J. reine angew. Math. **427** (1992), 107—135

Journal für die reine und angewandte Mathematik

Definable sets over finite fields

By *Zoé Chatzidakis* at Paris, *Lou van den Dries* at Urbana and *Angus Macintyre* at Oxford

Introduction and statement of results

This article originated with a question posed by Ulrich Felgner (Oberwolfach, January '90):

Is there a formula $\phi(Y)$ in the language of rings that defines in each finite field of the form $\mathbb{F}_{q^2}$ its subfield $\mathbb{F}_q$?

Note that for a given prime power q the formula $Y^q = Y$ defines in $\mathbb{F}_{q^2}$ its subfield $\mathbb{F}_q$, but this formula depends on q. It turns out that a negative answer to Felgner's question is easy to obtain from a theorem of Ax [1], see (4.2) below, but it is natural to look for a stronger negative result, namely:

(*) *Given any formula $\phi(Y)$ in the language of rings there are only finitely many prime powers q such that $\phi(Y)$ defines in $\mathbb{F}_{q^2}$ the subfield $\mathbb{F}_q$.*

We give here a new and (modulo the Lang-Weil estimates) selfcontained treatment of various logical aspects of finite (and pseudo-finite) fields. In particular we get new results on definable sets with (*) as an obvious consequence. Our main result extends the Lang-Weil estimates on absolutely irreducible varieties to arbitrary formulas with parameters. However, a finite number of case distinctions, depending on the formula, becomes necessary. Here is a precise formulation.

Main Theorem. *Let $\phi(X, Y)$ be a formula in the language of rings, with $X = (X_1, \ldots, X_m)$ as parametric variables and $Y = (Y_1, \ldots, Y_n)$. Then there is a positive constant C and a finite set D of pairs (d, μ) with $d \in \{0, \ldots, n\}$ and μ a positive rational number, such that for each finite field $k = \mathbb{F}_q$ and each $x \in k^m$, if the set $\phi(x, k^n) := \{y \in k^n : k \models \phi(x, y)\}$ is nonempty, then $|\operatorname{card}(\phi(x, k^n)) - \mu q^d| \leqq C q^{d-(1/2)}$ for some $(d, \mu) \in D$.*

For instance, when $m = 0$ (no parameters) and $n = 1$, the theorem says:

Given a formula $\phi(Y)$ in one free variable Y there are positive constants A, B and positive rationals $0 < \mu_1 < \ldots < \mu_k \leqq 1$ such that for each finite $k = \mathbb{F}_q$: either $\operatorname{card}(\phi(k)) \leqq A$, or $|\operatorname{card}(\phi(k)) - \mu_i q| \leqq B\sqrt{q}$ for some $i \in \{1, \ldots, k\}$.

In particular there are constants $A, C > 0$ such that either $\text{card}(\phi(\mathcal{k})) \leqq A$, or $\text{card}(\phi(\mathcal{k})) \geqq C \cdot \text{card}(\mathcal{k})$. By taking here $\mathcal{k} = \mathbb{F}_{q^2}$ one obtains (*) above.

Remarks. (1) It can certainly happen that in this result about $\phi(Y)$ one needs more than one rational μ_i. For example, let $\phi(Y)$ be the formula $\exists Z(Z^2 = Y)$ ("Y is a square"). When $\text{char}(\mathcal{k}) \neq 2$ there are $(1/2)(q+1)$ squares in $\mathcal{k}$, while for $\text{char}(\mathcal{k}) = 2$ all elements of $\mathcal{k}$ are squares. So here we need two rationals: $\mu_1 = 1/2$ and $\mu_2 = 1$. One obvious contrast with Lang-Weil type estimates is the presence of proper fractions μ: this is the effect of allowing quantifiers in the formulas.

(2) Here is an important addition to the Main Theorem.

For each $(d, \mu) \in D$ there is a formula $\phi_{d,\mu}(X)$ that defines in each finite field $\mathcal{k} = \mathbb{F}_q$ the set of $x \in \mathcal{k}^m$ such that $|\text{card}(\phi(x, \mathcal{k}^n)) - \mu q^d| \leqq Cq^{d-(1/2)}$.

(3) In our main theorem it is clear that for sufficiently large $\mathcal{k} = \mathbb{F}_q$ (depending on the formula ϕ) there is for each $x \in \mathcal{k}^m$ with $\phi(x, \mathcal{k}^n) \neq \emptyset$ a *unique* pair $(d, \mu) \in D$ such that $|\text{card}(\phi(x, \mathcal{k}^n)) - \mu q^d| \leqq Cq^{d-(1/2)}$, or equivalently: $\mathcal{k} \models \phi_{d,\mu}(x)$.

In terms of $\phi_{d,\mu}(x)$ these numbers d and μ also make sense for *pseudo-finite* $\mathcal{k}$ and $x \in \mathcal{k}^m$: d is the algebraic dimension of the Zariski closure of $\phi(x, \mathcal{k}^n)$, and μ is the measure of $\phi(x, \mathcal{k}^n)$ with respect to a finitely additive measure on its Zariski closure. These aspects are treated in detail in section 4.

(4) A more difficult variant of Felgner's question is whether the field $\mathbb{F}_q$ is *interpretable* in the field $\mathbb{F}_{q^2}$, uniformly for infinitely many q. Again the answer is negative: this follows by extending the main theorem to definable sets modulo definable equivalence relations. See (3.10) and (3.11) for details.

In this connection it would be interesting to know whether the theory of finite fields admits some kind of *elimination of imaginaries*, cf. Poizat [11], where this notion is introduced (for complete theories).

We now give a brief description of the contents of the various sections.

Proof of the Main Theorem (sections 1, 2, 3). Basic to our approach is the Decomposition-Intersection Procedure, a procedure that constructs from an affine algebraic set a finite union of absolutely irreducible algebraic subsets defined over the same field F as the original algebraic set and with the same F-points. For our purpose it is vital to obtain some information on how this procedure depends on parameters, and this aspect is studied in section 1.

The next step in the direction of our Main Theorem is a variant of Kiefe's quantifier elimination for finite fields [9]. This variant is as follows. Enrich the language L of rings with extra constant symbols $c_{n1}, \ldots, c_{nn}$, for each $n > 1$, and consider *enriched* finite fields: these are finite fields $\mathcal{k}$ in which for each $n > 1$ the symbols $c_{n1}, \ldots, c_{nn}$ are interpreted as the coefficients of an irreducible polynomial

$$T^n + c_{n1} T^{n-1} + \ldots + c_{nn}$$

over $\mathfrak{k}$. Each finite field $\mathfrak{k}$ can be so enriched, in infinitely many ways. In section 2 we prove the following Positive Quantifier Elimination:

Each formula $\phi(X)$, $X = (X_1, \ldots, X_m)$, in the enriched language is equivalent, uniformly for all sufficiently large enriched finite fields, to a conjunction of formulas of the form $\exists T g(c, X, T) = 0$, where $g(c, X, T)$ is a polynomial over $\mathbb{Z}$ in the extra symbols c_{ni}, the variables $X_1, \ldots, X_m$ and the single variable T.

In Kiefe's result ϕ is equivalent to a boolean combination of formulas $\exists T g(X, T) = 0$, so that negations $\neg \exists T g(X, T)$ may appear; both ϕ and the boolean combination are in the language of rings; Kiefe's theorem is not used in the proof of our positive quantifier elimination. We also prove in section 2 that *each pseudo-finite field is generated as a ring by each of its infinite definable subsets*, cf. (2.12).

The rest of the proof of the Main Theorem is given in section 3 and consists of easy counting arguments and estimates using the Lang-Weil Theorem.

(J. Denef suggested later another proof of our main result: instead of intersection-Decomposition + Lang-Weil, one could use Galois stratification (cf. [6]) + formulas of Grothendieck & Deligne involving the action of Frobenius on cohomology.)

