Notes on the model theory of finite and pseudo-finite fields

Zoé Chatzidakis, CNRS - Université Paris 7.

These notes contain the material covered during a mini-course given at the University of Helsinki, 22 - 29 April 2009. The reader wishing to see more on pseudo-finite fields can also consult the notes on the course given in Madrid (November 2005), posted on my web page. The main part of this course is based on a paper by James Ax [A], The elementary theory of finite fields. The interested reader can find a very complete account of the theory of finite fields in the book of Fried and Jarden [FJ].

The course was funded by the Finnish network MALJA. I also thank the audience for their enthusiasm and comments.

Table of contents

1. Finite fields - properties

(1.1) Basic properties of finite fields

The characteristic of a unitary commutative ring is the smallest positive integer n such that $1+1+\cdots+1$ (n times) equals 0. If there is no such integer n, one says that the characteristic is 0. If R is a finite ring, and a fortiori a finite field, then its characteristic is finite. Hence, if F is a finite field, the homomorphism $\mathbb{Z} \to F$ which sends $1 \in \mathbb{Z}$ to $1 \in F$ must have kernel a prime ideal, i.e., $p\mathbb{Z}$ for some prime p.

Conversely, if p is a prime number, then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements. This field is denoted by $\mathbb{F}_p$, and it is the *prime field of characteristic* p, i.e., it is contained in every field of characteristic p (by the above). In a field of characteristic 0, the subring generated by 1 is (isomorphic to) $\mathbb{Z}$, and therefore the field also contains the field of fractions of $\mathbb{Z}$, $\mathbb{Q}$. We call $\mathbb{Q}$ the *prime field of characteristic* 0.

Let F be a finite field of characteristic $p > 0$. Since $1 \in F$, it necessarily contains the field $\mathbb{F}_p$, and is therefore a vector space over $\mathbb{F}_p$, whence of cardinality p^n for some $n \in \mathbb{N}$.

Let F be a field of characteristic p having $q = p^n$ elements, let K be an algebraically closed field containing F. Let us consider the multiplicative group $F^\times = F \setminus \{0\}$ of F. It has $q-1$ elements and hence every non-zero element of F satisfies the equation $X^{q-1} - 1 = 0$. [If G is a finite group of size n, then every element g of G satisfies $g^n = 1$]. Thus all elements of F satisfy $X^q - X = 0$. Let $f(X) = X^q - X$, a polynomial over $\mathbb{F}_p$. Then $f'(X) = qX^{q-1} - 1 = -1$ because "$q = 0$" since it is a power of the characteristic. Hence all roots of $F(X) = 0$ are simple roots, and we obtain

$$X^q - X = \prod_{a \in F} (X - a).$$

Indeed, since every element of $\mathbb{F}_q$ satisfies $X^q - X = 0$, we know that each $(X-a)$, $a \in \mathbb{F}_q$, divides $X^q - X$, and therefore so does their product $\prod_{a\in F}(X-a)$. Degree considerations and the fact that the coefficient of X^q is 1 imply that these two polynomials are equal.

Conversely, let us consider the set $S \subset K$ of all solutions of $X^q - X = 0$. As above, its roots are all distinct. S is closed under multiplication, and $S \setminus \{0\}$ by multiplicative inverse. Because we are in characteristic p and q is a power of p, we obtain, using the binomial expansion of $(a+b)^n$ and the fact that "$p = 0$", that $(a+b)^p = a^p + b^p$, and $(a+b)^q = a^q + b^q$. This implies that S is closed under addition, and is therefore a subfield of K.

So, we have shown:

Theorem. Let F be a finite field. Then for some prime p and $q = p^n$, F has q elements. Its elements are exactly the roots of the equation $X^q - X = 0$.

(1.2) Existence? We actually haven't shown that for every n there is a field with p^n elements. To do that, we accept that $\mathbb{F}_p$ exists, and that it embeds into some algebraically closed field K. Then, one shows, by induction on the degree n of a polynomial $f(X)$, that $f(X)$ can be written as the product of an element $c \in K$ (c is the coefficient of X^n) and of n linear terms $(X-a)$ for some elements $a \in K$. Thus, in K, the polynomial $X^q - X$ is the product of q linear factors of this form, and because the derivative of $X^q - X$ is

identically equal to -1, these roots are simple: i.e., $X^q - X$ has q distinct solutions in K. By the above, the set S of these roots is a field with q elements, and which is unique up to isomorphism. We denote this field by $\mathbb{F}_q$.

(1.3) The Frobenius map. We have noticed above that when F is a field of characteristic p, then $(a+b)^p = a^p + b^p$ for $a, b \in F$. The map $x \mapsto x^p$ is therefore a ring morphism (as it obviously is a multiplicative map). Also, as $x^p = 0$ implies $x = 0$, it is injective. The map $x \mapsto x^p$ is called the *Frobenius map*, and I will denote it by Frob_p, or Frob. Similarly, if $q = p^n$, then I'll denote Frob^n also by Frob_q.

(1.4) The multiplicative group of a finite field. Let $F = \mathbb{F}_q$ be a finite field. We will show that $F^\times$ is cyclic. It can be written as a finite direct sum of cyclic subgroups, and if it is not cyclic, then its exponent[1] m is a proper divisor of $q-1$. But all roots of $X^{q-1} = 1$ are simple roots, whence all roots of $X^m = 1$ are simple as well. This implies that $q - 1 = m$.

(1.5) Perfect fields. A field F of characteristic $p > 0$ is *perfect* if every element of F has a p-th root. By convention, every field of characteristic 0 is perfect.

If $F = \mathbb{F}_{p^n}$ is finite, then the order of $F^\times$ is prime to p, which implies that every element is (multiplicatively) divisible by p, i.e., F is perfect. Another way of seeing this is the fact that the map $\mathrm{Frob} : x \mapsto x^p$ is injective: as F is finite, it must be onto.

An example of imperfect field is $\mathbb{F}_p(t)$, where t is transcendental over $\mathbb{F}_p$. Then the image by Frob of $\mathbb{F}_p(t)$ is $\mathbb{F}_p(t^p)$.

(1.6) The algebraic closure of $\mathbb{F}_p$.

Let m, n be positive integers, p a prime. Then

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \text{ divides } n,$$

and in that case we have $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$.

Indeed, if $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ then $\mathbb{F}_{p^n}$ is in particular an $\mathbb{F}_{p^m}$-vector space, which implies that for some ℓ, $|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^\ell$, i.e., $p^n = p^{m\ell}$ and $n = m\ell$. We then have $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \ell$. Conversely, if m divides n, then $p^m - 1$ divides $p^n - 1$, whence all roots of $X^{p^m-1} = 1$ are contained in $\mathbb{F}_{p^n}$, i.e., $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

It follows easily that for any $m, n \geq 1$,

$$\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^d} \text{ and } \mathbb{F}_{p^m}\mathbb{F}_{p^n}$$

where d is the greatest common divisor of m and n, and e is the least common multiple of m and n. Here, $\mathbb{F}_{p^m}\mathbb{F}_{p^n}$ denotes the field composite of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$, i.e., the subfield (of the large algebraically closed field K) they generate.

Let α be algebraic over $\mathbb{F}_p$. Then $\mathbb{F}_p(\alpha)$ is a finite-dimensional $\mathbb{F}_p$-vector space, and is therefore also finite. This implies that the algebraic closure $\mathbb{F}_p^{alg}$ of $\mathbb{F}_p$ is $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$. [I assume known the fact that every element of the algebraic closure of a field satisfies a

[1] The exponent of a group G is the smallest $n > 0$ such that every element $g \in G$ satisfies $g^n = 1$, and ∞ if such an n doesn't exist.

non-trivial equation with coefficients in the field. One can also show the result directly: if $f(X)$ is a non-constant polynomial with coefficients in $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$, then it in fact belongs to $\mathbb{F}_q[X]$ for some $q = p^n$; hence the roots of $f(X)$ generate a finite field.]

(1.7) More on the Frobenius map. The Frobenius map is the identity on $\mathbb{F}_p$ (since every element of $\mathbb{F}_p$ satisfies $X^p - X = 0$), and defines an automorphism of each $\mathbb{F}_{p^n}$. Hence it defines an element φ of $\mathrm{Aut}(\mathbb{F}_p^{alg}/\mathbb{F}_p)$. Observe that if $d \in \mathbb{N}$, the elements of $\mathbb{F}_p^{alg}$ which are fixed by φ^d are precisely the elements of $\mathbb{F}_{p^d}$. Furthermore, one checks that the restriction $\varphi|_{\mathbb{F}_{p^d}}$ of φ to $\mathbb{F}_{p^d}$ has order exactly d: φ^ℓ being the identity on $\mathbb{F}_{p^d}$ means exactly that all elements of $\mathbb{F}_{p^d}$ satisfy $X^{p^\ell} = X$, and therefore that d divides ℓ.

As $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$, we know that $\mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ has siez at most d. Since $\varphi \in \mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ has order exactly d, this therefore implies that

$$\mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p) \simeq \mathbb{Z}/d\mathbb{Z},$$

and that φ generates $\mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)$.

(1.8) Description of $\mathrm{Aut}(\mathbb{F}_p^{alg}/\mathbb{F}_p)$. While we will not explicitly use it, we can now describe completely $\mathrm{Aut}(\mathbb{F}_p^{alg}/\mathbb{F}_p)$. As $\mathbb{F}_p^{alg}$ is a direct limit of the finite fields $\mathbb{F}_{p^n}$, it follows, by Galois duality, that

$$\mathrm{Aut}(\mathbb{F}_p^{alg}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} := \hat{\mathbb{Z}}.$$

The connecting maps are, for n dividing m, the canonical projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. That is, the group $\hat{\mathbb{Z}}$ is described as the set of sequences $(a_n)_n \in \prod_{n>1} \mathbb{Z}/n\mathbb{Z}$ such that if n divides m, then $a_n \equiv a_m \mathrm{mod}\ n$. It is a profinite group, i.e., an inverse limit of finite groups. It is a closed subgroup of $\prod_{n>1} \mathbb{Z}/n\mathbb{Z}$, where each $\mathbb{Z}/n\mathbb{Z}$ is equipped with the discrete topology, and we take the product topology on $\prod_{n>1} \mathbb{Z}/n\mathbb{Z}$. The element $\varphi = \mathrm{Frob}_p$ is a *topological generator* of $\mathrm{Aut}(\mathbb{F}_p^{alg}/\mathbb{F}_p)$: its restriction to any $\mathbb{F}_q$ generates $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$.

2. An aside: a result of Ax

(2.1) The fact that $\mathbb{F}_p^{alg}$ is a union of finite fields, has a very nice consequence: Let $\bar{X} = (X_1, \ldots, X_n)$ and $\bar{f}(\bar{X})$ be an n-tuple[2] of polynomials $\mathbb{F}_p^{alg}[\bar{X}]$. Assume that $\bar{f}(\bar{X})$ defines an injective map $\tilde{f} : (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$. Then $\tilde{f}$ is also surjective.

Proof. Indeed, the elements of $\bar{f}$ have their coefficients in some $\mathbb{F}_q$, and therefore the restriction of $\tilde{f}$ to $\mathbb{F}_q^n$ is also injective; as $\mathbb{F}_q$ is finite, $\tilde{f}|_{\mathbb{F}_q^n}$ is surjective. This being true on all finite fields containing $\mathbb{F}_q$, we obtain the result.

(2.2) Theorem (Ax) Let $\bar{f}(\bar{X})$ be a n n-tuple of polynomials in $\mathbb{C}[\bar{X}]$, $\bar{X} = (X_1, \ldots, X_n)$, and assume that the map $\tilde{f}$ it defines $\mathbb{C}^n \to \mathbb{C}^n$ is injective. Then it is also surjective.

[2] In class I forgot to say/insist that $\bar{f}$ had to be an n-tuple of polynomials for the map $\tilde{f}$ to make sense. Sorry.

There are two proofs of this result, which we present below. They are essentially equivalent, but one of them uses ultraproducts.

Proof 1 of Ax's result (2.2). One uses the fact that the completions of the theory ACF of algebraically closed fields[3] is obtained by specifying the characteristic. Thus the theory of algebraically closed fields of characteristic 0 is obtained by adding to ACF an infinite set of sentences: for each prime p, an axiom saying that "$p \neq 0$". Any statement true in all (or some) algebraically closed fields of characteristic 0 must therefore be true in all algebraically closed fields of sufficiently large characteristic. Let $m_i(\bar{X})$, $i = 1, \ldots, N(d)$, be an enumeration of the monomials in $\bar{X} = (X_1, \ldots, X_n)$ of degree $\leq d$, and consider the formulas $\varphi(\bar{x})$, $\psi(\bar{x})$, where $\bar{x} = (x_{i,j})_{1 \leq i \leq n, 1 \leq j \leq N(n)}$, and $\bar{y} = (y_1, \ldots, y_n)$, $\bar{z} = (z_1, \ldots, z_n)$:

$$\varphi(\bar{x}): \ \forall \bar{y}, \bar{z} \ \Big(\bigwedge_i \sum_j x_{i,j} m_i(\bar{y}) = \sum_i x_{i,j} m_i(\bar{z})\Big) \rightarrow (\bar{y} = \bar{z})$$

$$\psi(\bar{x}): \ \forall \bar{z} \exists \bar{y} \ \bigwedge_i \sum_j x_{i,j} m_i(\bar{y}) = z_i.$$

Thus $\varphi(\bar{x})$ says that the map $\tilde{f}$ defined by the n-tuple $\bar{f}(\bar{X})$ of polynomials, with $f_i(\bar{X}) = \sum_j x_{i,j} m_j(\bar{X})$, $i = 1, \ldots, n$, is injective, while $\psi(\bar{x})$ says that $\tilde{f}$ is surjective.

