This clearly defines an embedding of S into $SG(S)$. It remains to show that i is onto: let N be an open normal subgroup of $G(S)$. Because $G(S)$ is a closed subgroup of $\prod_{\alpha \in S/\sim} [\alpha]_\sim$, and by the definition of the product topology, there are $\alpha_1, \ldots, \alpha_m \in S$ such that N contains the intersection of the N_{α_i}. Because of axiom (2), there is $\alpha \in S$ such that $N_\alpha \subseteq N$, and by axiom (6), there is a unique $\beta \in S/\sim$ such that N/N_α is the kernel of the map $\pi_{\alpha\beta}$. Thus $N = N_\beta$, and this shows that i is onto.

A continuous epimorphism of profinite groups $\pi : G \to H$ induces a dual $\mathcal{L}_G$-embedding $S\pi : SH \to SG$: if $hN \in SH$, define $S\pi(hN) = \pi^{-1}(hN)$. Conversely, we will show below that if $S_1, S_2 \models T_G$, an $\mathcal{L}_G$-embedding $i : S_2 \to S_1$ defines a unique continuous epimorphism $G(i) : G(S_1) \to G(S_2)$. First observe that i induces a group isomorphism from $[y]_\sim$ onto $[i(y)]_\sim$ for every $y \in S_2$, because y and $i(y)$ have the same sort and i respects P. If $x \in S_1$ let us denote by π_x the canonical epimorphism $G(S_1) \to [x]_\sim$. Then for each $y \in S_2$, the map $f_y = i^{-1}\,\pi_{i(y)} : G(S_1) \to [i(y)]_\sim \to [y]_\sim$ is a group epimorphism, and is continuous since $Ker(f_y) = Ker(\pi_{i(y)})$. Furthermore, if $y \leq z \in S_2$, then $f_z = \pi_{i(y),i(z)} f_y$ because i respects C. The universal property of the inverse limit implies then that there is a unique continuous group morphism $G(i) : G(S_1) \to G(S_2)$ which agrees with the system $\{f_y \mid y \in S_2\}$. By definition, for every $y \in S_2$, $\pi_y G(i)(G(S_1)) = f_y(G(S_1)) = [y]_\sim$, which implies that $G(i)(G((S_1))$ is dense in $G(S_2)$, and therefore that $G(i)$ is onto since the continuous image of a compact set is compact.

Hence the functors G and S define a duality between the category of profinite groups with continuous epimorphisms and the category of models of T_G with $\mathcal{L}_G$-embeddings.

5.2. The inverse system of the absolute Galois group of a field. Let K be a field, $G(K)$ its absolute Galois group $\mathcal{G}al(K^s/K)$. Then $SG(K) = \bigcup \mathcal{G}al(L/K)$, where L ranges over all finite Galois extensions of K. The group epimorphisms encoded by the binary relation C correspond to the restriction maps $\mathcal{G}al(M/K) \to \mathcal{G}al(L/K)$ whenever M is a Galois extension of K containing L. The largest element of $SG(K)$ is $\mathcal{G}al(K/K) = (1)$. If K is a regular extension of some subfield E, then $SG(E)$ identifies naturally with a substructure of $SG(K)$ (as the restriction map $G(K) \to G(E)$ is onto).

The following result is due to Cherlin, van den Dries and Macintyre. It is stated in [11], and proved in the preprints [12] and [13].

5.3. Theorem. Let K and L be fields, and E a common subfield of K, L, such that K and L are regular extensions of E.

(1) If $K \equiv_E L$ then $SG(K) \equiv_{SG(E)} SG(L)$.

(2) If K is κ-saturated, so is $SG(K)$.

5.4. Since their result is unpublished, we will give a sketch of the proof. The approach we take is slightly different from theirs. As in [CDM2], we first introduce a new ω-sorted structure, $Sep(K)$, which encodes the direct system of finite Galois extensions of K together with the possible inclusions. 5.3 will then be an immediate corollary of 5.7 and 5.5.

Let $\mathcal{L}_{sep}$ be the language $\{\leq, I, A, M\}$, with sorts indexed by the positive integers. The elements of $Sep(K)$ are the pairs (a, L), where L is a finite Galois extension of K containing a. We interpret the language symbols in the natural way:

— The elements of sort n are the pairs (a, L) where L is a finite Galois extension of K of degree $\leq n$ which contains a. Thus the pairs (a, K) are the only elements of sort 1.

— $(a, L) \leq (b, M)$ if and only if $L \subseteq M$. We consider the (definable) equivalence relation $(a, L) \sim (b, M) \iff L = M$. Thus we may identify the equivalence class of (a, L) with L.

— $I((a, L), (b, M))$ if and only if $L \subseteq M$ and $a = b$.

— If L is a finite Galois extension of K, then $A \cap L^3$ and $M \cap L^3$ are the graphs of addition and multiplication on L respectively.