Applications of the Main Theorem (section 4). We already mentioned Felgner's question and its variants, which inspired our work. More important seem to us the following model-theoretic consequences:

Given a pseudo-finite field F and a definable set $S \subseteq F^{m+1}$ there is no infinite set $A \subseteq F^m$ such that all sets S_a $(a \in A)$ are infinite and all intersections $S_a \cap S_b$ $(a \neq b, a, b \in A)$ are finite.

This answers a question raised by Cherlin and Hrushovski, and it seems to imply that much of model theoretic stability theory makes sense for pseudo-finite fields, even though these structures are unstable, cf. Duret [5].

Another result in the same spirit is the failure of the "strict order property" for the theory of finite fields. This may sound ominous but is actually quite nice, cf. (4.6):

Given a formula $\phi(X, Y)$ with $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_n)$, there is a positive integer $M = M(\phi)$ such that for each finite field $\mathfrak{k}$ there is no strictly increasing sequence of sets $\phi(x^1, \mathfrak{k}^n) \subset \ldots \subset \phi(x^M, \mathfrak{k}^n)$ of length M, with $x^i \in \mathfrak{k}^m$.

Still open is the question, raised by Cherlin, whether the universal-homogeneous triangle-free graph (cf. [8]) can be interpreted in a pseudo-finite field.

Algebraic boundedness (section 5). Here we prove that *the theory of pseudo-finite fields is algebraically bounded*, cf. (5.7). We refer to the beginning of section 5 for the definition of *algebraically bounded theory of fields*. The main ingredient in the proof is a new general fact about perfect pseudo-algebraically closed fields (cf. (5.3)). Before our work on

this topic Jarden had mentioned to us (in Oberwolfach, January '90) that he had obtained algebraic boundedness of pseudo-finite fields, but his proof is not known to us.

Axiomatizability results (section 6). A totally different problem that was also stimulated by Felgner's question is to axiomatize the class of fields of the form $\mathbb{F}_{q^2}$, that is, to give a (reasonable) set of axioms in the language of rings equivalent to the set of sentences true in all $\mathbb{F}_{q^2}$. As usual it is convenient to disregard "small" finite fields, and change the problem as follows.

Let Psf be the theory of pseudo-finite fields: its models are the infinite fields satisfying the sentences that are true in all finite fields.

Given $n > 0$, let Psf^n be the theory whose models are the infinite fields satisfying the sentences that are true in all finite fields of the form $\mathbb{F}_{q^n}$ with q a prime power.

Then it is reasonable to ask:

$$\textit{Is } \mathrm{Psf}^2 \textit{ axiomatized by } \mathrm{Psf} \cup \{\exists x(x^2 = n) \colon n \in \mathbb{Z}\}\,?$$

If follows easily from Ax [1] that Psf^2 and $\mathrm{Psf} \cup \{\exists x(x^2 = n) \colon n \in \mathbb{Z}\}$ have indeed the same models of characteristic $\neq 0$, but this is not true anymore in characteristic 0, as we shall see in section 6, the last section. Nevertheless, we show, using again results from Ax [1], that Psf^2 can be axiomatized by Psf together with axioms requiring that certain one variable monic polynomials over $\mathbb{Z}$ have zeros.

There seems to be however no simple description of these polynomials, for instance one cannot restrict oneself to polynomials of degree bounded by some constant, nor to polynomials solvable by radicals over $\mathbb{Q}$, see (6.6) and (6.7).

Open questions. 1. *Does the theory of finite fields eliminate imaginaries*?

2. *Can one interpret the countable universal-homogeneous triangle-free graph in a pseudo-finite field*? (We don't have a clue: this may require new ideas.)

In both questions we may allow the use of extra constants.

Notations and conventions. We fix for each field F an algebraic closure $\tilde{F}$; we put $G(F) := \mathrm{Aut}(\tilde{F}|F)$, also for nonperfect F. Formulas and sentences are in the language $L := \{0, 1, -, +, .\}$ of rings, unless specified otherwise. The *theory of finite fields* is the set of all sentences true in all finite fields. We always let $X_1, \ldots, X_m, Y_1, \ldots, Y_n, T$ be distinct variables, and put $X = (X_1, \ldots, X_m)$, $Y = (Y_1, \ldots, Y_n)$. The X's generally serve as parametric variables.

Acknowledgement. We thank MSRI at Berkeley for making the collaboration between the authors on this topic possible, and G. Cherlin for a stimulating discussion. Van den Dries thanks the NSF for support during the writing of this paper.

§ 1. The decomposition-intersection procedure

(1.1) This procedure is basic in the logic of finite and pseudo-finite fields, but important properties of it (uniform bounds, dependence on parameters) that we need here seem to be unavailable elsewhere.

(1.2) Fix a field F and an algebraic closure $\tilde{F}$. Given a set $I \subseteq F[Y]$, $Y = (Y_1, \ldots, Y_n)$, $n \geqq 1$, we put $V(I) := \{y \in \tilde{F}^n : f(y) = 0 \text{ for all } f \in I\}$ and call $V(I)$ an F-algebraic set. Usually I is an ideal, or a finite set $\{f_1, \ldots, f_k\} \subseteq F[Y]$ in which case we write $V(f_1, \ldots, f_k)$.

(1.3) To an F-algebraic set $V = V(I) \subseteq \tilde{F}^n$ as in (1.2) we associate an F-algebraic set $V' \subseteq V$ as follows: let $V_1, \ldots, V_k \subseteq \tilde{F}^n$ be the (absolutely) irreducible components of V. Some of these V_i's may not be F-algebraic sets but they are F'-algebraic sets for some finite degree extension field $F' \subseteq \tilde{F}$, and each conjugate $\sigma(V_i)$, $\sigma \in G(F) = \mathrm{Aut}(\tilde{F}|F)$, also belongs to $\{V_1, \ldots, V_k\}$. For each $i \in \{1, \ldots, k\}$, set $W_i := \bigcap_\sigma \sigma(V_i)$, an F-algebraic set with $V_i \cap F^n = W_i \cap F^n$. We define $V' := W_1 \cup \ldots \cup W_k$. Clearly V' is an F-algebraic subset of V with $V \cap F^n = V' \cap F^n$.

We can now repeat the same process with V' and get V''. Continuing in this way we get a decreasing sequence of F-algebraic sets $V \supseteq V' \supseteq V'' \supseteq \ldots \supseteq V^{(r)} \supseteq \ldots$. By Hilbert's basis theorem all terms in this sequence from some point on are equal and we denote this ultimately constant term by V^*. Hence V^* is a (possibly empty) F-algebraic set with

$$V \cap F^n = V^* \cap F^n . \tag{1}$$

So when we are just interested in the F-points of V we can restrict attention to V^*. Call V^* the *F-absolute kernel of V*. The following properties are easy consequences of the construction of V^*:

(2) The absolutely irreducible components of V^* (if any) are F-algebraic sets.

(3) V^* contains every F-algebraic subset of V that is absolutely irreducible.

(1.5) How large should r be in order that $V^* = V^{(r)}$? In fact, $r = n$ will do as the following considerations show. Define a quantity $\alpha(V) \in \{-\infty, 0, 1, \ldots, n-1\}$ by:

$\alpha(V) := -\infty$ if all absolutely irreducible components V_i of V are F-algebraic,

$\alpha(V) := \max\{\dim(V_i) : V_i \text{ is not } F\text{-algebraic}\}$, otherwise.

We claim:

(i) $\alpha(V) \geqq 0 \quad \Rightarrow \alpha(V') < \alpha(V)$,

(ii) $\alpha(V) = -\infty \Leftrightarrow V' = V (\Leftrightarrow V^* = V)$.