All algebraically closed fields of positive characteristic satisfy $\forall \bar{x} \ \varphi(\bar{x}) \rightarrow \psi(\bar{x})$, hence also $\mathbb{C}$ satisfies this sentence. This proves the theorem.

(2.3) Ultraproducts

Definitions. Let I be a set, $(A_i, i \in I)$, a family of $\mathcal{L}$-structures, and $\mathcal{F}$ a subset of $\mathcal{P}(I)$ ($\mathcal{P}(I)$ is the set of subsets of I).

(1) $\mathcal{F}$ is a *filter* (on I) iff: (i) $\emptyset \notin \mathcal{F}$; (ii) if $X, Y \in \mathcal{F}$ then $X \cap Y \in \mathcal{F}$; (iii) if $X \in \mathcal{F}$ and $Y \supseteq X$ then $Y \in \mathcal{F}$.

(2) $\mathcal{F}$ is an *ultrafilter* iff it is a maximal filter, i.e., is contained properly in no filter. One shows easily that a filter $\mathcal{F}$ is an ultrafilter if and only if, for every $X \subseteq I$, either X or $I \setminus X$ is in $\mathcal{F}$.

(3) A filter $\mathcal{F}$ is *principal* iff there is some $i \in I$ such that $\{i\} \in \mathcal{F}$. If there is no such i, it is called *non-principal*.

(4) We define an $\mathcal{L}$-structure on the Cartesian product $\prod_{i \in I} A_i$ as follows. We view an element a of $\prod_{i \in I} A_i$ as a function from I to the disjoint union of the A_i's, whose value at i is in A_i. If f is an n-ary function symbol, R is an n-ary function symbol, and $(a_1, \ldots, a_n) \in \prod_{i \in I} A_i$, then $f(a_1, \ldots, a_n)(i) = f(a_1(i), \ldots, a_n(i))$, and $\prod_{i \in I} A_i \models R(a_1, \ldots, a_n)$ iff $A_i \models R(a_1(i), \ldots, a_n(i))$ for every $i \in I$. Finally, the interpretation of a constant c is the function which to i associates the interpretation of c in A_i.

(5) Let $\mathcal{F}$ be a filter on I. We define an equivalence relation $\equiv_{\mathcal{F}}$ on $\prod_{i \in I} A_i$ by setting

$$a \equiv_{\mathcal{F}} b \iff \{i \in I \mid a(i) = b(i)\} \in \mathcal{F}.$$

---

[3] The theory ACF is axiomatised by adding to the theory of fields for every $n \geq 1$ the axiom expressing that every polynomial of degree exactly n has a solution: $\forall y_0, \ldots, y_{n-1} \ \exists x \ x^n + \sum_{i=0}^{n-1} y_i x^i = 0$.

The equivalence class of $a \in \prod_{i\in I} A_i$ will be denoted by $[a]_{\mathcal{F}}$, and the set of equivalence classes by $\prod_{i\in I} A_i/\mathcal{F}$. $\prod_{i\in I} A_i/\mathcal{F}$ has a natural $\mathcal{L}$-structure: the constant c is interpreted by $[c]_{\mathcal{F}}$; $f([a_1]_{\mathcal{F}}, \ldots, [a_n]_{\mathcal{F}}) = [f(a_1, \ldots, a_n)]_{\mathcal{F}}$, and $R([a_1]_{\mathcal{F}}, \ldots, [a_n]_{\mathcal{F}})$ holds iff $\{i \in I \mid A_i \models R(a_1(i), \ldots, a_n(i))\} \in \mathcal{F}$. The structure $\prod_{i\in I} A_i/\mathcal{F}$ is called the *reduced product of the structures A_i with respect to $\mathcal{F}$*. If $\mathcal{F}$ is an ultrafilter, then $\prod_{i\in I} A_i/\mathcal{F}$ is called the *ultraproduct* of the A_i with respect to $\mathcal{F}$. If all A_i are equal to the same structure A, then we talk of *reduced power* and of *ultrapower* of A.

(6) Observe that the natural map $\prod_{i\in I} A_i \to \prod_{i\in I} A_i/\mathcal{F}$ is a homomorphism of $\mathcal{L}$-structures.

(2.4) Examples. If I is finite, then all ultrafilters on I are principal. Note that if $\mathcal{F}$ is principal, say $\{j\} \in I$, then the ultraproduct $\prod_{i\in I} A_i/\mathcal{F}$ is naturally isomorphic to A_j.

The best known non-principal filter (on an infinite set I) is called the *Fréchet filter* and is the set of all subsets X of I such that $I \setminus X$ is finite. It is contained in all non-principal ultrafilters on I (Exercise).

Observe that if $A \subseteq I$ is infinite, then it intersects every cofinite subset of I; hence A and the Fréchet filter generate a (proper) filter, and A belongs to a non-principal ultrafilter.

(2.5) Łos' Theorem. Let I be infinite, $\mathcal{F}$ a filter on I, $(A_i)_{i\in I}$ a family of $\mathcal{L}$-structures, and $A = \prod_{i\in I} A_i/\mathcal{F}$.

(1) Let $\varphi(x)$ be a positive $\mathcal{L}$-formula, a a tuple in $\prod_{i\in I} A_i$. Then

$$A \models \varphi([a]_{\mathcal{F}}) \iff \{i \in I \mid A_i \models \varphi(a(i))\} \in \mathcal{F}.$$

(2) Assume in addition that $\mathcal{F}$ is an ultrafilter, and let $\varphi(x)$ be any formula, a a tuple in $\prod_{i\in I} A_i$. Then

$$A \models \varphi([a]_{\mathcal{F}}) \iff \{i \in I \mid A_i \models \varphi(a(i))\} \in \mathcal{F}.$$

This result is not difficult to prove, using induction on the complexity of the formulas. Note the restriction in (1) of $\varphi(x)$ being positive: the result definitely doesn't hold for formulas involving a negation, as can be shown by the following easy example. Let $a, b \in \prod_i A_i$. Then $[a]_{\mathcal{F}} = [b]_{\mathcal{F}} \iff \{i \in I \mid a(i) = b(i)\} \in \mathcal{F}$. But if $\mathcal{F}$ is not an ultrafilter, choose $A \subset I$ such that A and $I \setminus A$ are not in $\mathcal{F}$; then (assuming $|A_i| \geq 2$ for all i, choose b such that $\{i \in I \mid a(i) = b(i)\} = A$. Clearly $[a]_{\mathcal{F}} \neq [b]_{\mathcal{F}}$ but $\{i \in I \mid a(i) \neq b(i)\} \notin \mathcal{F}$.

(2.6) One immediate consequence of Łos' theorem is that if $\mathcal{F}$ is an ultrafilter on I, then the $\mathcal{L}$-structure A embeds elementarily into its ultrapower $A^I/\mathcal{F}$, via the map which to an element a associates $[\hat{a}]_{\mathcal{F}}$, where $\hat{a}$ is the function taking the value a on I.

(2.7) Theorem (Keisler-Shelah). Two $\mathcal{L}$-structures A and B are elementarily equivalent if and only if they have isomorphic ultrapowers.

(2.8) *Second proof of Ax's result (2.2).* Let $\mathcal{U}$ be a non-principal ultrafilter on the set of all primes p, and consider $K = \prod_p \mathbb{F}_p^{alg}/\mathcal{U}$. Then this is an algebraically closed field of characteristic 0, of size $2^{\aleph_0}$, and therefore is isomorphic to $\mathbb{C}$. By Łos's theorem, since every $\mathbb{F}_p^{alg}$ satisfies the sentence $\forall \bar{x}\ \varphi(\bar{x}) \to \psi(\bar{x})$, so does $\mathbb{C}$.

3. Axiomatisation of a candidate for the theory of finite fields

In this section, we will give an axiomatisation of a theory, which we will call T_f^*, and verify that finite fields are models of T_f^*. We will also study its infinite models. In the next section, we will show that this theory is the *theory T_f of all finite fields*, i.e., is the set of sentences which are true in all finite fields.

(3.1) The theory T_f^* will be obtained by adding to the theory of fields the following axiom schemes:

– Axiom 1 saying that the fields are perfect,

– Axiom 2(ℓ) saying that the field has exactly one algebraic extension of degree ℓ, for every $\ell > 1$,

– Axiom 3(m, n, d) a scheme of axioms expressing that the field is pseudo-algebraically closed (abbreviated by PAC), see definition below (3.8) (for every $m, n, d \in \mathbb{N}$).

(3.2) Axiom 1. This one is easy: for each prime p, add the axiom

$$p = 0 \to \forall y \exists x \; y = x^p.$$

(3.3) First half of Axiom 2(ℓ). Fix ℓ, we will first define a formula $\mathrm{Irr}_\ell(\bar{y})$, where $\bar{y} = (y_0, \ldots, y_{\ell-1})$, which says that the polynomial $P_\ell(\bar{y})(X) := X^\ell + y_{\ell-1}X^{\ell-1} + y_{\ell-2}X^{\ell-2} + \cdots + y_0$ is irreducible, i.e., is not the product of two polynomials of lower (non-zero) degree. The formula $\mathrm{Irr}_\ell(\bar{y})$ expresses that $\forall z_0, \ldots, z_{\ell-1}$, for all $1 \leq d < \ell$ the polynomials $X^\ell + y_{\ell-1}X^{\ell-1} + y_{\ell-2}X^{\ell-2} + \cdots + y_0$ and $(X^d + z_{d-1}X^{d-1} + \cdots + z_0)(X^{\ell-d} + z_{\ell-1}X^{\ell-d-1} + z_{\ell-2}X^{\ell-d-2} + \cdots + z_d)$ are not equal.

I.e., $\mathrm{Irr}_\ell(\bar{y})$ is the disjunction over $j = 0, \ldots, \ell - 1$, of the formulas

$$y_j \neq \sum_{i=0}^{d-1} z_i z'_{j-i}$$

where $z'_m = z_{\ell-d+m}$ if $0 \leq m < \ell - d$, $z'_m = 1$ if $m = \ell - d$, and $z'_m = 0$ otherwise.

So the first half of axiom 2(ℓ) will say $\exists \bar{y}\ \mathrm{Irr}_\ell(\bar{y})$. A field F which satisfies this axiom will therefore have an algebraic extension of degree ℓ.

(3.4) Second half of Axiom 2(ℓ). To finish this axiomatisation, we need to say that this extension is unique. Equivalently, that if $P(X)$ and $Q(X)$ are irreducible polynomials of degree ℓ, then the extension of F generated by a root of $P(X)$ contains a root of $Q(X)$.

In order to do that, we first need to show that we can interpret, uniformly in the ℓ-tuple $\bar{y}$ (which satisfies Irr_ℓ in the field F) the extension generated over F by a root of the polynomial $P_\ell(\bar{y})(X)$.

(3.5) Interpretation of a finite algebraic extension of a field inside the field. Let $\bar{a} = (a_0, \ldots, a_{\ell-1})$ be an ℓ-tuple satisfying Irr_ℓ in the field F. Let α be a root of $P_\ell(\bar{a})(X)$, and recall that

$$F(\alpha) \simeq_F F[X]/(P_\ell(\bar{a})(X)).$$

In particular $F(\alpha)$ is an F-vector space of dimension ℓ, with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\}$. This remark allows us to interpret easily, inside F and uniformly in the ℓ-tuple $\bar{a}$, the

structure $(F(\alpha), +, \times, 0, 1, P_F)$, where $+, \times, 0, 1$ are the usual addition, multiplication and constants on the field $F(\alpha)$, and P_F is a unary predicate for the subfield F.

We let $S = F^\ell$ (the direct sum of ℓ copies of F), $+^*$ the usual addition on the vector space S, and $0^* = (0, 0, \ldots, 0)$, $1^* = (1, 0, \ldots, 0)$, P_F^* the set of elements $\{(b, 0, \ldots, 0) \mid b \in F\}$. Clearly these sets, elements and relations are definable in F, with no parameters.