5.5. Proposition. Let K be a field. Consider the ω2-sorted structure $(Sep(K), SG(K), \cdot)$ in the language $\mathcal{L}_{sep} \cup \mathcal{L}_G \cup \{\cdot\}$, where $\cdot$ denotes the action of $\mathcal{G}al(L/K)$ on L, for every finite Galois extension L of K. Then $(Sep(K), SG(K), \cdot)$ is interpretable in $Sep(K)$.

5.6. Theorem (Keisler [Ke]). Let K_1 and K_2 be fields, which are elementary equivalent in some language $\mathcal{L}'$ containing the language of fields, let P be a unary predicate not in $\mathcal{L}'$. Let F_1 and F_2 be algebraically closed fields containing K_1 and K_2, with F_i infinite dimensional as a K_i-vector space, and consider the $\mathcal{L}' \cup \{P\}$-structures (F_i, K_i) defined above.

(1) If $K_1 \equiv K_2$ then $(F_1, K_1) \equiv_{acl(\emptyset)} (F_2, K_2)$.

(2) If K_1 is κ-saturated and the transcendence degree of F_1 over K_1 is $\geq \kappa$, then (F_1, K_1) is κ-saturated.

5.7. Theorem.. Let K and L be fields, and E a subfield of K, L, such that K and L are regular extensions of E.

(1) If $K \equiv_E L$ then $Sep(K) \equiv_{Sep(E)} Sep(L)$.

(2) If K is κ-saturated, so is $Sep(K)$.

5.8. Interpretation of finite Galois extensions in K. Let L be a finite Galois extension of K, and assume that $L = K(\alpha)$. Let $p(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ be the minimal polynomial of α over K, and identify L with $K \oplus \alpha K \oplus \cdots \oplus \alpha^{n-1} K$. Then L is isomorphic to K^n as a K-vector space. Consider the structure $L^* = (K^n, +, \odot)$, where $\odot$ is a bilinear map, image of multiplication under the identification of L with $K \oplus \alpha K \oplus \cdots \oplus \alpha^{n-1} K$. E.g., $\alpha \odot -$ is the linear transformation with matrix

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$$

and similarly $\alpha^i \odot -$ has matrix M^i_α. Note that the only parameters needed to define L^* are the elements $a_1, \ldots, a_n$, and that this interpretation is uniform in n.

An element of $\mathcal{G}al(L/K)$ is then a linear transformation of K^n respecting $\odot$. Alternatively, an element σ of $\mathcal{G}al(L/K)$ is uniquely determined by $\sigma(\alpha)$, i.e., by an element of L^* satisfying $p(X) = 0$.

5.9. For later use, we will show an analog of the Keisler Shelah theorem.

Proposition. Let K_1 and K_2 be fields, which are regular extensions of a subfield E. We then have inclusions $SG(E) \subseteq SG(K_1)$ and $SG(E) \subseteq SG(K_2)$. Assume that $SG(K_1) \equiv_{SG(E)} SG(K_2)$. Then there is an ultrafilter $\mathcal{U}$ on some index set I such that

$$SG(K_1)^{\mathcal{U}} \simeq_{SG(E)} SG(K_2)^{\mathcal{U}}.$$

5.10. Theorem (Cherlin, Van den Dries, Macintyre). Let K_1 and K_2 be PAC fields, separable over a common subfield E. The following conditions are equivalent:

(1) $K_1 \equiv_E K_2$.

(2) (i) K_1 and K_2 have the same degree of imperfection.

(ii) There is $\varphi \in G(E)$ such that $\varphi(K_1 \cap E^s) = K_2 \cap E^s$, and

(iii) Let $\Phi : G(K_2 \cap E^s) \to G(K_1 \cap E^s)$ be the isomorphism of profinite groups induced by φ, and let $S\Phi : SG(K_1 \cap E^s) \to SG(K_2 \cap E^s)$ be the dual map. Then the partial map $S\Phi : SG(K_1) \to SG(K_2)$ (with domain $SG(K_1 \cap E^s)$) is an elementary $\mathcal{L}_G$-map.

5.11. Application to Frobenius fields. Recall that a Frobenius field is a PAC field K, whose absolute Galois group $G(K)$ has the so-called embedding property (also called Iwasawa property in [CDM]), namely:

Definition. A profinite group G has the *embedding property* iff every diagram

$$(*) \qquad \begin{array}{ccc} & & G \\ & & \downarrow \\ B & \longrightarrow & A \end{array}$$

where the maps are continuous epimorphisms and B is isomorphic to a finite (continuous) quotient of G, can be completed by a continuous epimorphism $G \to B$ making the diagram commutative.