Property (ii) is clear. For (i), assume $\alpha(V) \geqq 0$, let $V_1, \ldots, V_e$ be the absolutely irreducible components of V that are F-algebraic and of dimension $\geqq \alpha := \alpha(V)$, let

$V_{e+1}, \ldots, V_f$ be the absolutely irreducible components of V of dimension α that are not F-algebraic, and let $V_{f+1}, \ldots, V_k$ be the remaining absolutely irreducible components, which are of dimension $< \alpha$, so $0 \leqq e < f \leqq k$. Then we have, with the notations of (1.3): $W_i = V_i$ for $1 \leqq i \leqq e$ and $\dim(W_i) < \alpha$ for the remaining i's. So

$$V' = (V_1 \cup \ldots \cup V_e) \cup (W_{e+1} \cup \ldots \cup W_k) .$$

Let $C_1, \ldots, C_g$ be the absolutely irreducible components of $W_{e+1} \cup \ldots \cup W_k$, so $\dim(C_j) < \alpha$ for all j. Hence the absolutely irreducible components of V' are $V_1, \ldots, V_e$, plus those C_j that are not contained in $V_1 \cup \ldots \cup V_e$. From this description it is clear that

$$\alpha(V') < \alpha(V) .$$

Since $\alpha(V) \leqq n-1$, it follows that $\alpha(V^{(n)}) = -\infty$, hence by (ii) applied to $V^{(n)}$:

$$V^* = V^{(n)} . \tag{1.5}$$

(1.6) By similar arguments one proves, for F-algebraic subsets V_1 and V_2 of $\tilde{F}^n$:

$$(V_1 \cup V_2)' = V_1' \cup V_2', \text{ hence } (V_1 \cup V_2)^* = V_1^* \cup V_2^* .$$

We do not need this later on and leave the proof to the reader.

One of our goals in this section is the following proposition to be used in the proof of the Main Theorem.

(1.7) Proposition (Existence of bounds). *Let $V := V(f_1, \ldots, f_r)$, where $f_1, \ldots, f_r \in F[Y]$ are all of degree $\leqq d$. Then there are natural numbers D, M and R depending only on (d, n, r) and independent of the field F and the specific polynomials f_j, such that*

(i) *V^* has at most M absolutely irreducible components,*

(ii) *each absolutely irreducible component of V^* is of the form $V(h_1, \ldots, h_R)$ for h's in $F[Y]$ of degree $\leqq D$.*

This will be derived from a more precise result, Theorem (1.15) below, which states how V^* depends on parameters. We need several preparations.

(1.8) How does one actually get V' from $V := V(f_1, \ldots, f_r)$ when $f_1, \ldots, f_r \in F[Y]$ are given? Imagine the V_i's as in (1.3) have been constructed and are F'-algebraic sets, where $F' \subseteq \tilde{F}$ is a finite degree extension of F. Let $b_1, \ldots, b_N$ be a basis of F' as F-linear space, let $V_i := V(g_{i1}, \ldots, g_{ir(i)})$ with $g_{ij} \in F'[Y]$, and write $g_{ij} = \sum b_\nu \cdot g_{ij\nu}$, $g_{ij\nu} \in F[Y]$.

We may and shall assume that $F' | F$ is *separable*, since we can replace the b_ν, the g_{ij}, and the $g_{ij\nu}$ by their p^eth powers ($e > 0$) if $\mathrm{char}(F) = p > 0$.

Then one checks easily that, in the notation of (1.3):

$$W_i = V(\{g_{ijv} : 1 \leqq j \leqq r(i), 1 \leqq v \leqq N\}).$$

Combining this with $V' = W_1 \cup \ldots \cup W_k$ we obtain

$$V' = V(\{\prod_{1 \leqq i \leqq k} g_{ij(i)v(i)} : j \text{ and } v \text{ are functions on } \{1, \ldots, k\} \text{ such that } 1 \leqq j(i) \leqq r(i),\ 1 \leqq v(i) \leqq N\}).$$

(1.9) Now the key question: how does the intersection-decomposition procedure depend on *parameters*? The dependence is certainly not "rational" but we can expect it to be "algebraic". To express this dependence in a precise and quantifier free way we extend the language of rings with extra d-place function symbols ϱ_d ($d \geqq 2$), to be interpreted in each field F as "root functions" according to the following axioms:

$$t^d + x_1 t^{d-1} + \ldots + x_d = 0 \rightarrow \varrho_d(x)^d + x_1 \varrho_d(x)^{d-1} + \ldots + x_d = 0.$$

Formally, define a *field with root functions* to be a field F equipped for each $d \geqq 2$ with a function $\varrho_d : F^d \to F$ satisfying the axiom above. Clearly each field can be expanded to a field with root functions (in more than one way). Let L_ϱ be the language of rings augmented by the new function symbols ϱ_d.

(1.10) Lemma. *There is for each $d > 0$ a quantifier-free L_ϱ-formula $\mathrm{Irr}_d(x)$, $x = (x_1, \ldots, x_d)$, such that for each field F with root functions and each $a \in F^d$ we have:*

$$F \models \mathrm{Irr}_d(a) \Leftrightarrow \textit{the polynomial } T^d + a_1 T^{d-1} + \ldots + a_d \in F[T] \textit{ is irreducible.}$$

Proof. By a familiar model theoretic criterion it suffices to check for fields F_1 and F_2 with root functions with a common substructure $\mathscr{A} = (A, \ldots)$ and $a_1, \ldots, a_d \in A$: $T^d + a_1 T^{d-1} + \ldots + a_d$ is irreducible in $F_1[T]$ iff $T^d + a_1 T^{d-1} + \ldots + a^d$ is irreducible in $F_2[T]$. Since $\mathscr{A}$ is a substructure of F_1 the fraction field F of A is relatively algebraically closed in F_1, and similarly in F_2. It follows easily that $T^d + a_1 T^{d-1} + \ldots + a_d$ is irreducible in $F_1[T]$ if and only if it is irreducible in $F[T]$, which in turn is equivalent to its irreducibility in $F_2[T]$. □

(1.11) Fix polynomials $f_1(X, Y), \ldots, f_r(X, Y) \in \mathbb{Z}[X, Y]$, $X = (X_1, \ldots, X_m)$, $Y = (Y_1, \ldots, Y_n)$, and set for each field F and $x \in F^m$.

$$V_{F,x} := V(f_1(x, Y), \ldots, f_r(x, Y)) = \{y \in \tilde{F}^n : f_1(x, y) = \ldots = f_r(x, y) = 0\},$$

and let $V'_{F,x}$ and $V^*_{F,x}$ be V' and V^* as defined in (1.3) above, for $V = V_{F,x}$.

Fix a field F and a point $x = (x_1, \ldots, x_m) \in F^m$. Let $E \subseteq F$ be the relative algebraic closure in F of the subfield of F generated by $x_1, \ldots, x_m$, and let $\tilde{E} \subseteq \tilde{F}$ be the algebraic closure of E. Then the polynomials $f_1(x, Y), \ldots, f_r(x, Y)$ have their coefficients in the field E. If in (1.8) we take E instead of F and $V_{E,x} := \{y \in \tilde{E}^n : f_1(x, y) = \ldots = f_r(x, y) = 0\}$ instead of V we obtain a tuple $(q(T), g_1, \ldots, g_k)$ with the following properties:

(i) *$q(T) \in E[T]$ is a monic separable irreducible polynomial, say of degree N,*

(ii) *each g_i is a tuple $(g_{ijv})_{1 \leqq j \leqq r(i),\, 1 \leqq v \leqq N}$ of polynomials in $E[Y]$,*

(iii) *if α is a zero of q in $\tilde{E}$, and we set $E' := E(\alpha)$, $g_{ij} := \sum g_{ijv} \alpha^{v-1} \in E'[Y]$, and $V_{i,E} := \{y \in \tilde{E}^n : g_{i1}(y) = \ldots = g_{ir(i)}(y) = 0\}$, then the $V_{i,E}$ are the absolutely irreducible components of $V_{E,x}$.*