Multiplication by α induces a linear transformation of the vector space $F(\alpha)$, and its matrix is

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{\ell-1} \end{pmatrix}$$

since $\alpha^\ell = -\sum_{i=0}^{\ell-1} a_i \alpha^i$. Note that multiplication by α^i is also a linear transformation, and its matrix is simply M_α^i. So, we define $\times^*$ as follows

$$(x_1, \ldots, x_\ell) \times^* (y_1, \ldots, y_\ell) = (x_1 I_\ell + x_2 M_\alpha + \cdots x_\ell M_\alpha^{\ell-1}) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_\ell \end{pmatrix}.$$

Here I_ℓ denotes the identity $(\ell \times \ell)$-matrix. Observe that the definition of $\times^*$ uses the tuple $(a_0, \ldots, a_{\ell-1})$, but is totally uniform.

Hence, there is a formula $\theta^*(\bar{x}, \bar{y})$ of the language of fields, such that if $\mathrm{Irr}_\ell(\bar{a})$ and $\mathrm{Irr}_\ell(\bar{b})$ hold for some ℓ-tuples $\bar{a}$ and $\bar{b}$ in F and α is a root of $P_\ell(\bar{a})(X)$, then $F \models \theta^*(\bar{a}, \bar{b})$ if and only if $F(\alpha) \models \exists z\ P_\ell(\bar{b})(z) = 0$.

So, axiom 2 (ℓ) is:

$$\exists \bar{x}\ \mathrm{Irr}_\ell(\bar{x}) \wedge \forall \bar{y}\, [\mathrm{Irr}_\ell(\bar{y}) \to \theta^*(\bar{x}, \bar{y})].$$

(3.6) A comment on this condition. The condition of having at most one extension of each degree is equivalent to the following: whenever L is an algebraic extension of F of degree n, then $\mathrm{Aut}(L/F) \simeq \mathbb{Z}/n\mathbb{Z}$. In particular, $\mathrm{Aut}(L/F)$ is abelian and cyclic. For a proof, see e.g. (3.6) in the Madrid notes. You may also want to read some very basic facts on Galois theory which appear in that section.

(3.7) Algebraic sets, varieties .... Let F be a perfect field, Ω a large algebraically closed field containing it, and F^{alg} the algebraic closure of F (inside Ω). Given an n-tuple $\bar{a}$ in Ω, we look at

$$I(\bar{a}/F) = \{f(\bar{X}) \in F[\bar{X}] \mid f(\bar{a}) = 0\}.$$

We then have the following result:

$$I(\bar{a}/F)\Omega[\bar{X}] \text{is prime} \iff F(\bar{a}) \cap F^{alg} = F.$$

Here $\bar{X} = (X_1, \ldots, X_n)$, $I(\bar{a}/F)\Omega[\bar{X}]$ denotes the ideal generated by $I(\bar{a}/F)$ inside $\Omega[\bar{X}]$. If $I(\bar{a}/F)$ satisfies one of these equivalent conditions, then we say it is *absolutely prime*.

This terminology also applies to any prime ideal of $F[\bar{X}]$ which generates a prime ideal in $\Omega[\bar{X}]$.

An algebraic subset of Ω^n is the set of solutions of some (finite) set of polynomial equations with coefficients in Ω. The algebraic sets are the closed subsets of a topology on Ω^n, the *Zariski topology*. This topology is Noetherian, and therefore every closed set is the union of finitely many *irreducible closed subsets*[4]. Thus to an algebraic set S we can associate $I(S)$, the set of polynomials in $\Omega[\bar{X}]$ which vanish at all points of S. The set S is a *variety* iff the ideal $I(S)$ is prime, iff it is closed irreducible. It will be *defined over* F if $I(S)$ is generated by its intersection with $F[\bar{X}]$. A point of S is *F-rational* if all its coordinates are in F, and the set of F-rational points is denoted $S(F)$.

(3.8) Pseudo-algebraically closed fields. A field F is *pseudo-algebraically closed* (abbreviated by *PAC*) if every variety V defined over F has an F-rational point.

Before showing that being PAC is an elementary property, we will show an easy property of PAC fields:

(3.9) Lemma. Let F be a perfect PAC field, L a field containing F, and assume that $L \cap F^{alg} = F$. Then F is *existentially closed in* L, denoted $F \prec_1 L$, i.e.: every existential formula with parameters in F which is true in L is true in F.

Proof. An existential formula of $\mathcal{L}(F)$ is of the form $\exists\ \bar{y}\varphi(\bar{y})$, where $\varphi(\bar{y})$ is a boolean combination of polynomial equations with coefficients in F. Hence a disjunct of conjuncts of polynomial equations and inequations (over F), and we may therefore assume it is a conjunction of equations and inequations[5]. Using the fact that modulo the theory of fields, the formula $x \neq 0$, is equivalent to $\exists y\ xy = 1$, we may assume that $\varphi(\bar{y})$ is a conjunction of polynomial equations with coefficients in F.

Let $\bar{a} \in L$ be a solution of $\varphi(\bar{y})$. Since $L \cap F^{alg} = F$, we know that the ideal $I(\bar{a}/F) = \{f(\bar{X}) \in F[\bar{X}] \mid f(\bar{a}) = 0\}$ is an absolutely prime ideal, see (3.7). I.e., the set V of tuples on which all elements of $I(\bar{a}/F)$ vanish is a variety, which is defined over F. Since F is PAC, it follows that there is some tuple $\bar{b}$ on which all polynomials of $I(\bar{a}/F)$ vanish. Hence, $\bar{b}$ satisfies every polynomial equation over F that $\bar{a}$ satisfies, and in particular, will satisfy φ.

(3.10) Comments. The condition $L \cap F^{alg} = F$ is clearly necessary: if $\alpha \in L \cap F^{alg}$ and $\alpha \notin F$, and if $p(X)$ is the minimal polynomial of α over F, then $L \models \exists y\, p(y) = 0$, but $F \models \forall y\ p(y) \neq 0$.

It is in general not a sufficient condition. E.g., we will see that one can find a pseudo-finite field F such that $F \cap \mathbb{F}_p^{alg} = \mathbb{F}_p$, and clearly $\mathbb{F}_p \not\prec_1 F$.

(3.11) Theorem. There is a theory (in the language of rings) whose models are exactly the PAC fields.

Proof. Fix integers m, n, d. We need to express the following:

---

[4] A closed set U is irreducible if whenever $U = U_1 \cup U_2$ with U_1, U_2 closed, then $U_1 = U$ or $U_2 = U$

[5] Use that each of $\exists \bar{y}\ \varphi_i(\bar{y})$, $i = 1, 2$, implies $\exists \bar{y}\ (\varphi_1 \vee \varphi_2)(\bar{y})$ to get rid of the disjunctions.

Let $f_1(\bar{X}), \ldots, f_m(\bar{X})$ be polynomials in $\bar{X} = (X_1, \ldots, X_n)$ of degree $\leq d$, and assume they generate an absolutely prime ideal. Then they have a common zero.

This follows from results of Hermann, see below (3.14). If d is an integer, then we denote by $F[\bar{X}]_{\leq d}$ the set of polynomials of degree $\leq d$. They form a finite dimensional F-vector space, and are therefore definable in F. The following maps are also definable:
Addition: $F[\bar{X}]_{\leq d} \times F[\bar{X}]_{\leq d} \to F[\bar{X}]_{\leq d}$,
Multiplication: $F[\bar{X}]_{\leq d} \times F[\bar{X}]_{\leq d} \to F[\bar{X}]_{\leq 2d}$.

(3.12) Results of Hermann. (For a proof, see [He] or [S].)

(1) There is a constant $A = A(n,d)$ such that for every field F, polynomials $f_1, \ldots, f_m, g \in F[\bar{X}]_{\leq d}$, if g belongs to the ideal of $F[\bar{X}]$ generated by $f_1, \ldots, f_m$, then there are $h_1, \ldots, h_m \in F[\bar{X}]_{\leq A}$ such that $g = \sum_{i=1}^m f_i h_i$.

(2) There is a constant $B = B(n,d)$ such that for every field F, for every ideal I of $F[X]$ generated by elements of $F[X]_{\leq d}$ and for every $g \in F[X]_{\leq d}$, if $g^k \in I$ for some integer k, then $g^B \in I$.

(3) There is a constant $C = C(n,d)$ such that for every field F, ideals I and J generated by elements of $F[X]_{\leq d}$, the ideals $I \cap J$ and $J : I = \{f \in F[X] \mid fI \subseteq J\}$ are generated by elements of $F[X]_{\leq C}$.

(4) There is a constant $D = D(n,d)$ such that for every field F and ideal I of $F[X]$ generated by elements of $F[X]_{\leq d}$, if I is not prime, then there are $g, h \in F[X]_{\leq D}$ such that $gh \in I$ but $g, h \notin I$.

(5) There is a constant $E = E(n,d)$ such that for every field F and ideal I of $F[X]$ generated by elements of $F[X]_{\leq d}$, there are at most E minimal prime ideals containing I, and they are generated by elements of $F[X]_{\leq E}$.

(3.13) Corollary. Let $n, d \geq 1$. There is a formula $\varphi(\bar{y})$, $\bar{y}$ an $mN(d)$-tuple of variables, such that in every field F, for every $mN(d)$-tuple $\bar{a}$ in F, if $f_1, \ldots, f_m$ is the m-tuple of elements of $F[\bar{X}]_{\leq d}$ encoded by $\bar{a}$, then

$$F \models \varphi(\bar{a}) \iff \text{the ideal of } F[\bar{X}] \text{ generated by } f_1, \ldots, f_m \text{ is prime.}$$

Proof. Let $D = D(n,d)$, $A = A(n,D)$. Then

$f_1, \ldots, f_m$ generate a prime ideal I in $F[\bar{X}]$

if and only if for all $g, h \in F[\bar{X}]_{\leq D}$, either $gh \notin I$ or one of g, h is in I,

if and only if for all $g, h \in F[\bar{X}]_{\leq D}$, either for all $h_1, \ldots, h_m \in F[\bar{X}]_{\leq A}$, $gh \neq \sum_{i=1}^m h_i f_i$, or there are $h_1, \ldots, h_m \in F[\bar{X}]_{\leq A}$ such that $[g = \sum_{i=1}^m h_i f_i$ or $h = \sum_{i=1}^m h_i f_i]$.

This last statement is clearly an elementary property of the $mN(d)$-tuple $\bar{a}$ of coefficients of $f_1, \ldots, f_m$.

(3.14) Corollary. Let $n, d \geq 1$. There is a **quantifier-free** formula $\psi(\bar{y})$, $\bar{y}$ an $mN(d)$-tuple of variables such that in every field F, for every $mN(d)$-tuple $\bar{a}$ in F, if $f_1, \ldots, f_m$ is the m-tuple of elements of $F[\bar{X}]_{\leq d}$ encoded by $\bar{a}$, then

$$F \models \psi(\bar{a}) \iff \text{the ideal of } F^{alg}[X] \text{ generated by } f_1, \ldots, f_m \text{ is prime.}$$

Proof. Take the formula $\varphi(\bar{y})$ given by (3.13). By quantifier-elimination of the theory of algebraically closed fields[6], there is a quantifier-free formula $\psi(\bar{y})$ such that in every algebraically closed field K, for every $mN(d)$-tuple $\bar{a}$ in K we have

$$K \models \varphi(\bar{a}) \iff K \models \psi(\bar{a}).$$

But if the tuple $\bar{a}$ is in the subfield F of K, we have

$$K \models \psi(\bar{a}) \iff F \models \psi(\bar{a}).$$

Thus $F \models \psi(\bar{a})$ if and only if the m-tuple $(f_1, \ldots, f_m)$ of $F[\bar{X}]_{\leq d}$ encoded by $\bar{a}$ generates a prime ideal in $F^{alg}[\bar{X}]$.

(3.15) The theorem of Lang-Weil ([LW]). For every positive integers n, d, there is positive constant C $(= C(n,d))$ such that for every finite field $\mathbb{F}_q$ and variety V defined by polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]_{\leq d}$,

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

[Recall that $V(\mathbb{F}_q)$ is the set of points of $V \cap \mathbb{F}_q^n$, and $\dim(V)$ is the dimension of V, i.e., $tr.deg(\mathbb{F}_q(V)/\mathbb{F}_q)$.]

In particular, if $q > C^2$, then any variety V as above will have a rational point in $\mathbb{F}_q$. Indeed, we get

$$0 < -Cq^{\dim(V) - 1/2} + q^{\dim(V)} \leq |V(\mathbb{F}_q)|.$$

The constant C can be effectively computed.

(3.16) Axiom 3(m,n,d). So the third axiom will simply say: whenever $f_1(\bar{X}), \ldots, f_m(\bar{X})$ are polynomials in $\bar{X} = (X_1, \ldots, X_n)$ of degree $\leq d$ and which generate an absolutly prime ideal, then there is an n-tuple $\bar{a}$ such that $\bigwedge_i f_i(\bar{a}) = 0$, **unless** the field has less than $C(n,d)$ elements.

(3.17) Definition A field F is *pseudo-finite* iff it satisfies the axioms 1, 2(ℓ) and if it is PAC. In other words, if it is an infinite model of the theory T_f^*.