Note that the definition of the embedding property only talks about finite quotients of G, i.e., about $\sim$-equivalence classes of SG. Hence there is a $\mathcal{L}_G$-theory which we will denote by T_{IP}, whose models are precisely the complete systems associated to groups with the embedding property. If G is a profinite group, we denote by $Im(G)$ the set of (isomorphism classes of) finite continuous quotients of G. Iwasawa has shown that the free profinite group on $\aleph_0$ generator, $\hat{F}_\omega$, is characterised by the embedding property, by the fact that $Im(\hat{F}_\omega)$ contains all finite groups, and by $|S\hat{F}_\omega| = \aleph_0$. This result translates as the $\aleph_0$-categoricity of the theory of $S\hat{F}_\omega$, and was extended by Cherlin, Van den Dries and Macintyre as follows:

Theorem (Cherlin, Van den Dries, Macintyre). Let G be a profinite group with the embedding property. Then $Th(SG)$ is $\aleph_0$-categorical, and is axiomatised by adding to T_{IP} the sentences describing $Im(G)$.

Remark. The proof of this result shows more: given G and H with the embedding property, with $Im(G) = Im(H)$ and $|SG| = |SH| = \aleph_0$, and $\sim$-equivalence classes $[\alpha]_\sim$ in SG and $[\beta]_\sim$ in SH, and a partial isomorphism $f : [\alpha]_\sim \to [\beta]_\sim$, the isomorphism f lifts to an isomorphism $SG \to SH$ (or see [22] 23.21). This implies also, using compactness, that any partial $\mathcal{L}_G$-isomorphism $f : SG \to SH$, where $dom(f) \models T_G$, is an elementary $\mathcal{L}_G$-map. (Recall that the subsets of SG which are models of T_G correspond by duality to the continuous quotients of G. Our hypothesis implies that $Im(f)$ will also be a model of T_G.)

5.12. Theorem (Cherlin, Van den Dries, Macintyre). Let K_1 and K_2 be Frobenius fields of the same degree of imperfection, and separable over a subfield E. Assume that $Im(G(K_1)) = Im(G(K_2))$. The following conditions are equivalent:

(1) $K_1 \equiv_E K_2$.

(2) There is an E-isomorphism $\varphi : E^s \cap K_1 \to E^s \cap K_2$.

6 Difference fields

6.1. Setting and notation. We will always work inside a large algebraically closed field Ω, which will contain all fields considered. The language $\mathcal{L}_\sigma$ is obtained by adjoining to the language $\mathcal{L} = \{+, -, \cdot, 0, 1\}$ of rings a unary function symbol for σ. A difference field is a field K with a distinguished automorphism σ, and is naturally an $\mathcal{L}_\sigma$-structure. I should mention that our definition of difference fields slightly differs from the usual definition which only requires σ to be a field embedding, i.e., not necessarily onto. Our difference fields are called *inversive* by Cohn. All the basic algebraic results on difference fields can be found in the first few chapters of Cohn's book [14]. The main model-theoretic results can be found in [8] and [9].

In characteristic $p > 0$, the map $Frob : x \mapsto x^p$ defines a monomorphism on K, called the *Frobenius automorphism*, and the image K^p of K by this map is a subfield of K.

6.2. The theory ACFA

Recall that the model companion ACFA of the theory of difference fields in the language $\mathcal{L}_\sigma$ is axiomatised by the scheme of axioms expressing the following properties of (K, σ):

— K is an algebraically closed field and σ is an automorphism of K.

— If U and V are varieties defined over K, such that $V \subseteq U \times \sigma(U)$ and the projections $V \to U$ and $V \to \sigma(U)$ are generically onto, then there is a tuple $\bar{a}$ such that $(\bar{a}, \sigma(\bar{a})) \in V$ (here $\sigma(U)$ denotes the variety image by σ of the variety U).

6.3. Difference polynomial rings

Let $k \subseteq K$ be difference fields, with K a sufficiently saturated model of ACFA. We define the *difference polynomial ring* $k[X_1, \ldots, X_n]_\sigma$ by taking the ring $k[X_1, \ldots, X_n]_\sigma$ to be the ordinary

polynomial ring $k[\sigma^j(X_i) \mid i = 1, \ldots, n, j \in \mathbb{N}]$, and extending σ to $k[X_1, \ldots, X_n]_\sigma$ in the way suggested by the name of the generating elements. Note that σ is not onto. The order of a difference polynomial f is the largest m such that some indeterminate $\sigma^m(X_i)$ appears in f.

Ideals I of $k[X_1, \ldots, X_n]_\sigma$ satisfying $\sigma(I) \subseteq I$ are called *σ-ideals*. A *perfect* σ-ideal of $k[X_1, \ldots, X_n]_\sigma$ is a σ-ideal I satisfying moreover that $a\sigma(a^m) \in I$ implies $a \in I$ for all $m \in \mathbb{N}$. Thus a perfect σ-ideal is radical. A *prime σ-ideal* is a σ-ideal which is prime and perfect. Quotients of $k[X_1, \ldots, X_n]_\sigma$ by prime σ-ideals are domains, on which σ defines an embedding. Thus they embed uniquely in a smallest difference field. If $\bar{a}$ is an n-tuple of K, we define $I_\sigma(\bar{a}/k) = \{f(\bar{X}) \in k[\bar{X}]_\sigma \mid f(\bar{a}) = 0\}$, where $\bar{X} = (X_1, \ldots, X_n)$. Then $I_\sigma(\bar{a}/k)$ is a prime σ-ideal of $k[X_1, \ldots, X_n]_\sigma$.