We now claim: *$q(T)$ is also irreducible in $F[T]$, and the absolutely irreducible components of $V_{F,x}$ are exactly the $V_{i,F} := \{y \in \tilde{F}^n : g_{i1}(y) = \ldots = g_{ir(i)}(y) = 0\}$ $(1 \leqq i \leqq k)$, where q and the g_i and g_{ij} are as in* (i), (ii) *and* (iii) *above.*

To see this, note that if q would factor into two monic polynomials over F, then the coefficients of these factors would be algebraic over E, hence would belong to E. The statement about absolutely irreducible components follows from the fact that "absolute irreducibility of an algebraic set" can be expressed as a quantifier free condition on the coefficients of defining polynomials in the language of rings. More precisely we have the following general lemma, which we shall also need further on:

(1.12) Lemma. *There are quantifier-free formulas $AI(X)$ and $\mathrm{Dim}_d(X)$, $d \in \{-\infty, 0, \ldots, n\}$, in the language of rings such that for each field F and $x \in F^m$ we have:*

(i) *$V_{F,x} \subseteq \tilde{F}^n$ is absolutely irreducible $\Leftrightarrow$ $F \models AI(x)$;*

(ii) *$\dim(V_{F,x}) = d \Leftrightarrow F \models \mathrm{Dim}_d(x)$.*

These well-known results go back in one way or another to Kronecker. For modern treatments of this and similar properties, cf. [7], Ch. 0, §9, or [4].

(1.13) Resuming the discussion of (1.11), let R be the subring of F generated by $x_1, \ldots, x_m$ and $\bar{R}$ its integral closure in E, and note that E is the fraction field of $\bar{R}$. Hence by changing α we can take q and the g_{ijv}'s to have coefficients in R.

Suppose now that F is equipped with root functions. Then one easily checks that $\bar{R} = \{\tau(x) : \tau(X) \text{ an } L_Q\text{-term}\}$. Hence q can be taken of the form $q(x, T)$, where $q(X, T)$ is a term in the language L_Q that is polynomial and monic in the variable T. This leads us to the following definition. Write $f := (f_1, \ldots, f_r)$.

Definitions. (i) A *potential decomposition for f over F* is a tuple

$$\mathscr{D} := \big(q(X, T), g_1(X, Y), \ldots, g_k(X, Y)\big)$$

such that

(D1) $q(X, T)$ is an L_Q-term that is polynomial and monic in T, say of degree $N > 0$;

(D2) each g_i is a tuple $\big(g_{ijv}(X, Y)\big)_{1 \leqq j \leqq r(i),\, 1 \leqq v \leqq N}$ of L_Q-terms that are polynomial in Y (its "coefficients" $c(X)$ may involve root symbols).

(ii) Let $\mathscr{D}$ be a potential decomposition for f over F as in (i).

Then $\mathscr{D}$ is a *decomposition for f over F at the point $x \in F^m$* if

(D3) $q(x, T) \in F[T]$ is separable and irreducible;

(D4) if $\alpha \in \tilde{F}$ is a zero of $q(x, T)$ and we set $g_{ij} := \sum g_{ijv}(x, Y)\alpha^{v-1} \in F(\alpha)[Y]$ and $V_i := V(g_{i1}, \ldots, g_{ir(i)}) \subseteq \tilde{F}^n$, then the V_i are exactly the absolutely irreducible components of $V_{F,x} \subseteq \tilde{F}^n$.

Note that (D1) and (D2) are purely syntactic conditions, and that these definitions are relative to the data F and $f = (f_1, \ldots, f_r) \in \mathbb{Z}[X, Y]^r$.

The above discussion leads to the following conclusions, where F denotes an arbitrary field with root functions and x ranges over F^m.

(1) *If $\mathscr{D} = (q, g_1, \ldots, g_k)$ is a decomposition for f over F at x, then we have, with the notations above, and $V' := V'_{F,x}$:*

$$V' = V(\{\prod_{1 \leq i \leq k} g_{ij(i)v(i)}(x, Y) : j \text{ and } v \text{ are functions on } \{1, \ldots, k\},$$
$$1 \leq j(i) \leq r(i),\ 1 \leq v(i) \leq N\}).$$

(2) *There is a decomposition for f over F at x.*

(3) *Given a potential decomposition $\mathscr{D} = (q, g_1, \ldots, g_k)$ for f there is a quantifier free L_Q-formula* $\mathrm{Dec}_{\mathscr{D},f}(X)$ *(independent of F and x) such that*

$$\mathscr{D} \text{ is a decomposition for } f \text{ over } F \text{ at } x \Leftrightarrow F \models \mathrm{Dec}_{\mathscr{D},f}(x).$$

(4) *There are finitely many potential decompositions $\mathscr{D}(1), \ldots, \mathscr{D}(J)$ for f, such that for each F and x one of $\mathscr{D}(1), \ldots, \mathscr{D}(J)$ is an actual decomposition for f over F at x.*

Note that (3) follows from lemmas (1.10) and (1.12), and that (4) follows from (2) and (3) by model-theoretic compactness.

(1.14) By (1) and (4) above there is a "quantifier-free" construction that for input $V_{F,x} = V(f_1(x, Y), \ldots, f_k(x, Y)) \subseteq \tilde{F}^n$ gives output $V'_{F,x}$; which of the potential decompositions $\mathscr{D}(1), \ldots, \mathscr{D}(J)$ can be used depends by (3) on which of the conditions $\mathrm{Dec}_{\mathscr{D}(j),f}(x)(1 \leq j \leq J)$ holds in F.

We can now take $V'_{F,x}$ (that is, its defining polynomials $\prod g_{ij(i)v(i)}(x, Y)$) as new input and construct in the same way $V''_{F,x}$. Repeating this procedure n times we arrive by (1.5) at the F-absolute kernel $V^*_{F,x}$ of $V_{F,x}$. Roughly speaking, we have given a construction of $V^*_{F,x}$

that is piecewise uniform in the parameter x. Here is a precise formulation of this piecewise uniformity.

(1.15) Theorem. *For each field F with root functions we have a covering of F^m by finitely many sets $C_1, \ldots, C_I$, such that for $x \in C_i$ the absolutely irreducible components of $V^*_{F,x}$ are exactly the $M(i)$ distinct sets $V(h_{i1}(x, Y)), \ldots, V(h_{iM(i)}(x, Y))$. Here $I \in \mathbb{N}$ and the function $M: \{1, \ldots, I\} \to \mathbb{N}$ are independent of F, each set $C_i \subseteq F^m$ is defined in F by a quantifier free L_Q-formula $c_i(X)$ that is independent of F, and each $h_{ij}(X, Y)$ is a finite tuple, independent of F, of L_Q-terms in (X, Y) that are polynomial in Y. (Note that $M(i) = 0$ means that $V^*_{F,x}$ is empty for all $x \in C_i$.)*

(1.16) Note that proposition (1.7) is an immediate consequence of this theorem. Another consequence that will be needed later on is the following.

Let $1 \leqq \mu \leqq \max\{M(i): 1 \leqq i \leqq I\}$ and let $d \in \{0, \ldots, n\}$. Then the set of $x \in F^m$ such that $\dim(V^*_{F,x}) = d$ and $V^*_{F,x}$ has exactly μ absolutely irreducible components of maximal dimension d is defined in F by an L-formula $S_{f,d,\mu}(X)$ that does not depend on the field F.

To see this, note that by (1.12) and by the theorem this subset of F^m is certainly defined in the *field F with root functions* by an L_Q-formula independent of F. But this subset of F^m depends only on the field structure of F and not on the particular root functions of F. Hence by pure logic alone the subset must be definable in F by an L-formula independent of F.

§ 2. Positive quantifier elimination for enriched finite fields

(2.1) Let F be a perfect field with algebraic closure $\tilde{F}$, and suppose F has for each integer $n > 1$ exactly one field extension F_n such that $F \subseteq F_n \subseteq \tilde{F}$ and $[F_n : F] = n$. (Each finite field has this property.) It follows easily that $F_n | F$ is then a cyclic Galois extension. Fix for each $n > 1$ a generator α_n of F_n so that $F_n = F(\alpha_n)$, and let

$$f_n(T) = T^n + c_{n1} T^{n-1} + \ldots + c_{nn}$$

be the minimum polynomial of α_n over F.