Theorem.

(1) Finite fields are models of the axioms 1, 2(ℓ) and 3(m,n,d). In other words they are models of the theory T_f^* introduced in (3.1).
(2) Let $\mathcal{Q}$ be the set of all prime powers, and let $\mathcal{U}$ be a non-principal ultrafilter on $\mathcal{Q}$. Then the field $F^* = \prod_{q \in \mathcal{Q}} \mathbb{F}_q / \mathcal{U}$ is a pseudo-finite field.

Proof. Clearly any infinite model of the scheme of axioms 3(m,n,d) is pseudo-algebraically closed, so it suffices to show the first assertion. The result of Lang-Weil (3.15) gives scheme of axioms 3(m,n,d). We also know that finite fields are perfect, and that they have exactly one algebraic extension of each degree.

---

[6] Modulo the theory ACF, every formula is equivalent to a quantifier-free formula.

4. Showing that $T_f^* \vdash T_f$.

So, we have shown that the theory T_f^* is satisfied by every finite field, and therefore is contained in the theory T_f of all finite fields. In order to show that T_f^* axiomatises the theory of all finite fields, we need to show the converse. I.e., that if a sentence θ is true in all finite fields, then it is true in all models of T_f^*. Since such a sentence is obviously true in all finite models of T_f^*, it remains to show that it is true in all pseudo-finite fields. In other words, we need to show that the pseudo-finite fields are exactly the infinite models of the theory T_f.

To do that, it is enough to show that if F is a pseudo-finite field, then F is elementarily equivalent to an ultraproduct of finite fields. Indeed, this will imply that a formula which is true in all finite fields is also true in this arbitrary infinite model of T_f^* (by Łos' theorem), and therefore that $T_f = T_f^*$ (or rather, $T_f^* \vdash T_f$).

The strategy to do that, is to describe the completions of the theory T_f^*, or rather, of the theory Psf of pseudo-finite fields, obtained by adding to T_f^* axioms saying that there are infinitely many elements.

Once we have described the completions of Psf, we will relatively easily obtain the result, as well as some "quantifier-elimination" results.

The main tool in the description of the completions of Psf is the following

(4.1) The embedding Lemma. (Simplified version). Let K, E, K^* be perfect fields, contained in some large algebraically closed field Ω, and such that

(1) $K \subset E, K^*$,
(2) $K^{alg} \cap K^* = K^{alg} \cap E = K$,
(3) K^* is pseudo-finite and $\aleph_1$-saturated,[7]
(4) E is countable, has at most one extension of each degree.

Then there is a field embedding $\varphi : E^{alg} \to K^{*alg}$ such that $\varphi|_K = id$ and $\varphi(E) \subseteq K^*$. Thus in particular, $\varphi(E)^{alg} \cap K^* = \varphi(E)$.

I will not give a proof of this result, as it uses the Galois correspondence in an essential way. You can find a proof in (6.8) of the Madrid notes, or in the book of Fried and Jarden.

(4.2) Theorem. Let K and L be pseudo-finite fields, containing a common subfield k. Assume that

$$k^{alg} \cap K = k^{alg} \cap L = k.$$

Then $K \equiv_k L$ (i.e., K and L are elementarily equivalent in the language $\mathcal{L}(k)$ obtained by adding to the language of rings constant symbols for the elements of k).

Proof. If the result is false, then a formula showing it is false will only involve finitely many parameters from k. Hence, we may assume that k is countable. Passing to elementary extensions of K and L, we may also assume that K and L are $\aleph_1$-saturated: if $K \prec K^*$, $L \prec L^*$ and $K^* \equiv_k L^*$, then also $K \equiv_k L$.

---

[7] Recall that a model M is $\aleph_1$-saturated if for every countable subset A of M, and set $\Sigma(x)$ of formulas with parameters in A, if Σ is finitely consistent, then it has a realisation in M. Every model has an elementary extension which is $\aleph_1$-saturated.

We now consider the following family $\mathcal{I}$ of partial isomorphisms: $f : A \to B$, where $A \subset K$ and $B \subset L$, is in $\mathcal{I}$ if and only if it is a field isomorphism, A and B are countable, and $A^{alg} \cap K = A$, $B^{alg} \cap L = B$.

We will show that the family $\mathcal{I}$ has the *back-and-forth property*, i.e.:

– If $f \in \mathcal{I}$ and $a \in K$ there is $g \in \mathcal{I}$ extending f and with a in its domain,

– and if $b \in L$, there is $g \in \mathcal{I}$ extending f and with b in its image.

Suppose we have f and a as above. Let $E = A(a)^{alg} \cap K$. We first extend f to an automorphism $\tilde{f}$ of the big algebraically closed field Ω in which we are working, and let $E_0 = \tilde{f}(E)$. We wish to use the Embedding lemma (4.1). We already know that $E_0 \cap B^{alg} = B$, since we had $E \cap A^{alg} \subset K \cap A^{alg} = A$. Furthermore, as $E^{alg} \cap K = E$, and K has at most one algebraic extension of each degree, we know that E has at most one algebraic extension of each degree: indeed, if M is an algebraic extension of E of degree n, then MK is an algebraic extension of K of degree n also. This property is preserved by $\tilde{f}$, and we may therefore apply the Embedding lemma to B, E_0, L: there is $\psi : E_0 \to L$ which is the identity on B and such that $\psi(E_0)^{alg} \cap L = \psi(E_0)$. Then $g = \psi\tilde{f}|_E$ is our desired element of $\mathcal{I}$.

The other direction (back) follows by symmetry.

(4.3) Back and forth? This is just a saturated version of Ehrenfeuch-Fraïssé games. One shows by induction on the number of quantifiers, that if $f \in \mathcal{I}$, then f preserves all formulas with n quantifiers, i.e., if $\varphi(\bar{x})$ has n quantifiers, and $\bar{a}$ is in the domain of f, then $K \models \varphi(\bar{a})$ if and only if $L \models \varphi(f(\bar{a}))$.

(4.4) Definition. If K is a field and $k_0 \subseteq K$ the prime subfield of K (i.e., the field of fractions of the subring of K generated by 1; it equals $\mathbb{Q}$ or $\mathbb{F}_p$), then the *(field of) absolute numbers of* K is the field $k_0^{alg} \cap K$.

(4.5) Corollary. The completions of Psf are obtained by describing the isomorphism type of the field of absolute numbers of a model.

Proof. Clear from Theorem (4.2): if F_1 and F_2 are pseudo-finite and have isomorphic fields of absolute numbers k, then $F_1 \equiv F_2$.

(4.6) Corollary. If $F_1 \subseteq F_2$ are pseudo-finite fields then

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

Proof. This follows from Theorem (4.2), with $k = F_2$.

(4.7) Corollary (Kiefe). Modulo the theory Psf, any formula $\varphi(\bar{x})$ is equivalent to a Boolean combination of formulas of the form $\exists t\ f(\bar{x}, t) = 0$, where $f(\bar{X}, T) \in \mathbb{Z}[\bar{X}, T]$.

Proof. By compactness, it suffices to show that if F_1, F_2 are two pseudo-finite fields of the same characteristic, and $\bar{a}$, $\bar{b}$ are n-tuples in F_1, F_2 respectively, such that for every $f(\bar{X}, T) \in \mathbb{Z}[\bar{X}, T]$,

$$F_1 \models \exists t\ f(\bar{a}, t) = 0 \iff F_2 \models \exists t\ f(\bar{b}, t) = 0, \tag{1}$$

then for any formula $\varphi(\bar{x})$, we have

$$F_1 \models \varphi(\bar{a}) \iff F_2 \models \varphi(\bar{b}).$$

By Theorem (4.2), this last condition is equivalent to the existence of an isomorphism between the fields $A = k_0(\bar{a})^{alg} \cap F_1$ and $B = k_0(\bar{b})^{alg} \cap F_2$, where k_0 is the prime subfield of F_1 and F_2. We will show that (1) implies that such an isomorphism exists. First of all note that there is an isomorphism $\varphi : k_0(\bar{a}) \to k_0(\bar{b})$ which sends $\bar{a}$ to $\bar{b}$: this is because the tuples $\bar{a}$ and $\bar{b}$ satisfy the same polynomial equations over k_0. Extend φ to $\varphi : k_0(\bar{a})^{alg} \to k_0(\bar{b})^{alg}$. We need to show that such a φ can be chosen with $\varphi(A) = B$. Equivalently, we need to find $\sigma \in \mathrm{Aut}(k_0(\bar{b})^{alg})/k_0(\bar{b}))$ such that $\sigma(\varphi(A)) = B$. We know that for any $f(\bar{X}, T) \in \mathbb{Z}[\bar{X}, T]$, we have

$$\varphi(A) \models \exists t\ f(\bar{b}, t) = 0 \iff B \models \exists t\ f(\bar{b}, t) = 0.$$

The result will now follow from the following lemma:

(4.8) Lemma. Let B be a field, and B_1, B_2 two perfect subfields of B^{alg}. Assume that for every $f(T) \in B[T]$ we have

$$B_1 \models \exists t\ f(t) = 0 \iff B_2 \models \exists t f(t) = 0.$$

Then there is $\sigma \in \mathrm{Aut}(B^{alg}/B)$ such that $\sigma(B_1) = B_2$.

Proof. If the characteristic is $p > 0$ and $b \in B$, then there is a unique element of B^{alg} satisfying $X^p = b$, so we can assume that B is also perfect. As B^{alg} is the the union of finite normal extensions of B, we will show that for any finite normal[8] extension L of B, we have

$$B_1 \cap L \simeq_B B_2 \cap L.$$

For each finite normal extension L of B consider

$$\mathcal{S}_L = \{\sigma \in \mathrm{Aut}(B^{alg}/B) \mid \sigma(L \cap B_1) = L \cap B_2\}.$$

Claim. $\mathcal{S}_L$ is not empty.

Let $\alpha \in L$ be such that $L \cap B_1 = B(\alpha)$, and let $f(T)$ be its minimal polynomial[9]. Then $B_1 \models f(\alpha) = 0$, and so there is some $\beta \in B_2$ such that $f(\beta) = 0$. Let $\sigma \in \mathrm{Aut}(L/B)$ be such that $\sigma(\alpha) = \beta$. Then certainly $\sigma(B_1) \subseteq B_2$, and therefore $[B_1 : B] \leq [B_2 : B]$. The symmetric argument gives $[B_2 : B] \leq [B_1 : B]$, and this implies that the degrees are equal, and $\sigma(B_1) = B_2$. Lift σ to an element of $\mathrm{Aut}(B^{alg}/B)$.

Thus the family $\mathcal{S}_L$, L ranging over all finite normal extensions of B, has the finite intersection property: If L and M are finite normal extensions of B, then so is their field

[8] A normal extension of a field B is an extension L which is stable under all elements of $\mathrm{Aut}(B^{alg}/B)$. Equivalently, if $f(T)$ is an irreducible polynomial of $B[T]$, then either L contains all roots of $f(T)$, or it contains none.

[9] That such an element exists is because B is perfect

composite[10] LM ans we have $\mathcal{S}_{LM} \subseteq \mathcal{S}_L \cap \mathcal{S}_M$. By compactness of the profinite group $\mathrm{Aut}(B^{alg}/B)$, there is some σ in the intersection of all $\mathcal{S}_L$, and this σ satisfies $\sigma(B_1) = B_2$.

(4.9) Another way of stating Corollary (4.5) is to say that modulo Psf, every sentence is equivalent to a Boolean combination of sentences $\exists t\ f(t) = 0$, where $f(T) \in \mathbb{Z}[T]$.

What are the constraints on fields of absolute numbers of pseudo-finite fields? Actually, none, beside the fact that they must have at most one extension of each degree. [Recall that they must be relatively algebraically closed in a field having exactly one extension of each degree]. Hence $\mathbb{Q}^{alg}$ is allowable, as is any subfield of $\mathbb{F}_p^{alg}$.

To finish the proof that $T_f = T_f^*$, it therefore suffices to prove the following:

(4.10) Theorem. Let $k = \mathbb{F}_p$ or $k = \mathbb{Q}$, and let $E \subseteq k^{alg}$ have at most one extension of each degree. Then there is an ultraproduct K^* of finite fields such that the field of absolute numbers of K^* is isomorphic to E. When the characteristic of E is 0, K^* can be chosen to be an ultraproduct of prime fields.

Proof. We will start with the easy cases, when the characteristic of E is $p > 0$. The characteristic 0 case will need Chebotarev's theorem, see below (4.11)

Case 1. E is infinite (and of characteristic p).

Let n_m be a sequence of integers such that n_m divides n_{m+1}, and $E = \bigcup_m \mathbb{F}_{p^{n_m}}$. For instance, as $\mathbb{F}_p = \bigcup_m \mathbb{F}_{p^{m!}}$, we can define n_m by $\mathbb{F}_{p^{n_m}} = E \cap \mathbb{F}_{p^{m!}}$. Let $\mathcal{U}$ be any non-principal ultrafilter on $\mathbb{N}$ such that $\{n_m \mid m \in \mathbb{N}\} \in \mathcal{U}$, and let $K^* = \prod_m \mathbb{F}_{p^{n_m}}/\mathcal{U}$. Then $K^* \cap \mathbb{F}_p^{alg} \simeq E$.