While $k[X_1, \ldots, X_n]_\sigma$ has infinite ascending chains of σ-ideals, it satisfies the ascending chain condition on perfect σ-ideals and on prime σ-ideals. A *σ-equation* (over k) is an equation of the form $f(x_1, \ldots, x_n) = 0$ where $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]_\sigma$. The set of solutions (in K^n) of a set of σ-equations is called a *σ-closed set*; it can be defined by a finite set of σ-equations. Thus the topology on K^n whose basic closed sets are the σ-closed sets is Noetherian. A σ-closed set is called *irreducible* if it is not the union of two proper σ-closed subsets. Every σ-closed set of K^n is the union of finitely many irreducible σ-closed sets, which are called its *irreducible components*. If the irreducible σ-closed set V is defined by σ-equations over k, then V is *defined over* k, and the set of difference polynomials over k vanishing on V is a prime σ-ideal of $k[X_1, \ldots, X_n]_\sigma$, denoted by $I(V)$. If $\bar{a} \in K^n$ and $I(V) = I_\sigma(\bar{a}/k)$, then a is called a *generic of* V over k.

6.4. Transformal transcendence bases. Let $k \subseteq K$ be as above, and let $\bar{a}$ be a tuple of elements of K. We denote by $k(\bar{a})_\sigma$ the difference field generated by $\bar{a}$ over k, i.e., the difference subfield $k(\sigma^i(\bar{a}) \mid i \in \mathbb{Z})$ of K. If the transcendence degree $tr.deg(k(\bar{a})_\sigma/k)$ of $k(\bar{a})_\sigma$ over k is finite then we say that $\bar{a}$ is *transformally algebraic over k*. In that case, there is a non-negative integer m such that $k(\bar{a})_\sigma \subseteq k(\bar{a}, \ldots, \sigma^m(\bar{a}))^{alg}$. Observe that since σ and σ^{-1} are automorphisms of $k(\bar{a})_\sigma$, we then have $k(\bar{a})_\sigma \subseteq k(\sigma^j(\bar{a}), \ldots, \sigma^{j+m}(\bar{a}))^{alg}$ for every $j \in \mathbb{Z}$.

An element $b \in K$ is *transformally transcendental over k*, if the elements $\sigma^i(b)$, $i \in \mathbb{Z}$, are algebraically independent over k. Observe that a tuple $\bar{a}$ is either transformally algebraic over k, or contains an element which is transformally transcendental over k. We call a set $B \subseteq K$ *transformally independent* over k if the elements $\sigma^j(b)$, $b \in B$, $j \in \mathbb{Z}$, are algebraically independent over k. Equivalently, if the elements $\sigma^j(b)$, $b \in B$, $j \in \mathbb{N}$, are algebraically independent over k. If L is a difference subfield of K containing k, and $B \subset L$ is transformally independent over k and maximal such, then B is called a *transformal transcendence basis* of L over k. Observe that L is then transformally algebraic over $k(B)_\sigma$. Any two transformal transcendence bases of L over k have the same cardinality, and this cardinality is called the transformal transcendence degree of L over k, and denoted by $\Delta(L/k)$. If $\bar{a}$ is a finite tuple, we also define $\Delta(\bar{a}/k) = \Delta(k(\bar{a})_\sigma/k)$; observe that $\Delta(\bar{a}/k) \leq tr.deg(k(\bar{a})/k)$ (the transcendence degree of $k(\bar{a})$ over k).

7 Abelian varieties

7.1. Definitions. Recall that a variety V is complete if for any variety W the projection map $\pi : V \times W \to W$ is closed, that is the image of a (Zariski) closed set by π is closed.

Using the definition, one shows easily that a closed subvariety of a complete variety is complete, and that the image of a complete variety by a morphism is also complete. Examples of complete varieties are the projective spaces $\mathbb{P}^n$, $n \geq 1$.

An abelian variety is a connected algebraic group which is complete. The completeness and connectedness imply that the group law is commutative. By the above, a connected algebraic subgroup B of an abelian variety A is an abelian variety, and so is the quotient group A/B. Below we list some important results on abelian varieties. The references are to S. Lang's book on abelian varieties [38], chapter II.

From now on, A will denote an abelian variety defined over the field k. The group law of A is $+$, and its identity element is 0.

7.2. Let $f : V \to A$ be a rational map from a variety V into the abelain variety A. Then f is defined at every simple point of V.

Recall that in an algebraic group all points are simple. Hence if V is an algebraic group, f is everywhere defined.

7.3. Let $f : V \times W \to A$ be a rational map of a product of varieties into an abelian variety A. Then there are two rational maps $f_1 : V \to A$ and $f_2 : W \to A$ such that if (a, b) is a generic point of $V \times W$ then $f(a, b) = f_1(a) + f_2(b)$.

f_1 and f_2 are uniquely determined by this property, up to addition by an element of A. If f (and V, W, A) is defined over k and $V(k)$ contains a simple point, then f_1 and f_2 can be chosen defined over k.