(2.2) Let further $g(T) = a_0 + a_1 T + \ldots + a_d T^d \in F[T]$ be of degree $d > 1$. We want to find an *existential* condition on the coefficients $a_0, \ldots, a_d$ that is equivalent to the *universal* condition that g has no zero in F. We will see this is possible provided we use $c_{n1}, \ldots, c_{nn}$ as extra constants, where $n = d!$. With this value for n the polynomial $g(T)$ splits into linear factors over $F(\alpha_n)$, hence:

(1) $$F \models \neg \exists t\, g(t) = 0$$

if and only if

(2) there are $y_1, \ldots, y_d$ in $F(\alpha_n) \setminus F$ such that $F(\alpha_n) \models \phi_d(a, y)$ where the formula $\phi_d(a, y)$ is the conjunction of $d+1$ equations expressing that the polynomials $g(T)$ and $a_d \prod (T - y_j)$ are equal, $a = (a_0, \ldots, a_d)$, $y = (y_1, \ldots, y_d)$.

Now each element of $F(\alpha_n)$ can be coded by the n-tuple from F consisting of its coefficients relative to the basis $1, \alpha_n, \ldots, \alpha_n^{n-1}$. In this way one codes the field $F(\alpha_n)$ in the field F. Write each y_j from (2) as $y_j = z_{0j} + z_{1j}\alpha_n + \ldots + z_{n-1\,j}\alpha_n^{n-1}$ with $z_{ij} \in F$. Then the condition that $y_j \notin F$ can be expressed as $F \models \bigvee_{1 \leqq i \leqq n-1} z_{ij} \neq 0$.

If follows that (2) can also be equivalently expressed as

$$F \models \exists z \Big(\bigwedge_{1 \leqq j \leqq d} \Big(\bigvee_{1 \leqq i \leqq n-1} z_{ij} \neq 0 \Big) \Big) \,\&\, \psi_d(a, c_n, z), \tag{3}$$

where $z = (z_{ij})_{0 \leqq i \leqq n-1,\, 1 \leqq j \leqq d}$ and $c_n = (c_{n1}, \ldots, c_{nn})$, and $\psi_d(u_0, \ldots, u_d, v_1, \ldots, v_n, z)$ is a certain conjunction of equations in the indicated variables. The equations are in the language of rings; $\psi_d(u, v, z)$ depends only on d, not on the particular field F or choice of generator α_n or on the polynomial $g(T)$.

It is especially important that $c_{n1}, \ldots, c_{nn}$ can be replaced in (3) by the coefficients $b_1, \ldots, b_n$ of any other monic irreducible polynomial $T^n + b_1 T^{n-1} + \ldots + b_n$ over F. The equivalence of (1) and (3) is of the desired form. (Although we shall not use it we note that a similar equivalence holds for each perfect field F that has for each $n > 1$ only finitely field extensions of degree n inside $\tilde{F}$.)

(2.3) Recall that a *pseudo-algebraically closed* field (or PAC-field) is by definition a field F such that for each absolutely irreducible polynomial $f(X_1, X_2) \in F[X_1, X_2]$ there is a point $(x_1, x_2) \in F^2$ on the curve $f(X_1, X_2) = 0$.

It follows from Weil's famous theorem on curves over finite fields that all infinite models of the theory of finite fields are PAC-fields. Below we need the following result from [3] on PAC-fields. (This is a minor exception to our assertion in the introduction that the proof of our Main Theorem is selfcontained modulo the Lang-Weil estimates; the exception is minor since [3] is short, and elementary modulo Weil's theorem.)

(2.4) *Let $\phi(X)$ be an existential formula in the language of rings. Then $\phi(X)$ is equivalent, uniformly for all perfect* PAC*-fields, to a conjunction of formulas $\exists T(g(X, T) = 0)$, with $g(X, T) \in \mathbb{Z}[X, T]$, T a single variable.*

(2.5) We define a *pseudo-finite* field to be a perfect PAC-field that has for each $n > 1$ exactly one field extension of degree n inside its algebraic closure.

By the remark in (2.3) we have: *the infinite models of the theory of finite fields are pseudo-infinite fields*. The converse of this statement also holds (and usually serves as the definition of "pseudo-finite field") but is not needed in the proof of our Main Theorem. (Later in this paper, when dealing with applications and axiomatization questions, we shall freely use this conserve, which is due to Ax [1].)

(2.6) We now enrich the language L of rings with extra constant symbols $c_{n1}, \ldots, c_{nn}$, for each $n > 1$, and obtain the language $L(c)$. We consider *enriched finite fields*: these are

the $L(c)$-structures that are finite fields F in which for each $n > 1$ the symbols $c_{n1}, \ldots, c_{nn}$ are interpreted as the coefficients of an irreducible monic polynomial

$$T^n + c_{n1} T^{n-1} + \ldots + c_{nn}$$

over F. In the same way we define enriched pseudo-finite fields. Each finite or pseudo-finite field can be so enriched in several ways.

(2.7) Proposition. *Each $L(c)$-formula $\phi(X)$ is equivalent, uniformly for all enriched pseudo-finite fields, to a conjunction of formulas $\exists T(g(c, X, T) = 0)$, with*

$$g(C, X, T) \in \mathbb{Z}[C, X, T], \quad C = (C_{ni})_{n>1, 1 \leqq i \leqq n}.$$

Such an equivalence also holds for all sufficiently large enriched finite fields.

Proof. We need only prove the first part of the proposition since the second part follows from it by pure logic. For existential ϕ the desired result is a consequence of (2.4). Hence by simple logic, it suffices to show that each negation $\neg \exists T(g(c, X, T) = 0)$ is equivalent to an existential formula (uniformly for all pseudo-finite fields). This follows easily from the equivalence between (1) and (3) in (2.2) above. In that equivalence the degree d of the polynomial $g(T)$ was given. To apply the equivalence to the $L(c)$-formula $\neg \exists T(g(c, X, T) = 0)$, write $g(C, X, T) = \sum a_j(C, X) T^j$. By making the substitution $C \to c$ and interpreting X by a tuple x in a pseudo-finite field a finite number of cases for the degree of the polynomial $g(c, x, T)$ arise, and one takes a disjunction over these possibilities. □

(2.8) The following results combine a property of the F-absolute kernel from section 1 with our positive quantifier elimination. It is not needed for the proof of the Main Theorem, but useful in applications of the Main Theorem. We shall find it convenient to write $V(F)$ for $V \cap F^k$, where $V \subseteqq \tilde{F}^k$ is an F-algebraic set.

(2.9) Lemma. *Let F be a pseudo-finite field and $S \subseteqq F^m$ definable in F using constants. Then for some integers $e, n \in \mathbb{N}$ the set S is a finite union of sets of the form $\pi(V(F))$ with V an F-algebraic subset of $\tilde{F}^{m+n}$, $\pi : \tilde{F}^{m+n} \to \tilde{F}^m$ the projection on the first m coordinates, and such that for all $x \in \tilde{F}^m$ the set $V_x := \{y \in \tilde{F}^n : (x, y) \in V\}$ is finite of cardinality $\leqq e$.*

Proof. By (2.7) we may assume S is defined by a conjunction of formulas

$$\exists T f(X, T) = 0 \tag{1}$$

where $f(X, T) \in F[X, T]$, $X = (X_1, \ldots, X_m)$ and T a single variable.