Indeed, clearly K^* is of characteristic p. Let $d \in \mathbb{N}$. If $\mathbb{F}_p^d \subset E$, then $\mathbb{F}_{p^d}$ will be contained in all fields $\mathbb{F}_{p^{n_m}}$ with $m \geq d$. Hence, by Łos' theorem, K^* will satisfy the sentence "there is an element of multiplicative order exactly $p^d - 1$", and therefore will contain (a copy of) $\mathbb{F}_{p^d}$. On the other hand, if $\mathbb{F}_p^d \not\subset E$, then $\mathbb{F}_{p^d}$ is contained in no $\mathbb{F}_{p^{n_m}}$, therefore K^* will satisfy "there is no element of multiplicative order exactly $q^d - 1$", and K^* will not contain $\mathbb{F}_{q^d}$. Hence we will have $K^* \cap \mathbb{F}_p^{alg} = \mathbb{F}_q$.

Case 2. E is finite.

Let $q = |E|$, so that $E = \mathbb{F}_q$. Consider any non-trivial ultrafilter $\mathcal{U}$ on the set $\mathcal{P}$ of prime numbers, and let $K^* = \prod_{\ell \in \mathcal{P}} \mathbb{F}_q^\ell/\mathcal{U}$. Then K^* is of characteristic p and contains $\mathbb{F}_q$. But, if $d > 1$, all but at most one field $\mathbb{F}_{q^\ell}$ satisfy "there is no element of multiplicative order exactly $p^d - 1$", and therefore $K^* \cap \mathbb{F}_p^{alg} = \mathbb{F}_q$.

Case 3. E is of characteristic 0.

Write $\mathbb{Q}^{alg}$ as the union of an increasing chain L_n, $n \in \mathbb{N}$, of finite Galois extensions of $\mathbb{Q}$. For each n, let $E_n = L_n \cap F$, and let $I(n)$ be the (finite) set of subfields of L_n which properly contain E_n. We will find a sentence θ_n which describes $L_n \cap F$. Choose a generator α of E_n over $\mathbb{Q}$, and let $f_n(T)$ be its minimal polynomial over $\mathbb{Q}$. Similarly, for each $M \in I(n)$, choose a generator β_M of M over $\mathbb{Q}$, let $g_M(T)$ be the minimal polynomial of β_M over $\mathbb{Q}$, and define $g_n(T) = \prod_{M \in I(n)} g_M(T)$. Consider now the sentence $\theta_n : \exists t\ f_n(t) = 0 \wedge \forall t\ g_n(t) \neq 0$. This is a sentence satisfied by E, and if F is any field of characteristic 0, then $F \models \theta_n \iff F \cap L_n \simeq E_n$.

---

[10] the subfield of B^{alg} generated by L and M.

As the L_n's form an increasing chain, so do the E_n's, and we have $\theta_n \to \theta_{n-1}$. In order to find an ultraproduct of prime fields with field of absolute numbers isomorphic to F, it is therefore enough to show that for each n, the set

$$S_n := \{p \in \mathcal{P} \mid \mathbb{F}_p \models \theta_n\}$$

is infinite. As $S_n \supset S_{n+1}$, there will be a non-principal ultrafilter $\mathcal{U}$ containing all S_n's, and if $K^* = \prod_{p\in\mathcal{P}} \mathbb{F}_p/\mathcal{U}$, then $K^* \models \theta_n$ for each n, i.e.: $K^* \cap \mathbb{Q}^{alg} \simeq E$.

That S_n is infinite follows from Tchebotarev's theorem. Here is the consequence of Tchebotarev's theorem that we will use:

(4.11) Let $f_1(T), \ldots, f_m(T), g(T) \in \mathbb{Z}[T]$, T a single variable. Let L be the Galois extension of $\mathbb{Q}$ obtained by adjoining all roots of the polynomials $f_i(T)$, $i = 1, \ldots, m$. Assume that there is a subfield E of L such that $\mathrm{Aut}(L/E)$ is cyclic and

$$E \models \bigwedge_{i=1}^{m} \exists t\ f_i(t) = 0 \wedge \forall t\ g(t) \neq 0.$$

Then the set of prime numbers p such that $\mathbb{F}_p \models \bigwedge_{i=1}^{m} \exists t\ f_i(t) = 0 \wedge \forall t\ g(t) \neq 0$ is infinite.

(4.12) Decidability issues. Observe first that by Theorem (4.10) we have

$$\mathrm{Psf} \subset \mathrm{Psf}_0 \subset T_{\mathrm{prime}} \text{ and } \mathrm{Psf} \subset T_f \subset T_{\mathrm{prime}}.$$

(Here Psf_0 denotes the theory of pseudo-finite fields of characteristic 0 and T_{prime} the theory of all prime fields. We will first show that the theory Psf is decidable, that is, that there is an algorithm which decides, given a sentence θ, whether it is true in all pseudo-finite fields or not. From this we will be able to derive the decidability of the other theories.

We have an enumeration of a set Γ consisting of axioms for the theory Psf (this assumes that the bounds given in (3.12) on degrees of polynomials can be computed effectively, but they can). Hence, we can produce an enumeration of the set of all proofs made using axioms of Γ, and therefore of the theory Psf (by the completeness theorem, if a sentence is true in all pseudo-finite fields, then it is provable from Γ). Similarly, we have an enumeration of a set Γ_0 of axioms for the theory Psf_0 of all pseudo-finite fields of characteristic 0, and of the theory Psf_0. Note that $\Gamma_0 = \Gamma \cup \{p \neq 0 \mid p \text{ a prime}\}$.

This tells us that if θ is in Psf, then going through the enumeration of Psf we will find it. However, we need another procedure to decide if $\theta \notin \mathrm{Psf}$. This is what we will do below. Let us fix a sentence θ.

Let ψ_n, $n \in \mathbb{N}$, be an enumeration of all sentences which are Boolean combinations of sentences of the form $\exists t\ f(t) = 0$, where $f(T) \in \mathbb{Z}[T]$. By (4.9), we know that $\Gamma \vdash \theta \leftrightarrow \psi_n$ for some n, i.e., $\theta \leftrightarrow \psi_n \in \mathrm{Psf}$, and therefore we can effectively find this ψ_n. Note that the proof of $\theta \leftrightarrow \psi_n$ uses only a finite number of axioms expressing the PAC property, and we can therefore find a constant C_1 (given by Lang-Weil (3.15)) such that in all finite fields $\mathbb{F}_q$ with $q > C_1$ we have

$$\mathbb{F}_q \models \theta \leftrightarrow \psi_n.$$

It now remains to decide whether ψ_n is true in all pseudo-finite fields. I.e., we need to show that if k is a prime field, and $E \subseteq k^{alg}$ has at most one algebraic extension of each degree, then $E \models \psi_n$.

Step 1. Decide whether $\psi_n \in \mathrm{Psf}_0$ or not.

We know that ψ_n is (equivalent to) a disjunction of sentences of the form $\bigwedge_i \exists t\ f_i(t) = 0 \wedge \forall t\ g(t) \neq 0$. Let L be the extension of $\mathbb{Q}$ generated by all roots of all polynomials appearing in ψ_n. Then one can compute effectively $\mathrm{Aut}(L/\mathbb{Q})$, as well as those subfields E of L such that $\mathrm{Aut}(L/E)$ is cyclic. Hence we can decide whether or not ψ_n is true in all subfields E of L such that $\mathrm{Aut}(L/E)$ is cyclic. If it is not, then $\psi_n \notin \mathrm{Psf}_0$ and therefore $\psi_n \notin \mathrm{Psf}$, i.e., $\theta \notin \mathrm{Psf}_0$, $\theta \notin \mathrm{Psf}$.

Step 2. Decide whether $\psi_n \in \mathrm{Psf}$.

Assume that $\psi_n \in \mathrm{Psf}_0$. Then it is provable from Γ_0, and its proof only uses finitely many axioms expressing that the characteristic is $\neq p$; therefore there is a constant C_2 such that ψ_n holds in all pseudo-finite fields of characteristic $p > C_2$. It therefore remains to check whether ψ_n holds in all pseudo-finite fields of characteristic $p \leq C_2$. Fix one such p. Then, as in step 1 we let $\mathbb{F}_{p^m}$ be the extension of $\mathbb{F}_p$ generated by all roots of polynomials appearing in ψ_n. It then suffices to check whether $\mathbb{F}_{p^d} \models \psi_n$ or not for all d dividing m. This is certainly decidable, and finishes the proof that Psf is decidable.

Step 3. Decidability of T_f and of T_{prime}.

We assume now that all pseudo-finite fields satisfy θ. Hence there is a proof of θ from Γ, and this proof will involve only finitely many axioms saying that varieties have points. Hence, there is a constant C_3 such that $T_f \cup \{\text{there are at least } C_3 \text{ elements}\}$ proves θ. It now remains to check whether θ holds in the finitely many finite fields of size $< C_3$. But this is decidable.

Similarly, assume that all pseudo-finite fields of characteristic 0 satisfy θ. Then the proof of θ from Psf_0 uses only finitely many axioms saying that varieties have points and that "$p \neq 0$", and there is a constant C_4 such that $T_f \cup \{\text{"}p \neq 0\text{"},\ p < C_4\}$ proves θ. It now remains to check whether θ holds in the finitely many prime fields of size $< C_4$.

[So we didn't need C_1 after all].

5. More results on pseudo-finite fields

If M is a structure, and $\varphi(\bar{x})$ is a formula in the language of M, we denote by $\varphi(M)$ the set of tuples in M satisfying φ.

(5.1) Examples of pseudo-finite fields. If F is an infinite subfield of $\mathbb{F}_p^{alg}$, then F is PAC by the theorem of Lang-Weil (3.15), and is perfect. Hence, any infinite subfield F of $\mathbb{F}_p^{alg}$ pseudo-finite as soon as it satisfies axiom $2(\ell)$ for all ℓ. (By group theory results, it actually suffices to have it for all primes). Hence, if f is any function from the set of prime numbers to the positive integers, and F is the field composite of all $\mathbb{F}_{p^{f(\ell)}}$, ℓ a prime, then F is pseudo-finite.

This gives us many pseudo-finite fields of positive characteristic. In characteristic 0, there are no such explicit examples. However a result of Jarden (see [FJ] for a proof) shows that there are many such fields. The profinite group $\mathrm{Aut}(\mathbb{Q}^{alg}/\mathbb{Q})$ is compact, and has a unique Haar probability measure. In the sense of this measure, for almost all

$\sigma \in \mathrm{Aut}(\mathbb{Q}^{alg}/\mathbb{Q})$, the subfield of $\mathbb{Q}^{alg}$ fixed by σ is pseudo-finite. Other examples are of course non-principal ultraproducts of prime fields.

(5.2) Quantifier-elimination results for pseudo-finite fields. An easy consequence of Kiefe's result (4.7) is:

Theorem. Let $\mathcal{L}'$ be the language obtained by adding to the language of rings an $(n+1)$-ary predicate R_n for every $n > 1$, and add to the theory Psf the axioms

$$R_n(x_0, \ldots, x_n) \iff \exists y \sum_{i=0}^{n} x_i y^i = 0,$$

to obtain a theory Psf$'$. Then Psf$'$ eliminates quantifiers.

Proof. Let F_1 and F_2 be pseudo-finite fields, containing a common $\mathcal{L}'$-substructure A. Then A is a subring. We need to show that $F_1 \equiv_A F_2$. By Lemma (4.8) (or its proof), there is an isomorphism $f : A^{alg} \cap F_1 \to A^{alg} \cap F_2$ which is the identity on A. Now apply Theorem (4.2).

(5.3) A language in which Psf is model complete. We form the language $\mathcal{L}_c$ by adjoining to the language $\mathcal{L}$ of rings new constant symbols $c_{i,n}$, where $2 \leq n \in \mathbb{N}$ and $0 \leq i \leq n-1$. The theory Psf_c is obtained by adding to the theory Psf for each n an axiom stating that the polynomial $X^n + \sum_{i=0}^{n-1} c_{i,n} X^i$ is irreducible.

Note that every pseudo-finite field expands to a model of Psf_c: if F is pseudo-finite, for each n choose the $c_{i,n}$ to be the coefficients of some (monic) irreducible polynomial of degree n.

Recall that a theory T is *model complete* if whenever $M \subseteq N$ are models of T, then $M \prec N$. If T is model complete, then every formula is equivalent modulo T to an existential formula (and to a universal formula).

Theorem. The theory Psf_c is model complete.