7.4. Let $f : G \to A$ be a rational map of a connected algebraic group G into an abelian variety A. Then the map $f_0 : G \to A$ defined by $f_0(a) = f(a) - f(e)$ is an algebraic group homomorphism (e is the identity element of G).

7.5. Let $f : G \times H \to A$ be an algebraic group homomorphism defined over k, where G, H are connected algebraic groups. Then there are algebraic group homomorphisms $f_1 : G \to A$ and $f_2 : H \to A$, both defined over k, and such that $f(a, b) = f_1(a) + f_2(b)$ for $(a, b) \in G \times H$.

7.6. Chow's Theorem. Let B be an abelian subvariety of A, defined over $K \supseteq k$. Assume that the relative algebraic closure of k in K is purely inseparable over k. Then B is defined over k.

Note that this in particular implies:

7.7. All abelian subvarieties of A are defined over the separable closure k^s of k.

7.8. If B is an abelian variety defined over k, then the group $Hom(A, B)$ of algebraic homomorphisms from A to B is countable, and all its elements are defined over k^s.

7.9. Let B be an abelian variety. Then $Hom(A, B)$ is a a free $\mathbb{Z}$-module of finite rank.

7.10. Poincaré's complete reducibility theorem. Let B be an abelian subvariety of A. Then there is an abelian subvariety C of A such that $A = B + C$ and $B \cap C$ is finite. If B is defined over k then we can take C also defined over k.

7.11. Let B be an abelian variety, and $f : A \to B$ be a homomorphism. Then the graph of f is an abelian subvariety C of $A \times B$ satisfying: for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in C$.

The converse is also true: if C is an abelian subvariety of $A \times B$ having the property that for every $a \in A$ there is a unique $b \in B$ with $(a, b) \in C$, then C is the graph of a homomorphism from A to B.

From this one deduces:

7.12. Let A, B, C be abelian varieties. Assume that $f : A \to B$ and $g : A \to C$ are homomorphisms and satisfy $\ker(f) \subseteq \ker(g)$, and that f is onto. Then there is a unique homomorphism $h : B \to C$ such that $g = hf$. *Proof.* Let $D \subseteq A \times B \times C$ be the graph of $(f \times g)$, and let $E \subseteq B \times C$ be its projection. Then E is an abelian variety, which projects onto B since f is surjective. Let $b \in B$, $c \in C$ such that $(b, c) \in E$. By definition of E, there is $a \in A$ such that $f(a) = b$ and $g(a) = c$. If $a' \in A$ is such that $f(a') = b$, then $f(a - a') = 0$, which implies that $g(a - a') = 0$ and $g(a') = c$. This shows that given $b \in B$, there is a unique $c \in C$ such that $(b, c) \in E$, and therefore that E is the graph of a homomorphism $h : B \to C$. Clearly $g = hf$, and h is unique.

7.13. Definition. Let B be an abelian variety. We say that a homomorphism $f : A \to B$ is an *isogeny* if f is onto and its kernel is finite. We say that A and B are isogenous if there is an isogeny $f : A \to B$.

Clearly the relation of isogeny is reflexive and transitive. It is also symmetric:

7.14. Let $f : A \to B$ be an isogeny, and let n be the size of its kernel. There is a unique isogeny $g : B \to A$ such that $fg = [n]_B$ and $gf = [n]_A$ (multiplication by n in the abelian groups B and A respectively). *Proof.* By definition f is onto, and its kernel is contained in $A[n] = \ker([n]_A)$ (the elements of A of order n). Now apply 7.12 to get $g : B \to A$ such that $[n]_A = gf$. Since gf is an isogeny and f is onto, g is an isogeny. We then have $(fg)f = f(gf) = f[n]_A = [n]_B f$, which implies that $fg = [n]_B$.

7.15. Torsion subgroup. Let $Tor(A)$ be the subgroup of torsion elements of A. Then $Tor(A)$ is divisible, and is dense in A. Thie implies in particular that if $f, g : A \to B$ are homormorphisms of abelian varieties which agree on $Tor(A)$, then they are equal. If ℓ is a prime number different from $char(k)$, the same is true for $Tor_\ell(A)$, the subgroup of elements of A of order a power of ℓ.

Let q be a prime power, and $A[q]$ the subgroup of A of elements of order q. There are numbers $s \leq r$ not depending on q such that

$$A[q] \simeq \begin{cases} (\mathbb{Z}/q\mathbb{Z})^r & \text{if } q \text{ is prime to } char(k), \\ (\mathbb{Z}/q\mathbb{Z})^s & \text{if } char(k) \text{ divides } q. \end{cases}$$

7.16. Definition. An abelian variety is simple if it has no infinite proper abelian subvariety. Assume that A and B are simple varieties.