It may happen that for certain $x \in F^m$ we have $f(x, T) = 0$ and we take care of this as follows. Write $f(X, T) = \sum f_i(X) T^i$ and note that then (1) is equivalent to

$$\left(\bigwedge f_i(X) = 0\right) \vee \left(\exists T \exists U \left(f(X, T) = 0 \,\&\, \left(\Pi \left(f_i(X) \cdot U - 1\right) = 0\right)\right)\right). \tag{2}$$

Working out the conjunction of the formulas (2) by means of the distributive law we see that the conjunction of the formulas (1) is equivalent to a disjunction of formulas of the form

$$(3) \qquad \left(\bigwedge g_j(X) = 0\right) \& \exists Y \left(\bigwedge h_k(X, Y_k) = 0\right)$$

where $g_j \in F[X]$ and $h_k \in F[X, Y_k]$, $1 \leqq k \leqq n$, $Y = (Y_1, \ldots, Y_n)$, and there is $e \in \mathbb{N}$ such that for each $x \in \tilde{F}^m$ we have: $\operatorname{card}\{y \in \tilde{F}^n : h_k(x, y_k) = 0 \text{ for all } k\} \leqq e$. (We can take the same e and n for each disjunct (3).) For each disjunct (3) we take the F-algebraic set $V := V((g_j), (h_k)) \subseteqq \tilde{F}^{m+n}$ and we note that S is the union of the sets $\pi(V(F))$. □

For $m = 1$ we can draw a further useful conclusion.

(2.10) Lemma. *Let F be a pseudo-finite field and $S \subseteqq F$ an infinite set definable in F using constants. Then there is an absolutely irreducible polynomial $f(X, T)$ in $F[X, T] \setminus F[X]$ such that S contains the infinite set $\{x \in F : f(x, t) = 0$ for some $t \in F\}$.*

Proof. By the previous lemma S contains an infinite set of the form $\pi(C(F))$ where $C \subseteqq \tilde{F}^{1+n}$ is an absolutely irreducibe F-algebraic set, and there is $e \in \mathbb{N}$ such that for each $x \in \tilde{F}$ there are at most e points $y \in \tilde{F}^n$ with $(x, y) \in C$. Hence $\dim(C) = 1$; let $\mathfrak{p}$ be the ideal of polynomials in $F[X, Y]$ that vanish on C, so $\mathfrak{p}$ is an absolutely prime ideal. (Here we use that F is perfect.) Then the function field of C over F is the fraction field $F(X, y)$ of $F[X, Y]/\mathfrak{p}$, where we put $y := Y \bmod \mathfrak{p}$ and identify X with $X \bmod \mathfrak{p}$. The identification is allowed since $\pi(C(F))$ is infinite, so that the canonical map $F[X, Y] \to F[X, Y]/\mathfrak{p}$ is injective on $F[X]$. The field $F(X, y)$ is algebraic over $F(X)$ (since $\dim(C) = 1$) and $F(X)$ has degree of imperfectness at most 1, hence $F(X, y) = F(X, \alpha)$ for a single α, and we can even take α such that $y_1, \ldots, y_n \in F[X, \alpha]$. Let $f(X, T) \in F[X, T]$ be irreducible with $f(X, \alpha) = 0$. Then f is easily seen to have the desired properties. □

(2.11) We can now show that each infinite definable subset of a pseudo-finite field has the same cardinality as the field: there are no Vaughtian pairs of pseudo-finite fields. In fact we have a stronger result, which implies that each pseudo-finite field is the definable closure of each of its infinite definable subsets, and which also gives once more an answer to problem (*) in the beginning of the introduction.

(2.12) Proposition. *Let F be a pseudo-finite field and $S \subseteqq F$ an infinite set definable in F using constants. Then each element of F is of the form $a + b + cd$ with $a, b, c, d \in S$.*

Proof. By the last lemma we may reduce to the case that for some absolutely irreducible $f(X, T)$ in $F[X, T] \setminus F[X]$ we have $S = \{x \in F : f(x, t) = 0 \text{ for some } y \in F\}$. Let $e \in F$. The idea is to find elements a and c in S such that the two equations

$$f(X, T) = f(e - a - cX, T') = 0$$

in the unknowns (X, T, T') define an absolutely irreducible F-algebraic set.

Then there will be an F-point (d, t, t') on this variety, so that $d \in S$ and $b := e - a - cd \in S$, hence $e = a + b + cd$, as desired.

As in the proof of the last lemma, let $F[X, \tau] := F[X, T]/(f)$ where $\tau := T \bmod (f)$ and X is identified with its image in $F[X, T]/(f)$. Then $F(X, \tau)$ is the function field of the curve $f(X, T) = 0$ over F, and similarly $\tilde{F}(X, \tau)$ is the function field of this curve over $\tilde{F}$.

We now apply a strong form of Hilbert's irreducibility theorem for function fields to the irreducible polynomial $f(X', T')$ over the function field $\tilde{F}(x, \tau)$, namely Theorem 3.4 from Roquette [12]. Since S is infinite, this theorem gives us $a, c \in S$ such that the polynomial $f(e - a - cX, T') \in \tilde{F}(X, \tau)[T']$ is irreducible. Hence the two equations

$$f(X, T) = f(e - a - cX, T') = 0$$

define an irreducible $\tilde{F}$-algebraic set, and therefore an absolutely irreducible F-algebraic set, as required. □

(2.13) We conclude this section with a remark on an alternative definition of the F-absolute kernel V^* of V when $V \subseteq \tilde{F}^m$ is an F-algebraic set, and F is a PAC-field: in this case V^* is simply the Zariski closure in $\tilde{F}^m$ of $V(F)$. This follows easily from the properties (1), (2) and (3) mentioned in (1.3), and [6], proposition 10.1.

§ 3. The main theorem

(3.1) In this section k denotes an arbitrary but fixed finite field of cardinality q, so $k \cong \mathbb{F}_q$.

(3.2) Let $f = (f_1, \ldots, f_r) \in k[Y]^r$, $Y = (Y_1, \ldots, Y_n)$. We call f *of degree* $\leqq e$ (where $e \in \mathbb{N}$) if each polynomial $f_i(Y)$ is of total degree $\leqq e$ in Y.

We set

$$V := V(f_1, \ldots, f_r) = \{y \in \tilde{k}^n : f(y) = 0\},$$

and

$$V(k) := V \cap k^n = \{y \in k^n : f(y) = 0\},$$

so $\operatorname{card}(V(k)) \leqq q^n$.

Our starting point is the following theorem of Lang & Weil [10]:

Let f be of degree $\leqq e$. Then there is a positive constant C depending only on (e, n, r) (not on k or the particular polynomials $f_1, \ldots, f_r$) such that if V is absolutely irreducible and $\dim(V) = d$, *then*

$$|\operatorname{card}(V(k)) - q^d| \leqq Cq^{d-(1/2)}.$$

Actually the Lang-Weil theorem is more explicit, but we shall not use this extra precision. We also remark that the Lang-Weil theorem is a relatively elementary consequence of Weil's earlier theorem on curves over finite fields.

Our first step is to get Lang-Weil type estimates for the set of k-points on a k-algebraic set that is not necessarily absolutely irreducible.

(3.3) Proposition. *Let f be of degree $\leqq e$. Then there is a positive constant C and a natural number M, both depending only on (e, n, r), such that if $V(\mathfrak{k}) \neq \emptyset$, then*

$$|\operatorname{card}(V(\mathfrak{k})) - \mu q^d| \leqq C q^{d-(1/2)},$$

for some $d \in \{0, \ldots, \dim(V)\}$ and some $\mu \in \{1, \ldots, M\}$.

Proof. By induction on $\dim(V)$. Assume $V(\mathfrak{k}) \neq \emptyset$. Let V^* be the result of the intersection-decomposition procedure applied to V over $\mathfrak{k}$, and let $V_1, \ldots, V_s$ be the distinct absolutely irreducible components of V^*, so $V(\mathfrak{k}) = V_1(\mathfrak{k}) \cup \ldots \cup V_s(\mathfrak{k})$. By Proposition (1.7) the number s is bounded by a natural number M depending only on (e, n, r). By rearranging we may assume that $V_1, \ldots, V_\mu$ are of maximal dimension

$$d = \dim(V^*) \leqq \dim(V),$$

while $\dim(V_j) < d$ for $\mu < j \leqq s$.