Proof. Let $F_1 \subseteq F_2$ be models of Psf_c. If L is an algebraic extension of F_1 of degree n, then L is generated over F_1 by a solution of the equation $X^n + \sum_{i=0}^{n-1} c_{i,n} X^i$. Since $F_i \models \mathrm{Psf}_c$, this polynomial stays irreducible over F_2, i.e., $F_2 \cap L = F_1$. By (4.6), we obtain $F_1 \prec F_2$.

(5.4) Other quantifier-elimination results. Fried and Sacerdote introduce a more geometric language, in which one has quantifier elimination. They are using "Galois formulas", and the process is called "elimination through Galois stratification". The elimination procedure is primitive recursive. For details see [FHJ1] or [FJ]. One should note that this is the language that Denef and Loeser found more convenient to set up motivic integration in [DL].

(5.5) Results of Kiefe on Zeta and Poincaré series. Recall that if R is a ring, then $R[[t]]$, the *ring of formal power series over* R, is the set of formal sums $\sum_{i=0}^{\infty} a_i t^i$. Addition and multiplication are defined by

$$\sum a_i t^i + \sum b_j t^j = \sum (a_i + b_i) t^i, \qquad \sum_i a_i t^i \sum b_j t^j = \sum_n \Big(\sum_{i+j=n} a_i b_j \Big) t^n.$$

[Note that there are only finitely many non-negative integers such that $i+j=n$, so that $\sum_{i+j=n} a_i b_j$ is a finite sum and is well defined].

Let $\varphi(\bar{x})$ be an $\mathcal{L}$-formula, with parameters in $\mathbb{F}_q$, some $q=p^n$, p a prime. For each $s \geq 1$, we define

$$N_s(\varphi) = |\varphi(\mathbb{F}_{q^s})|.$$

We then define two formal series over $\mathbb{Q}$, the Poincaré series P and the Zeta series Z by

$$P(\varphi,t) = \sum_{s=1}^{\infty} N_s(\varphi) t^s, \qquad Z(\varphi,t) = \exp(\sum_{s=1}^{\infty} \frac{N_s(\varphi)}{s} t^s).$$

Theorem (Kiefe). $P(\varphi,t)$ is rational in t (i.e., is of the form $p(t)/q(t)$, with $p(t), q(t) \in \mathbb{Q}[t]$, and $q(0) \neq 0$), and $Z(\varphi,t) = \exp(f(t))(g(t)/h(t))^{1/\ell}$ for some integer ℓ and polynomials $f(t), g(t), h(t) \in \mathbb{Q}[t]$.

Note that we have the functional equation

$$P(\varphi,t) = t\frac{d}{dt}(\log(Z(\varphi,t))), \qquad Z(\theta,0) = 1.$$

Hence the first assertion will follow from the first. When φ is a quantifier-free formula, this is a result of Dwork. For a proof, see the book of Fried and Jarden [FJ], for instance. The proof given there uses Galois formulas.

6. Measure, definability, and other applications

(6.1) Counting points. We saw in Theorem (4.10) that every pseudo-finite field is elementarily equivalent to an ultraproduct of finite fields. This implies in fact that every pseudo-finite field elementarily embeds into an ultraproduct of finite fields (an ultrapower of ultraproducts is an ultraproduct). Now, every finite field can be equipped with a measure (the counting measure), and one would think that the ultraproduct of these measures might define something interesting on F. It turns out that this is the case, and we will see below how it works. The main tool is the following

Theorem ([CDM]). Let $\varphi(\bar{x},\bar{y})$ be a formula, $\bar{x}$ an n-tuple of variables ($\bar{y}$ an m-tuple of variables). Then there is a finite set $D \subset \{0,1,\ldots,n\} \times \mathbb{Q}^{>0} \cup \{(0,0)\}$ of pairs (d,μ), and a constant $C>0$, formulas $\varphi_{d,\mu}(\bar{y})$ for $(d,\mu) \in D$ such that:

(1) If $\mathbb{F}_q$ is a finite field and $\bar{a}$ an m-tuple in $\mathbb{F}_q$, then there is some $(d,\mu) \in D$ such that

$$\big||\varphi(\mathbb{F}_q,\bar{a})| - \mu q^d\big| < C q^{d-1/2}. \qquad (*)$$

[Here $\varphi(\mathbb{F}_q,\bar{a})$ denotes the set $\{\bar{b} \in \mathbb{F}_q^n \mid \mathbb{F}_q \models \varphi(\bar{b},\bar{a})\}$.]

(2) The formula $\varphi_{d,\mu}(\bar{y})$ defines in each $\mathbb{F}_q$ the set of tuples $\bar{a}$ such that $(*)$ holds.

I am not going to give a proof of this result, although I will later sketch a strategy for the proof. With some work one can show that the constant C can be found effectively, see [FHJ2], and also [FS], [FHJ1]. First a few remarks.

(6.2) Remarks.

(1) Observe that the pair $(0,0)$ has been put in D to take care of the case when $\varphi(\mathbb{F}_q, \bar{a})$ is empty.
(2) If $\varphi(\bar{x}, \bar{a})$ defines a variety V, then this is simply the Theorem of Lang-Weil, with $d = \dim(V)$ and $\mu = 1$.
(3) Thus, if $\varphi(\bar{x}, \bar{a})$ defines an algebraic set W, all of whose irreducible components are defined over $\mathbb{F}_q$, then d will be the maximal dimension of the irreducible components of W, and μ the number of these components of maximal dimension. Note that therefore, if $\varphi(\bar{x}, \bar{y})$ is quantifier-free, then the associated set of pairs will be contained in $\{0, \ldots, n\} \times \mathbb{N}^{>0} \cup \{(0,0)\}$.
(4) If q is sufficiently large, the formulas $\varphi_{d,\mu}(\bar{y})$ will define a partition of the parameter set $\mathbb{F}_q^m$.
(5) If $n = 1$, then there are positive numbers $A \in \mathbb{N}$ and $r \in \mathbb{Q}$ such that for every $\mathbb{F}_q$ and tuple $\bar{a}$ in $\mathbb{F}_q$,

$$\text{either } |\varphi(\mathbb{F}_q, \bar{a})| < A \text{ or } |\varphi(\mathbb{F}_q, \bar{a})| \geq rq.$$

Indeed, let D be the set of pairs (d, μ) associated to $\varphi(x, \bar{y})$; define $A_0 = \sup\{\mu \mid (0,\mu) \in D\}$, $r_0 = \inf\{\mu \mid (1,\mu) \in D\}$. Let $r = r_0/2$ and $A = \sup\{A_0 + C, 4C^2/r_0^2\}$. Using $(*)$, this gives the assertion.
(6) Observe that if q is sufficiently large, $(0,\mu) \in D$ and $\mathbb{F}_q \models \varphi_{0,\mu}(\bar{a})$, then, because $q^{-1/2}$ becomes very small, and in particular $< 1/2$, the number μ must give the exact size of the set $\varphi(\mathbb{F}_q, \bar{a})$ defined by $\varphi(\bar{x}, \bar{a})$.

(6.3) Some simple applications of this result.
(1) There is no formula of the language of rings which defines in each field $\mathbb{F}_q^2$ the subfield $\mathbb{F}_q$.
(2) We know that the multiplicative group of $\mathbb{F}_q$ is cyclic, of order $q-1$. There is no formula which defines in all fields $\mathbb{F}_q$ the set of generators of the multiplicative group $\mathbb{F}_q^\times$.
(3) Let G, H be groups definable in the pseudo-finite field F, and assume that $f : G \to H$ is definable, $\ker(f)$ is finite, and $\dim(G) = \dim(H) = d$. Then

$$\mu(G)[H : f(G)] = \mu(H)|\ker(f)|.$$

Proof. (1) If $\varphi(x)$ is a formula, there are $A > 0$ and $r \in \mathbb{Q}^{>0}$ such that for every finite field $\mathbb{F}_q$, the size of the set defined by φ is either $\leq A$ or greater than rq. hence, we cannot have a formula which defines in all $\mathbb{F}_{q^2}$ a set of size $q = \sqrt{q^2}$.

(2) The function ϕ (called the Euler function) giving the number of generating elements of a cyclic group can be computed. Note that if m, n are relatively prime integers then $\phi(nm) = \phi(n)\phi(m)$ (since $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$). Also, $\phi(p^n) = (p-1)p^{n-1}$, since any lifting of a generator of $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p^n/\mathbb{Z}$ is a generator of $\mathbb{Z}/p^n\mathbb{Z}$.

First observe that if $p^n > 2$, then $\phi(p^n) \geq \sqrt{n}$. Hence, for every $A \in \mathbb{N}$, the set of integers n such that $\phi(n) < A$ is finite.

We will now show that for every $\varepsilon > 0$, there is some prime power q such that $\phi(q-1) < \varepsilon(q-1)$. Observe that

$$\phi(n)/n = \prod_{\ell \text{ a prime divisor of } n} (1 - \frac{1}{\ell}).$$

Fix some prime p, and let $\ell_1, \ldots, \ell_m$ be distinct prime numbers, $M = \prod_{i=1}^m (\ell_i - 1)$. Then for every i, we have $p^M \equiv 1 \bmod(\ell_i)$ and therefore $\phi(p^M - 1) \leq (p^M - 1) \prod_{i=1}^m (1 - 1/\ell_i)$. Hence we can find arbitrarily small values of $\frac{\phi(p^M-1)}{p^M-1}$, which shows our assertion.

The existence of a formula defining the set of generators in all $\mathbb{F}_q$ would then, as in (1), contradict (6.2)(5).

(3) Let $F^* = \prod_{i \in I} \mathbb{F}_{q_i}/\mathcal{U}$ be an elementary extension of F, let a be a tuple of elements of F needed to define f, G and H (and their group law, and $(a(i))_i$ a sequence such that $[a(i)_i]_{\mathcal{U}} = a$.

Let $\varphi_1(\bar{x}, \bar{a})$ be the formula defining G, $\psi_1(\bar{x}, \bar{y}, \bar{z}, \bar{a})$ the one defining its group law, $\varphi_2(\bar{x}, \bar{a})$ the formula defining H, $\psi_2(\bar{x}, \bar{y}, \bar{z}, \bar{a})$ the one defining its group law, and $\theta(\bar{x}, \bar{y}, \bar{a})$ the formula defining the graph of f. The following property is then a first order property of the parameter $\bar{a}$:

$\psi_i(\bar{x}, \bar{y}, \bar{z}, \bar{a})$ is the graph of a group operation on the set defined by $\varphi_i(\bar{x}, \bar{a})$ $(i = 1, 2)$, and $\theta(\bar{x}, \bar{y}, \bar{a})$ is the graph of a group morphism between the set defined by $\varphi_1(\bar{x}, \bar{a})$ and the set defined by $\varphi_2(\bar{x}, \bar{a})$, whose kernel is of size m.

Hence, by Łos' theorem, for a set $J \in \mathcal{U}$, we have, for all $j \in J$, that the following statement holds in $\mathbb{F}_{q_j}$:
$\psi_1(\bar{x}, \bar{y}, \bar{z}, \bar{a}(j))$ is the graph of a group operation on the set G_j defined by $\varphi_1(\bar{x}, \bar{a}(j))$, $\psi_2(\bar{x}, \bar{y}, \bar{z}, \bar{a}(j))$ is the graph of a group operation on the set H_j defined by $\varphi_2(\bar{x}, \bar{a}(j))$, and $\theta(\bar{x}, \bar{y}, \bar{a}(j))$ is the graph of a group morphism $f_j : G_j \to H_j$, whose kernel is of size m.

But G_j and H_j are finite!! Hence we have $|G_j|[H_j : f_j(G_j)] = |H_j| |\ker(f_j)|$. For q_j sufficiently large, dividing by q_j^d, we get $\mu(G_j)[H_j : f_j(G_j)] = \mu(H_j) |\ker(f)|$.

There is a first-order formula which expresses that fact, is satisfied in all $\mathbb{F}_{q_j}$ for $j \in J$, and therefore is satisfied by $\bar{a}$ in F^*, whence also in F. This gives the result.

(6.4) Very rough sketch of the proof of Theorem (6.1). The result is proved by induction on the complexity of formulas.

Let us first assume that $\varphi(\bar{x}, \bar{y})$ is positive quantifier-free, that is, it is a disjunction of conjunction of equations (over $\mathbb{Z}$).