(1) If A and B are isogenous, then every non-zero element of $Hom(A, B)$ (the group of homomorphisms from A to B) is an isogeny.

(2) If A and B are not isogenous, then $Hom(A, B) = (0)$.

(3) Let $End(A)$ be the ring of endomorphisms of A; it contains a copy of $\mathbb{Z}$, namely $\{[n]_A \mid n \in \mathbb{Z}\}$. The ring $E(A) = End(A) \bigotimes_{\mathbb{Z}} \mathbb{Q}$ is a division ring.

Proof. Let $f : A \to B$ be a homorphism. The simplicity of A and B implies that $\ker(f)$ is either finite or all of A. In the first case, $f(A)$ is an infinite abelian subvariety of B, which must therefore equal B, which shows that f is then an isogeny. If $\ker(f) = A$ then $f = 0$. This proves (1) and (2).

For (3), let $f \in E(A)$ be non-zero, and choose $N \in \mathbb{N}^*$ such that $[N]f \in End(A)$. By 7.14, there is $g \in End(A)$ such that $g[N]f \in \mathbb{Z}$, which shows that f is invertible in $E(A)$ since all non-zero integers are invertible in $E(A)$.

7.17. By Poincaré's reducibility theorem 7.10, there are simple subvarieties $A_1, \ldots, A_k$ of A such that for any i, the intersection of A_i with the sum of the others is finite. From this one deduces that the abelian varieties $A_1 \times \cdots \times A_k$ and A are isogenous. Moreover, by the above, the varieties $A_1, \ldots, A_k$ are uniquely determined up to an isogeny and a permutation of indices.

Observe also that if B is a simple variety and $Hom(A, B) \neq (0)$, then B is isogenous to a subvariety of A.

Assume that $A_1, \ldots, A_m$ are pairwise non-isogenous, and that each A_j, $j > m$, is isogenous to A_i for some $i \leq m$. For $i \leq m$ let n_i be the number of varieties among $\{A_1, \ldots, A_k\}$ which are isogenous to A_i. By 7.5, every endomorphism of A decomposes into a product of homorphisms $A_i \to A_j$ for $1 \leq i, j \leq k$, and therefore

$$End(A) \simeq \prod_{i=1}^{m} M_{n_i}(End(A_i)).$$

7.18. Let B be an abelian subvariety of A. There are homomorphisms $f_i : A \to A_i$ where the A_i's are isogenous to simple subvarieties of A, $i = 1, \ldots, m$, such that $B = \bigcap_i \ker(f_i)$. *Proof.* Let$C = A/B$, and choose simple subvarieties $A_1, \ldots, A_k$ of A and an isogeny $f : C \to A_1 \times \cdots \times A_k$. Let $\pi : A \to C$ and $\pi_i : A_1 \times \cdots \times A_k \to A_i$, $i = 1, \ldots, k$ be the natural projections. Then $ker(f) = \bigcap_i \ker(\pi_i f)$. Let $n = |\ker(f)|$, and let $f_i = [n]\pi_i f \pi : A \to A_i$. Since B is connected, $B = \bigcap_i \ker(f_i)$.

From this one deduces easily:

Let A, B be abelian varieties, and assume that $Hom(A, B) = (0)$. Let C be an abelian subvariety of $A \times B$. Then $C = C_1 \times C_2$ where C_1 and C_2 are abelian subvarieties of A and B respectively.

8 Graded rings, twisted Laurent polynomial rings

8.1. Definitions. A ($\mathbb{Z}$-)graded ring is a ring R whose underlying additive group is written as $R = \bigoplus_{m\in\mathbb{Z}} R_m$, with $R_iR_j \subset R_{i+j}$ for $i, j \in \mathbb{Z}$.

The decomposition $\bigoplus R_m$ is called the grading of R. The elements of R_m are called homogeneous of degree m, and R_m is the homogeneous component of degree m.

8.2. Example. Let R be a ring, t an indeterminate. Then $R[t]$ has a natural grading: $K[t] = \bigoplus_{m\in\mathbb{N}} Rt^m$. Observe that the homogeneous components of negative degree are 0. In fact, since the component of degree 0 contains R, $R[t]$ is a graded R-algebra.

8.3. Let R be a ring, and $\tau \in Aut(R)$. We define the twisted Laurent polynomial ring $R^t[\tau, \tau^{-1}]$ to be the ring whose underlying additive group is $\bigoplus_{m\in\mathbb{Z}} R\tau^m$, with multiplication defined by $a\tau^i b\tau^j = a\tau^i(b)\tau^{i+j}$ for $i, j \in \mathbb{Z}$, and extended using distributivity to $R^t[\tau, \tau^{-1}]$.

$R^t[\tau, \tau^{-1}]$ has a natural $\mathbb{Z}$-grading, with $R\tau^m$ the homogeneous component of degree m for $m \in \mathbb{Z}$. We also consider the subring $R^t[\tau]$ of $R^t[\tau, \tau^{-1}]$. If $f = \sum_{i=0}^n a_i\tau^i \in R^t[\tau]$ satisfies $a_n \neq 0$, we will call n the degree of f.