We claim that then for these values of d and μ we have:

$|\operatorname{card}(V(\mathfrak{k})) - \mu q^d| \leqq C q^{d-(1/2)}$, for a positive constant C depending only on (e, n, r).

Clearly this claim implies the desired result. To see why the claim holds, note that by (1.7) each V_j is of the form $V(h_1, \ldots, h_R)$ for polynomials $h_1, \ldots, h_R \in \mathfrak{k}[Y]$ of degree $\leqq E$, where R and E only depend on (e, n, r). By the Lang-Weil theorem this gives:

(1) $|\operatorname{card}(V_j(\mathfrak{k})) - q^d| \leqq C_1 q^{d-(1/2)}$ for $j \in \{1, \ldots, \mu\}$ and a positive constant C_1 that depends only on (E, n, R) and hence only on (e, n, r);

(2) $|\operatorname{card}(V_j(\mathfrak{k}))| \leqq C_2 q^{d-1}$ for $\mu < j \leqq s$ and a positive constant C_2 that depends only on (E, n, R) and hence only on (e, n, r).

Let $1 \leqq j(1) < j(2) \leqq s$. Then $V_{j(1)}$ and $V_{j(2)}$ are different absolutely irreducible $\mathfrak{k}$-algebraic sets, hence their intersection is a $\mathfrak{k}$-algebraic set of dimension $< d$, and we have $2R$ defining polynomials over $\mathfrak{k}$ for this intersection, and their degrees are all bounded by E. Hence by the inductive hypothesis:

(3) $|\operatorname{card}(V_{j(1)}(\mathfrak{k}) \cap V_{j(2)}(\mathfrak{k}))| \leqq C_3 q^{d-1}$ for a positive constant C_3 that depends only on (E, n, R) and hence only on (e, n, r).

Our claim now follows by combinating (1), (2) and (3). □

(3.4) For later purposes we add some extra precision to this result.

Let now $f = (f_1, \ldots, f_r) \in \mathbb{Z}[X, Y]^r$ with $X = (X_1, \ldots, X_m)$ as parametric variables and $Y = (Y_1, \ldots, Y_n)$. Say the f_i's are all of degree $\leqq e$ in Y. Then Proposition (3.3) applies in particular to $f(x, Y) := (f_1(x, Y), \ldots, f_r(x, Y)) \in \mathfrak{k}[Y]^r$, for each finite field $\mathfrak{k}$ and $x \in \mathfrak{k}^m$. Set $V_x := \{y \in \tilde{k}^n : f(x, y) = 0\}$ and $V_x(\mathfrak{k}) := \{y \in \mathfrak{k}^n : f(x, y) = 0\}$ $(x \in \mathfrak{k}^m)$.

Here is the additional information:

Let C and M be constants as in the proposition, and let $d \in \{0, \ldots, n\}$ and $\mu \in \{1, \ldots, M\}$. Then the set of $x \in \mathfrak{k}^m$ such that $|\operatorname{card}(V_x(\mathfrak{k})) - \mu q^d| \leqq Cq^{d-(1/2)}$ is defined in the field $\mathfrak{k}$ by an L-formula $S_{f,d,\mu}(X)$ that is independent of $\mathfrak{k}$.

This follows from the particular way we obtained μ and d in the proof of (3.3), together with the remarks made in (1.16). We also observe that if $q = \operatorname{card}(\mathfrak{k})$ is sufficiently large compared to the constant C, then there is for each $x \in \mathfrak{k}^m$ with $V_x(\mathfrak{k}) \neq \emptyset$ exactly one pair $(d, \mu) \in \{0, \ldots, n\} \times \{1, \ldots, M\}$ such that $\mathfrak{k} \models S_{f,d,\mu}(x)$, while if $V_x(\mathfrak{k}) = \emptyset$ there is no such pair.

Next we extend the result to quantifier free formulas.

(3.5) Lemma. *Let $\phi(X, Y)$ be a quantifier free L-formula. Then there is a positive constant C and a natural number M, both depending only on ϕ and not on $\mathfrak{k}$, such that if $x \in \mathfrak{k}^m$ and $\phi(x, \mathfrak{k}^n) \neq \emptyset$, then $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leqq Cq^{d-(1/2)}$ for some $d \in \{0, \ldots, n\}$ and some $\mu \in \{1, \ldots, M\}$.*

Proof. By disjunctive normal form manipulations we see that ϕ is equivalent to a disjunction $\bigvee_{1 \leqq \nu \leqq N} (f_\nu(X, Y) = 0 \,\&\, g_\nu(X, Y) \neq 0)$, where $f_\nu(X, Y) \in \mathbb{Z}[X, Y]^{r(\nu)}$, $g_\nu(X, Y], \in \mathbb{Z}[X, Y]$ and where moreover any two different disjuncts are "disjoint", in the sense of defining disjoint sets in every field. Now let $Y' := (Y_{n+1}, \ldots, Y_{n+N})$ be a tuple of new variables, and let $\phi'(X, Y, Y')$ be the formula

$$\bigvee_{1 \leqq \nu \leqq N} \left(f_\nu(X, Y) = 0 \,\&\, g_\nu(X, Y) \cdot Y_{n+\nu} = 1 \,\&\, \bigwedge_{\lambda \neq \nu} Y_{n+\lambda} = 0\right).$$

Then $\phi'(X, Y, Y')$ is a *positive* quantifier-free formula, and is therefore for fields equivalent to a conjunction of polynomial equations in (X, Y, Y'). Hence we can apply Proposition (3.3) to the sets $\phi'(x, \mathfrak{k}^{n+N})$. Since clearly $\phi'(x, \tilde{\mathfrak{k}}^{n+N})$ has dimension $\leqq n$, it follows that there is a positive constant C and a natural number M, both depending only on ϕ' and hence on ϕ, such that if $x \in \mathfrak{k}^m$ and $\phi'(x, \mathfrak{k}^{n+N}) \neq \emptyset$, then

$$|\operatorname{card}(\phi'(x, \mathfrak{k}^{n+N})) - \mu q^d| \leqq Cq^{d-(1/2)} \text{ for some } d \in \{0, \ldots, n\} \text{ and } \mu \in \{1, \ldots, M\}.$$

Because any two different disjuncts in the disjunctions above are disjoint we have for each $x \in \mathfrak{k}^m$ a bijection $(y, y') \to y : \phi'(x, \mathfrak{k}^{n+N}) \to \phi(x, \mathfrak{k}^n)$. Hence C and M as above have the desired property. □

(3.6) As before we have an additional result:

Let C and M be constants as in the lemma, and let $d \in \{0, \ldots, n\}$ and $\mu \in \{1, \ldots, M\}$. Then the set of $x \in \mathfrak{k}^m$ such that $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leqq Cq^{d-(1/2)}$ is defined in the field $\mathfrak{k}$ by an L-formula $\phi_{d,\mu}(X)$ that is independent of $\mathfrak{k}$.

(3.7) Main Theorem. *Let $\phi(X, Y)$ be an arbitrary L-formula. Then there is a positive constant C and a finite set D of pairs (d, μ) with $d \in \{0, \ldots, n\}$ and μ a positive rational such*

that if $x \in \mathfrak{k}^m$ *and* $\phi(x, \mathfrak{k}^n) \neq \emptyset$, *then* $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leqq C q^{d-(1/2)}$ *for some* $(d, \mu) \in D$. *The constant* C *and the set* D *depend only on* ϕ *and not on* $\mathfrak{k}$.

Remark. In the introduction we gave the example "Y is a square" to show that in contrast with (3.3) and (3.5) we cannot require μ to be an integer. It suffices to prove the Main Theorem for $q = \operatorname{card}(\mathfrak{k})$ greater than some constant depending only on ϕ, since we can always enlarge the constant C to take care of the exceptional $\mathfrak{k}$'s.