Let $\mathbb{F}_q$ be a finite field, and $\bar{a}$ a tuple in $\mathbb{F}_q$. Consider the set S defined by $\varphi(\bar{x}, \bar{a})$. Then $S = W(\mathbb{F}_q)$, where W is the algebraic set given by the equations of $\varphi(\bar{x}, \bar{a})$. However, we do not know that the Theorem of Lang-Weil can tell us the estimate of how many points there are: we will be able to apply this theorem only if *all irreducible components of W are defined over $\mathbb{F}_q$*. In order to be able to use Lang-Weil, we must therefore find an algebraic set W' such that $W'(\mathbb{F}_q) = W(\mathbb{F}_q)$ and all irreducible components of W' are defined over $\mathbb{F}_q$. This is done in the following fashion:

Write $W = W_1 \cup \cdots \cup W_m$ where each W_i is irreducible over $\mathbb{F}_q$. If W_i is a variety, then we know by Lang-Weil (3.15) that $|W(\mathbb{F}_q)| \sim q^{\dim(W_i)}$ and we do nothing. If W_i is not a variety, then W_i has several irreducible components, and any point in $W_i(\mathbb{F}_q)$ will belong to the intersection W_i' of all these components, and we replace W_i by W_i'. We repeat the procedure and find eventually an algebraic set W', all of whose irreducible components are defined over $\mathbb{F}_q$ and such that $W'(\mathbb{F}_q) = W(\mathbb{F}_q)$. This procedure is effective, and using the results on bounds in polynomial rings, and we can write $W' = W_1' \cup \cdots \cup W_\ell'$, where the W_i' are varieties defined over $\mathbb{F}_q$. If d is the maximum of the dimensions of the W_i', and μ is the number of components of W' of dimension d, the result of Lang-Weil will then give us

that $|W(\mathbb{F}_q)| \sim \mu q^d$. One also knows that having dimension d is an elementary property of the coefficients of a set of polynomials defining a variety. Thus, there is a formula $\varphi_{\bar{a}}(\bar{y})$ satisfied by $\bar{a}$ in $\mathbb{F}_q$ and which expresses how we obtained W' from W, and that W' has exactly μ components of maximal dimension d. For each pair $(\mathbb{F}_q, \bar{a})$ we can find such a formula. By compactness, there are a finite number of those, say $\varphi_1(\bar{y}), \ldots, \varphi_k(\bar{y})$ such that in any finite field $\mathbb{F}$, we have $\mathbb{F} \models \forall \bar{y}\ (\exists \bar{x} \varphi(\bar{x}, \bar{y})) \leftrightarrow (\bigvee_j \varphi_j(\bar{y}))$. To each formula $\varphi_j(\bar{y})$ is associated a pair (d, μ), and we put them together to obtain the desired $\varphi_{d,\mu}$.

The case of a quantifier-free formula $\varphi(\bar{x}, \bar{y})$ follows, observing that modulo the theory of fields, an inequation $z \neq 0$ is equivalent to $\exists y\ yz = 1$. Thus, every quantifier-free definable set is in bijection, via a projection, with an algebraic set. We then use the first case.

Let us now assume that $\varphi(\bar{x}, \bar{y})$ is arbitrary. Then, Theorem (5.3) tells us, using compactness, that there are positive quantifier-free $\mathcal{L}_c$-formulas $\psi_1(\bar{x}, \bar{y}, \bar{z}), \ldots, \psi_m(\bar{x}, \bar{y}, \bar{z})$ such that

$$\mathrm{Psf} \vdash \forall \bar{x}, \bar{y}\ (\varphi(\bar{x}, \bar{y}) \leftrightarrow \exists \bar{z} \bigvee_j \psi_j(\bar{x}, \bar{y}, \bar{z})),$$

and furthermore such that for some integer N, in any field F one has

$$F \models \forall \bar{x}, \bar{y}\ (\exists \bar{z}\ \psi_j(\bar{x}, \bar{y}, \bar{z}) \rightarrow \exists^{\leq N} \bar{z}\ \psi_j(\bar{x}, \bar{y}, \bar{z})).$$

The same equivalence holds in sufficiently large finite fields, say of size $\geq C'$ for some C' (only depending on $\varphi(\bar{x}, \bar{y})$). Given some sufficiently large finite field $\mathbb{F}$ and tuple $\bar{a}$ in $\mathbb{F}$, we know by the previous steps how to estimate the size of the sets defined by the formulas $\psi_i(\bar{x}, \bar{a}, \bar{z})$. The problem is that the set defined by $\bigvee_j \psi_j(\bar{x}, \bar{a}, \bar{z})$ is not in bijection with the set defined by $\varphi(\bar{x}, \bar{a})$: given some $\bar{x}$ in that set, there may be several $\bar{z}$ such that $\psi_j(\bar{x}, \bar{a}, \bar{z})$ holds. One uses a trick to transform the algebraic sets defined by the ψ_j, in such a way that we are able to count how many $\bar{z}$ are sitting above an $\bar{x}$. Then we use some counting arguments and induction to conclude. The constant C of the Theorem will be sufficiently large so that, in field of size smaller than C' (and in which we do not necessarily have the equivalence), the inequality still holds. E.g., one can choose $C \geq C'^n$, where $n = |x|$.[11]

(6.5) Definition of the measure on pseudo-finite fields. Let $\varphi(\bar{x}, \bar{y})$ be a formula ($\bar{x}$ an n-tuple of variables), and D, $\varphi_{d,\mu}(\bar{y})$ the set and formulas given by Theorem (6.1). It follows from Remark (6.2)(6) that if F is a pseudo-finite field and $\bar{a}$ a tuple in F, then there will be a unique pair $(d, \mu) \in D$ such that $F \models \varphi_{d,\mu}(\bar{a})$. We then define $\dim(\varphi(\bar{x}, \bar{a})) = d$ and $\mu(\varphi(\bar{x}, \bar{a})) = \mu$. If S is the set defined by $\varphi(\bar{x}, \bar{a})$, then we also write $\dim(S)$ and $\mu(S)$ respectively.

Proposition. Let F be a pseudo-finite field, S, T two definable sets.
(1) If V is a variety defined over F, then $\dim(V(F)) = \dim(V)$ and $\mu(V(F)) = 1$.
(2) Assume that $T \cap S = \emptyset$. Then

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

[11] The argument I gave in class was not completely correct I think; it needs to be refined. An alternate proof can be given using Galois stratification, see [FHJ1].

(3) Assume that $f : S \to T$ is a definable function, which is onto. If for all $\bar{y} \in T$, $\dim(f^{-1}(\bar{y})) = d$, then $\dim(S) = \dim(T)+d$. If moreover for every $\bar{y} \in T$, $\mu(f^{-1}(\bar{y})) = m$, then $\mu(S) = m\mu(T)$.

(4) Let us define a function m_S on definable subsets of S as follows. Assume that $T \subseteq S$ is definable, and let $(d, \mu) = (\dim(S), \mu(S))$, $(e, \nu) = (\dim(T), \mu(T))$. Then

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

Then m_S is a finitely additive measure on the set of definable subsets of S.

(5) Let $\bar{S}$ be the Zariski closure of S (in F^{alg}. I.e., the smallest Zariski closed set containing S. It is defined over F). Then $\dim(S) = \dim(\bar{S})$. [That is, we are saying that the algebraic dimension of the algebraic set $\bar{S}$ coincides with the model-theoretic dimension of the set S]

Proof. (1) is clear.

Recall that F embeds elementarily in some ultraproduct $\prod_{q \in \mathcal{Q}} \mathbb{F}_q/\mathcal{U}$ of finite fields. Assume that S is defined by $\varphi(\bar{x}, \bar{a})$, write $\bar{a} = [\bar{a}_q]_{\mathcal{U}}$, and S_q for the subset of $\mathbb{F}_q^n$ defined by $\varphi(\bar{x}, \bar{a}_q)$. Note that for some set $A \in \mathcal{U}$, we will then have $\mathbb{F}_q \models \varphi_{d,\mu}(\bar{a}_q)$ for all $q \in A$, and therefore $|S_q| \sim \mu q^d$. A moment's thought shows that this gives items (2) - (4).

(5) By (5.3), there is an algebraic set $W(F) \subset F^{n+\ell}$ such that $S = \pi(W(F))$ and the restriction of the projection π to W is finite-to-one. Without loss of generality, $W(F)$ is Zariski dense in W, and by (3) we obtain that $\dim(W) = \dim(S)$. Working now in F^{alg}, we have that π is also finite-to-one on a Zariski-dense open subset of W, and therefore $\dim(W) = \dim(V)$ (algebraic dimensions). Since $V \supseteq \bar{S}$, we get that $\dim(V) = \dim(\bar{S})$.

(6.6) Existence of certain bounds. Let $\varphi(\bar{x}, \bar{y})$ be a formula.

(1) (Not the Strict Order Property)There is a number M such that in any finite or pseudo-finite field F, the length of a chain of definable subsets of F^n defined by formulas $\varphi(\bar{x}, \bar{a})$ for some tuples $\bar{a}$ in F, is bounded by M.

(2) (Finite Shelah rank) There is a number M such that in any finite field or pseudo-finite field F, if S is a definable set and $(\bar{a}_i)_{i \in I}$ is a set of tuples such that each $\varphi(\bar{x}, \bar{a}_i)$ defines a subset of S of the same dimension d as S, and for $i \neq j$, $\dim(\varphi(\bar{x}, \bar{a}_i) \wedge \varphi(\bar{x}, \bar{a}_j)) < d$, then $|I| \leq M$.

Proof. These two facts follow from general properties of measures. It suffices to show them for all pseudo-finite fields, since then they will be true in all sufficiently large finite fields, whence, taking into account the finitely many small finite fields, we will get the bound M.

(1) Assume that this is not the case, i.e., that there are such chains of arbitrarily large length. Then, going to a sufficiently saturated pseudo-finite field F, we can find a sequence $(\bar{a}_i)_{i \in \mathbb{N}}$ of tuples in F such that if $i < j$ then the set S_j defined by $\varphi(\bar{x}, \bar{a}_j)$ is strictly contained in the set S_i defined by $\varphi(\bar{x}, \bar{a}_i)$. Let D be the finite set of pairs associated to φ. Because D is finite, we may, going to a subsequence, assume that for every $i \in \mathbb{N}$, $\dim(S_i) = d$ and $\mu(S_i) = \mu$. The proof is by induction on d.

If $d = 0$, then we know that μ is the size of the set S_i, and therefore $|I| = 1$. Assume $d > 0$ and that the result holds for all definable sets of smaller dimension. For $i > 0$ let

$T_i = S_0 \setminus S_i$. Then the sets T_i, $i \in \mathbb{N}$, form a strictly increasing chain of subsets of S_0, and we have $\dim(T_i) < d$ (since $(\dim(S_i), \mu(S_i)) = (\dim(S_0), \mu(S_0))$). This contradicts the induction hypothesis and proves the result.

(2) Let D be the set of pairs associated to the formula $\varphi(\bar{x}, \bar{y})$, and let ν be the inf of all μ such that $(d, \mu) \in D$. If $\varphi(\bar{x}, \bar{a}_i)$, $i \in I$, define subsets S_i of S such that $\dim(S_i) = d$ and $\dim(S_i \cap S_j) < d$, then we get $m_S(S_i) \geq \nu/\mu(S)$ and $m_S(S_i \cap S_j) = 0$. This gives $|I| \leq \mu(S)/\nu$.

(6.7) The independence property. Recall that a formula $\varphi(\bar{x}, \bar{y})$ has the *independence property* (in the model M) iff for every n, there are tuples $\bar{a}_i$, $1 \leq i \leq n$, and $\bar{b}_s$, $s \in \mathcal{P}(\{1, \ldots, n\})$, in M such that

$$M \models \varphi(\bar{a}_i, \bar{b}_s) \iff i \in s$$

for every i and s. A complete theory has the independence property if there is a formula which has the independence property.

Theorem (Duret [D]) The theory of any pseudo-algebraically closed field which is not separably closed, has the independence property.

We will give here a simple case of his proof, for a pseudo-finite field of characteristic $\neq 2$. (In characteristic 2, the example can be modified). Let F be a pseudo-finite field and consider the formula $\varphi(x, y)$ which says that $x + y$ is a square and $x \neq y$. Let $a_1, \ldots, a_n$ be distinct elements of F, s a subset of $\{1, \ldots, n\}$, we want to find an element b such that $b + a_i$ is a square if and only if $i \in s$. Renumbering the a_i's, we may assume that $i \in s \iff i \leq r$.

Because F is pseudo-finite, it contains an element c which is not a square. Then, as F has a unique extension of degree 2, we have $F^\times = F^{\times 2} \cup cF^{\times 2}$, and therefore

$$F \models \forall x \, [(\forall y \; y^2 \neq x) \leftrightarrow (\exists y \; y^2 = cx)].$$

Let t be transcendental over F, and consider the extension

$$L = F(t, \sqrt{t + a_1}, \ldots, \sqrt{t + a_r}, \sqrt{c(t + a_{r+1})}, \ldots, \sqrt{c(t + a_n)}).$$

Then $L \cap F^{alg} = F$ (This needs a proof which I will not give). Hence, by Lemma (3.9), in F there is an element d such that $d + a_1, \ldots, d + a_r, c(d + a_{r+1}), \ldots, c(d + a_n)$ are squares. I.e., $d + a_i$ is a square if and only if $i \leq r$.

(6.8) Graphs interpretable in pseudo-finite fields. The above proof shows that the random graph is interpretable in any pseudo-finite field (of characteristic $\neq 2$), by the formula expressing that $x + y$ is a square and $x \neq y$.