8.4. Proposition. Assume that R is a division ring (every element has an inverse). Then $R^t[\tau]$ is a left-euclidian domain and every ideal of $R^t[\tau, \tau^{-1}]$ is principal. If $m \in \mathbb{N}^*$, then every left ideal of $R^t[\tau, \tau^{-1}]$ is generated by m elements.

Proof. Let $f = \sum_{i=0}^m a_i\tau^i$, $g = \sum_{j=0}^n b_j\tau^j$, with $a_mb_n \neq 0$. First of all, $fg \neq 0$: the coefficient of τ^{m+n} is $a_m\tau^m(b_n)$ which is non-zero since a_m and b_n are non-zero and τ is an automorphism. This shows that $R^t[\tau]$ is a domain.

We will now show that there is a unique pair (u, v), with v of degree $< n$, such that $f = ug + v$. Note that the unicity will follow from the existence: an element of degree $< n$ is in $\bigoplus_{i=0}^{n-1} R\tau^i$, a multiple of g is in $\bigoplus_{i\geq n} R\tau^i$, and $R^t[\tau]$ is a domain. We show the existence of (u, v) by induction on m: if $m < n$, then $u = 0$, $v = f$. Suppose $m \geq n$, and that it is proved for all polynomials of degree $\leq m - 1$.

Consider $f' = f - a_m\tau^{m-n}(b_n^{-1})\tau^{m-n}g$. Then f' is of degree $\leq m$, and the coefficient of τ^m in f' is equal to $a_m - (a_m\tau^{m-n}(b_n^{-1})\tau^{m-n}(b_n)) = 0$. By induction hypothesis, $f' = u'g + v$, with v of degree $< n$, and therefore $f = ug + v$ with $u = u' + a_m\tau^{m-n}(b_n^{-1})\tau^{m-n}$.

Let I be a left ideal of $R^t[\tau, \tau^{-1}]$. Then I is generated by the left ideal $I_0 = I \cap R^t[\tau]$ of $R^t[\tau]$, and it therefore suffices that I_0 is principal. Let $g \in I_0$ be of least possible degree, and let $f \in I_0$. Then $f = ug + v$ with $v \in I_0$ of degree smaller than the degree of g. By choice of g, we have $v = 0$, which shows that I_0 is the ideal generated by g.

Let I be a left ideal of $R^t[\tau, \tau^{-1}]^m$. If $m = 1$, then I is principal. Assume $m > 1$ and that the result is proved for $m - 1$. Let I_1 be the projection on the first coordinate of I, and $I_2 = I \cap ((0) \times R^t[\tau, \tau^{-1}]^{m-1})$. Then I_1 is principal, generated by f_1 say, and I_2 is a left ideal of $(0) \times R^t[\tau, \tau^{-1}]^{m-1}$. Let $f_2, \ldots, f_m \in R^t[\tau, \tau^{-1}]$ be such that $(f_1, \ldots, f_m) \in I$.

Let $(g_1, \ldots, g_m) \in I$. Then $g_1 = h_1f_1$ for some $h_1 \in R^t[\tau, \tau^{-1}]$. Thus $(g_1, \ldots, g_m) - h_1(f_1, \ldots, f_m) \in I_2$, which shows that I is generated by I_2 and $(f_1, \ldots, f_m)$. Using the induction hypothesis, this shows that I is generated by m elements.

References

[1] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239 – 271.

[2] N. Bourbaki, XI, Algèbre Chapître 5, Corps commutatifs, Hermann, Paris 1959.

[3] E. Bouscaren, The group configuration – after E. Hrushovski, in: The model theory of groups, Nesin-Pillay ed., Notre Dame Math. Lect. 11, Notre Dame (1989).

[4] C.C. Chang, H.J. Keisler, Model Theory, North-Holland Publishing Company, Amsterdam 1973.

[5] Z. Chatzidakis, Model theory of profinite groups having the Iwasawa property, Ill. J. of Math. 42 Nr 1 (1998), 70 – 96.

[6] Z. Chatzidakis, Simplicity and Independence for Pseudo-algebraically closed fields, in: Models and Computability, S.B. Cooper, J.K. Truss Ed., London Math. Soc. Lect. Notes Series 259, Cambridge University Press, Cambridge 1999, 41 – 61.

[7] Z. Chatzidakis, L. van den Dries, A. Macintyre, Definable sets over finite fields, J. reine u. ang. Math. 427 (1992), 107 – 135.

[8] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. A.M.S. 351 (1999), 2997 – 3071.

[9] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics, preprint 1999.

[10] Z. Chatzidakis, A. Pillay, Generic structures and simple theories, Ann. P. Appl. Logic 95 (1998), 71 – 92.

[11] G. Cherlin, L. van den Dries, A. Macintyre, Decidability and Undecidability Theorems for PAC-Fields, Bull.AMS 4 (1981), 101-104.

[12] G. Cherlin, L. van den Dries, A. Macintyre, The elementary theory of regularly closed fields, preprint 1980.

[13] G. Cherlin, L. van den Dries, A. Macintyre, The elementary theory of regularly closed fields, preprint 1982.

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

[15] F. Delon, Idéaux et types sur les corps séparablement clos, Supplément au Bull. de la S.M.F, Mémoire 33, Tome 116, 1988.

[16] L. van den Dries, Dimension of definable sets, algebraic boundedness and henselian fields, Annals of Pure and Applied Logic 45 (1989), 189 – 209.

[17] L. van den Dries, K. Schmidt, Bounds in the theory of polynomials rings over fields. A non-standard approach. Invent. Math. 76 (1984), 77 – 91.

[18] J.-L. Duret, Les corps pseudo-algébriquement clos non séparablement clos ont la propriété d'indépendance, in: Model theory of algebra and arithmetic, Proc. Karpacz 1979, Springer LN 834 (1980), 136 – 161.

[19] Yu. Ershov, Fields with a solvable theory (Eng. transl.), Sov. Math. Doklady 8 (1967), 575 – 576.

[20] Ju. L. Ershov, Regularly closed fields, Soviet Math. Doklady 21 (1980), 510 – 512.

[21] Ju. L. Ershov, Undecidability of regularly closed fields, Alg. and Log. 20 (1981), 257 – 260.

[22] M. Fried, M. Jarden, Field Arithmetic, Ergebnisse 11, Springer Berlin-Heidelberg 1986.

[23] D. Haran, M. Jarden, Regular split embedding problems over complete local fields, Forum Mathematicum 10 (1998) no 3, 329 – 351.

[24] W. Hodges, Groups in pseudo-finite fields, this volume.

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

[26] E. Hrushovski, The Mordell-Lang conjecture for function fields, J. of the AMS Vol 9 Nr 3 (1996), 667 – 690.

[27] E. Hrushovski, The Manin-Mumford Conjecture and the Model Theory of Difference Fields, preprint 1996.

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

[29] E. Hrushovski, A. Pillay, Definable subgroups of algebraic groups over finite fields, J. reine angew. Math 462 (1995), 69 –91.

[30] M. Jarden, The elementary theory of ω-free Ax fields, Inv. Math. 38 (1976), 187 – 206.

[31] M. Jarden, Algebraic dimension over Frobenius fields, Forum Math. 6 (1994), 43-63.

[32] H. J. Keisler, Complete theories of algebraically closed fields with distinguished subfields, Michigan Math. J. 11, 71 – 81.

[33] M. Jarden, U. Kiehne, The elementary theory of algebraic fields of finite corank, Inv. Math. 30 (1975), 275 –294.

[34] B. Kim, Forking in simple unstable theories, J. London Math. Soc. 57 (1998), 257 – 267.

[35] B. Kim, A. Pillay, Simple theories, Ann. P. Appl. Logic 88 Nr 2-3 (1997), 149 – 164.

[36] G. Kreisel, J.-L. Krivine, Eléments de logique mathématique, Dunod, Paris 1967.

[37] S. Lang, Introduction to algebraic geometry, Addison-Wesley Pub. Co., Menlo Park 1973.

[38] S. Lang, Abelian varieties, Springer-Verlag, New-York Tokyo 1983.

[39] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag New York Inc., 1983.

[40] S. Lang, Algebra, Addison-Wesley Pub. Co., Menlo Park 1984.

[41] A. Macintyre, Generic automorphisms of fields, APAL 88 Nr 2-3 (1997), 165 – 180.

[42] M. Messmer, Groups and fields interpretable in separably closed fields, Trans. A.M.S. 344 (1994), 361 – 377.

[43] A. Pillay, An introduction to stability theory, Oxford Logic Guide 8, Clarendon Press, Oxford, 1983.

[44] A. Pillay, Model theory of algebraically closed fields, in: Stability theory and algebraic geometry, an introduction, Bouscaren and Lascar ed., to appear in Springer LN.

[45] A. Pillay, Geometric Stability, Oxford University Press, Oxford 1996.

[46] B. Poizat, Cours de Théorie des Modèles, Nur Al-Mantiq Wal-Ma'rifah, Paris 1985.

[47] B. Poizat, Groupes stables, Nur Al-Mantiq Wal-Ma'rifah, Paris 1987.

[48] F. Pop, Embedding problems over large fields, Ann. of Math. (2) 144 (1996), no. 1, 1 – 34.

[49] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's papers in pure and applied math., No 24, 1970.

[50] S. Shelah, Simple unstable theories, Ann. P. Appl. Logic 19 (1980), 177 – 203.

[51] C. Wood, Notes on the stability of separably closed fields, JSL 44 (1979), 412 – 416.

[52] O. Zariski, P. Samuel, Commutative Algebra Vol. 1, Graduate Texts in Mathematics 28, Springer-Verlag New York Inc., 1986.