Observe that if -1 is a square in F, then the formula $\psi(x, y)$ saying that $x - y$ is a square and is non-zero would work as well. If -1 is not a square in F, then the formula $\psi(x, y)$ defines the random tournament. (a *tournament* is a binary relation not intersecting the diagonal and such that given two distinct elements, one exactly of (a, b), (b, a) is in the relation. The *random tournament* is a tournament in which given any two disjoint finite sets A and B there is an element c such that $\bigwedge_{a \in A} R(c, a) \wedge \bigwedge_{b \in B} R(b, c)$.

Hrushovski proves in [H1] that one cannot interpret the *random triangle-free* graph in any countable pseudo-finite field. Beyarslan proves in [B] that one can interpret in any pseudo-finite field the random n-hypergraph. Recall that if $n \geq 2$, an *n-hypergraph* is a sn n-ary relation R satisfying:

– $R(x_1, \ldots, x_n) \to \bigwedge_{i \neq j} x_i \neq x_j$,

– $R(x_1, \ldots, x_n) \to \bigwedge_{\sigma \in \mathrm{Sym}(\{1,\ldots,n\})} R(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

The *random n-hypergraph* is the existentially closed countable n-hypergraph. I.e., it is countable, and satisfies, for all m, ℓ,

if $a_1, \ldots, a_m, b_1, \ldots, b_\ell$ are distinct $(n-1)$-element subsets, then there is an element x such that $\bigwedge_i R(x, a_i) \wedge \bigwedge_j \neg R(x, b_j)$.

(6.9) Another interesting result, in the vein of (6.3). Say that $I \subset \mathbb{F}_p$ is an interval (p a prime) if there is some interval J in $\mathbb{Z}$ such that I is the image of J under the natural reduction modulo $p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Proposition (Kowalski [K]). If $\varphi(x)$ is a formula of the language of rings which defines in all prime field $\mathbb{F}_p$ an interval, then there is a number N such that for every prime p, one of $|\varphi(\mathbb{F}_p)|$, $|\neg\varphi(\mathbb{F}_p)|$ has size $\leq N$.

Note that an argument using measures is not sufficient, since the interval $[0, \frac{p-1}{2}]$ has size approximately $\frac{p}{2}$.

(6.10) N-dimensional asymptotic classes. Let N be a positive integer. A class $\mathcal{C}$ of finite structures is an *N-dimensional asymptotic class* if to each formula $\varphi(\bar{x}, \bar{y})$, $\bar{x}$ an n-tuple, $\bar{y}$ an m-tuple, one can associate a finite set D of pairs $(d, \mu) \in \{0, \ldots, Nn\} \times \mathbb{R}^{>0} \cup \{(0,0)\}$, as well as formulas $\varphi_{d,\mu}$ for $(d, \mu) \in D$, and a constant $C > 0$ such that

(1) For any $M \in \mathcal{C}$ and m-tuple $\bar{a} \in M$, one has, for some $(d, \mu) \in D$,

$$\big||\varphi(M, \bar{a})| - \mu |M|^{d/N}\big| = o(|M|^{d/N}). \qquad (*)$$

[Here $\varphi(M, \bar{a})$ denotes the set $\{\bar{b} \in M^n \mid M \models \varphi(\bar{b}, \bar{a})\}$.]

(2) The formula $\varphi_{d,\mu}(\bar{y})$ defines in each $M \in \mathcal{C}$ the set of tuples $\bar{a}$ such that $(*)$ holds.

Here the notation $o(|M|^{d/N})$ means: for every $\varepsilon \in \mathbb{R}^{>0}$, there is $Q \in \mathbb{N}$ such that if $M \in \mathcal{C}$ has size $> Q$ and if $\bar{a}$ satisfies $\varphi_{d,\mu}$ in M, then $\big||\varphi(M, \bar{a})| - \mu |M|^{d/N}\big| < \varepsilon |M|^{d/N}$.

The universe M is then thought to be N-dimensional. Because of the definability condition, it turns out that one only need to verify the properties for formulas with x a singleton. For more details one can consult the survey paper by Elwes and Macpherson [EM].

(6.11) Measurable structures. A structure M is measurable if there is a function $h = (\mathrm{Dim}, \mu)$ (dimension and measure) from the set $\mathrm{Def}(M)$ of definable subsets of cartesian powers of M, taking values in $\mathbb{N} \times \mathbb{R}^{>0} \cup \{(0,0)\}$, and satisfying the following conditions:

(1) For every formula $\varphi(\bar{x}, \bar{y})$ there is a finite set $D = D_\varphi$ such that for any $\bar{a}$ in M $h(\varphi(M, \bar{a})) \in D$.

(2) If S is finite (or empty), then $h(S) = (0, |S|)$,

(3) For every formula φ, and $(d, \mu) \in D_\varphi$, the set $\{\bar{a} \mid h(\varphi(M, \bar{a})) = (d, \mu)\}$ is definable in M (without parameters).

(4) (Additivity) Let S, T be disjoint definable subsets of M^n. Then $\mathrm{Dim}(S \cup T) = \sup\{\mathrm{Dim}(S), \mathrm{Dim}(T)\}$, and

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

(5) (Fubini) Assume that $f : S \to T$ is a definable function, which is onto. If for all $\bar{y} \in T$, $\mathrm{Dim}(f^{-1}(\bar{y})) = d$, then $\mathrm{Dim}(S) = \mathrm{Dim}(T) + d$. If moreover for every $\bar{y} \in T$, $\mu(f^{-1}(\bar{y})) = m$, then $\mu(S) = m\mu(T)$.

(6.12) Comments. The motivating example are pseudo-finite fields. Because of the definability condition and the Fubini condition, one can restrict one's attention to definable subsets of M. Also, as with pseudo-finite fields, it follows that the theory of a measurable structure is supersimple.

If $\mathcal{C}$ is an N-dimensional asymptotic class of finite structures, then any structure in the elementary class generated by $\mathcal{C}$ will be measurable, and we also see that the definitions and measures will be uniform through the structures in this elementary class.

The converse is however not true: there exists measurable structures which are not elementarily equivalent to ultraproducts of finite structures. Below we will give such an example.

(6.13) Definitions.

(1) Recall that a first order theory T is *strongly minimal* if in any model M of T, any definable (with parameters) subset of M is finite or cofinite.

(2) In a strongly minimal theory one can define a rank, called the *Morley rank* as well as a multiplicity, the *Morley degree*, of definable sets. I will not give precise definitions, let me say that the rank satisfies the obvious axioms of a dimension (see properties (4) and (5) of Dim in (6.11)), and that the Morley degree of a definable set S is the maximal number n such that S can be definably partitioned into sets of the same rank as S. Furthermore, the Morley rank of the universe is 1, and of a finite set is 0. A strongly minimal theory T has the DMP (*definable multiplicity property*) if for any model M, formula $\varphi(\bar{x}, \bar{y})$ and integer $n > 0$, the set of tuples $\bar{a}$ in M such that $\varphi(M, \bar{a})$ has Morley degree n, is definable.

Important examples of strongly minimal theories with the DMP are the completions of the theory ACF of algebraically closed fields. Moreover, if T_1 and T_2 are strongly minimal with the DMP, then so is the Hrushovski fusion T_3 constructed from T_1 and T_2.

(6.14) Theorem (Ryten-Tomasic [RT]) Let T be a strongly minimal theory with the DMP and which eliminates imaginaries. Consider the theory T_σ of models of T with an automorphism σ (so, structures in the language $\mathcal{L}$ to which one has added a unary function symbol σ), let N be an existentially closed model of T_σ, and let F be the $\mathcal{L}$-structure $\{a \in N \mid \sigma(a) = a\}$. Then F is measurable of dimension 1.

(6.15) Example of a measurable structure not arising from an asymptotic class of finite structures. So, let T_1 be the theory of algebraically closed fields of characteristic

2 (in a language $\mathcal{L}_1$), and T_2 the theory of algebraically closed fields of characteristic 3 (in the language $\mathcal{L}_2$). Let T_3 be the Hrushovski fusion of T_1 and T_2, and let F be as above. Then the reduct of F to $\mathcal{L}_1$ is a pseudo-finite field of characteristic 2, the reduct of F to $\mathcal{L}_2$ is a pseudo-finite field of characteristic 3, and F cannot be elementarily equivalent to an ultraproduct of finite $\mathcal{L}_1 \cup \mathcal{L}_2$-structures: a power of 2 can never equal a power of 3 unless they both equal 1. But, by the result of Ryten-Tomasic, the $\mathcal{L}_1 \cup \mathcal{L}_2$-structure F is measurable of dimension 1.

(6.16) Examples of finite dimensional asymptotic classes. By Theorem (6.1), the collection of all finite fields forms a 1-dimensional asymptotic class, as does any subclass. Also, for a fixed $n > 1$, the class of all $\mathrm{GL}_n(\mathbb{F}_q)$ is an (n^2-1)-dimensional asymptotic class. The definability assumption comes from the fact that there is a uniform interpretation of the field $\mathbb{F}_q$ in these groups ([P]). Here is another example.

Fix a prime p, and relatively prime integers m, n with $m \geq 1$ and $n > 1$. Let $\mathcal{C}_{(m,n,p)}$ be the class of all fields $\mathbb{F}_{p^{kn+m}}$ with a distinguished automorphism Frob^k, for $k \in \mathbb{N}^{>0}$. One can show that there is no formula of the field language which defines in each field $\mathbb{F}_{p^{kn+m}}$ the graph of Frob^k. These structures appear in a significant way in the study of certain finite simple groups: for instance $\mathcal{C}_{(1,2,2)}$ is uniform parameter biinterpretable with the classes of Suzuki groups ${}^2B_2(2^{2k+1})$ and the Ree groups ${}^2F_4(2^{2k+1})$, and $\mathcal{C}_{(1,2,3)}$ with the class of Reee groups ${}^2G_2(3^{2k+1})$.

Bibliography

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

[B] O. Beyarslan, Interpreting Random Hypergraphs in Pseudofinite Fields, to appear in J. of Inst. Math. Jussieu.

[CK] C.C. Chang, H.J. Keisler, *Model theory*, North-Holland, Amsterdam 1977.

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

[DL] J. Denef, F. Loeser, Definable sets, motives and p-adic integrals, J. Amer. Math. Soc. 14 (2001), no. 2, 429–469.

[DS] 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.

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

[EM] R. Elwes, H.D. Macpherson, A survey of asymptotic classes and measurable structures, in *Model theory and applications to algebra and analysis* (Eds. Z. Chatzidakis, H.D. Macpherson, A. Pillay, A.J. Wilkie), Cambridge University Press, 2008, 125 – 159.

[FHJ1] M. Fried, D. Haran, M. Jarden, Galois stratification over Frobenius fields, Adv. in Math. 51 (1984), 1 – 35.

[FHJ2] M. Fried, D. Haran, M. Jarden, Effective counting of the points of definable sets over finite fields, Israel J. Math. 85 (1994), 103 – 133.

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

[FS] M. Fried, G. Sacerdote, Solving diophantine problems over all residue class fields of a number field and all finite fields, Annals of Math. 104 (1976), 203 – 233.

[H] I. Halupczok, A measure for perfect PAC fields with pro-cyclic Galois group. Journal of Algebra 310 (2007), 371-395.

[He] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann. 95 (1926), no. 1, 736 – 788.

[H1] E. Hrushovski, Pseudo-finite fields and related structures, in: Model Theory and Applications, Bélair et al. ed., Quaderni di Matematica Vol. 11, Aracne, Rome 2005, 151 – 212.

[H2] E. Hrushovski, The first-order theory of the Frobenius, preprint, available at ArXiv: `http://front.math.ucdavis.edu/math.LO/0406514`.

[HP1] E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. of Math. 85 (1994), 203 – 262.

[HP2] E. Hrushovski, A. Pillay, Definable subgroups of algebraic groups over finite fields, J. reine angew. Math. 462 (1995), 69 – 91.

[K] E. Kowalski, Exponential sums over definable subsets of finite fields, Israel J. Math. 160 (2007), 219–251.

[L1] S. Lang, *Introduction to algebraic geometry*, Addison-Wesley Pub. Co., Menlo Park 1973.

[L2] S. Lang, *Algebra*, Addison-Wesley Pub. Co., Menlo Park 1984.

[LW] S. Lang, A. Weil, Number of points of varieties in finite fields, Am. J. of Math. 76 (1954), 819 –827.

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

[MS] H.D. Macpherson, C. Steinhorn, One-dimensional asymptotic classes of finite structures, Trans. Amer. Math. Soc. 360(2008), 411–448.

[P] F. Point, Ultraproducts and Chevalley groups, Arch. Math. Logic 38 (1999), 355–372.

[R] M. Ryten, *Results around asymptotic and measurable groups*, PhD thesis, University of Leeds, 2008.

[RT] M. Ryten, I. Tomašić, ACFA and measurability, Selecta Mathematica New series, 11 (2005), 523-537.

[S] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc. 197 (1974), 273 – 313.