Proof. By (2.7) the formula ϕ is equivalent, for all sufficiently large *enriched* finite fields, to a conjunction of formulas

$$\exists T\, g(X, Y, T) = 0\,, \tag{1}$$

where $g(X, Y, T)$ is a term in the enriched language. Each such term g can be written as $G(X, c, Y, T)$ where $c := (c_1, \ldots, c_M)$ is a tuple of new constant symbols from the enriched language, and $G(X, X', Y, T) \in \mathbb{Z}[X, X', Y, T]$, with $X' = (X'_1, \ldots, X'_M)$. We may assume c is the same for all conjuncts (1). It is easy to see that it suffices to prove the desired result for the conjunction of the formulas $\exists T\, G(X, X', Y, T) = 0$ that correspond to the conjuncts (1). (That is, we replace the constants c_i by extra parametric variables X'_i.) But in order not to complicate notations, we may as well assume that ϕ is already a conjunction of formulas (1) such that $g(X, Y, T) \in \mathbb{Z}[X, Y, T]$, T a single variable, so g is free of the new constant symbols from the enriched language.

It may happen that for certain $(x, y) \in \mathfrak{k}^{m+n}$ we have $g(x, y, T) = 0$, and we take care of this as follows. Write $g(X, Y, T) = \sum g_i(X, Y) T^i$ and note that (1) is equivalent to

$$\left(\bigwedge g_i(X, Y) = 0\right) \vee \left(\exists T\, g(X, T) = 0 \,\&\, \exists U \prod \left(g_i(X, Y) \cdot U - 1\right) = 0\right) \tag{2}$$

and that the two disjuncts are disjoint (:= define disjoint sets in every field). Working out the conjunction of the formulas (2) by means of the distributive law, we see that $\phi(X, Y)$ is equivalent to a disjunction of formulas of the form

$$f(X, Y) = 0 \,\&\, \exists Z \left(\bigwedge h_j(X, Y, Z_j) = 0\right), \tag{3}$$

where $f \in \mathbb{Z}[X, Y]^r$, $h_j \in \mathbb{Z}[X, Y, Z_j]$ for $1 \leqq j \leqq k$, $Z = (Z_1, \ldots, Z_k)$, such that any two distinct disjuncts (3) in ϕ are disjoint. Moreover, each such disjunct (3) has a bound on the number of solutions in Z, that is, there is a natural number e with the property:

(4) for each field F and $(x, y) \in F^{m+n}$ there are at most e points $(z_1, \ldots, z_k) \in F^k$ such that $F \models \Psi(x, y, z)$ where $\Psi(X, Y, Z) := f(X, Y) = 0 \,\&\, \bigwedge_j h_j(X, Y, Z_j) = 0$.

Therefore we may reduce to the following situation:

ϕ is a formula (3), *and a number* $e \in \mathbb{N}$ *is given with property* (4). *We may and shall also assume that* $q = \operatorname{card}(\mathfrak{k})$ *is sufficiently large, depending on* ϕ.

By (3.5) there is a positive constant A and an integer $N \geqq 1$ (both only depending on Ψ and hence only on ϕ, but independent of k) such that if $x \in k^m$ and $\Psi(x, k^{n+k}) \neq \emptyset$, then

$$|\operatorname{card}(\Psi(x, k^{n+k})) - \mu q^d| \leqq A q^{d-(1/2)} \text{ for some } d \in \{0, \ldots, n+k\} \text{ and } \mu \in \{1, \ldots, N\}.$$

Let us fix momentarily such $x \in k^m$ with $\Psi(x, k^{n+k}) \neq \emptyset$, and let $d \in \{0, \ldots, n+k\}$ and $\mu \in \{1, \ldots, N\}$ have values such that the above estimate on $\operatorname{card}(\Psi(x, k^{m+k}))$ holds. Then we define

$$\begin{aligned} \mathscr{F} &:= \phi(x, k^n); \\ \mathscr{F}_j &:= \{y \in k^n : \operatorname{card}(\Psi(x, y, k^k)) = j\} \quad \text{for } j = 1, \ldots, e; \\ \mathscr{G} &:= \Psi(x, k^{n+k}). \end{aligned}$$

Hence by (4) and the definitions:

$$\begin{aligned} (5) \qquad \operatorname{card}(\mathscr{F}) &= \operatorname{card}(\mathscr{F}_1) + \operatorname{card}(\mathscr{F}_2) + \ldots + \operatorname{card}(\mathscr{F}_e), \\ \operatorname{card}(\mathscr{G}) &= \operatorname{card}(\mathscr{F}_1) + 2 \cdot \operatorname{card}(\mathscr{F}_2) + \ldots + e \cdot \operatorname{card}(\mathscr{F}_e), \\ |\operatorname{card}(\mathscr{G}) - \mu q^d| &\leqq A q^{d-(1/2)}, \end{aligned}$$

so that $\operatorname{card}(\mathscr{F}) \geqq \operatorname{card}(\mathscr{G})/e$, and therefore

$$(6) \qquad \operatorname{card}(\mathscr{F}) \geqq (\mu/e) q^d - (A/e) q^{d-(1/2)};$$

hence $0 \leqq d \leqq n$, since q is large.

To get an estimate on $\operatorname{card}(\mathscr{F}_j)$ we consider the quantifier free formulas

$$\Psi_j(X, Y, Z^1, \ldots, Z^j) := \bigwedge_{1 \leqq i \leqq j} \Psi(X, Y, Z^i) \,\&\, \bigwedge_{i(1) \neq i(2)} Z^{i(1)} \neq Z^{i(2)}, \quad 1 \leqq j \leqq e,$$

where the $Z^i := (Z_1^i, \ldots, Z_k^i)$ are k-tuples of new variables, and $Z^{i(1)} \neq Z^{i(2)}$ is the disjunction expressing that some coordinate of $Z^{i(1)}$ differs from the corresponding coordinate of $Z^{i(2)}$. Put $\mathscr{H}_j := \Psi_j(x, k^{n+jk})$. Observe that each point $y \in \mathscr{F}_j$ gives rise to $j!$ points in $\mathscr{H}_j$, and more generally for $0 \leqq t \leqq e-j$, each $y \in \mathscr{F}_{j+t}$ gives rise to

$$j![(j+t)!/j!\,t!] = (j+t)!/t!$$

points in $\mathscr{H}_j$. Hence

$$\operatorname{card}(\mathscr{H}_j) = j! \operatorname{card}(\mathscr{F}_j) + (j+1)! \operatorname{card}(\mathscr{F}_{j+1}) + \ldots + (e!/(e-j)!) \operatorname{card}(\mathscr{F}_e), \quad 1 \leqq j \leqq e.$$

Solving for $\operatorname{card}(\mathscr{F}_1), \ldots, \operatorname{card}(\mathscr{F}_e)$ from these equations and using (5) we get

$$\begin{aligned} (7) \qquad &\operatorname{card}(\mathscr{F}) = r_1 \operatorname{card}(\mathscr{H}_1) + \ldots + r_e \operatorname{card}(\mathscr{H}_e) \\ &\text{for rationals } r_1, \ldots, r_e \text{ depending only on } e. \end{aligned}$$

Next observe that $\operatorname{card}(\mathscr{H}_j) \leqq \text{constant} \cdot \operatorname{card}(\mathscr{G})$. Taking into account this inequality and the estimate in (5) we apply (3.5) to the quantifier free formula Ψ_j and obtain:

$$(8) \qquad |\operatorname{card}(\mathscr{H}_j) - \mu_j q^d| \leqq A_j q^{d-(1/2)}$$
$$\text{for some } \mu_j \in \{0, \ldots, M_j\} \text{ where } M_j \in \mathbb{N} \text{ and } A_j > 0.$$

Note that we allow here the possibility that $\mu_j = 0$; M_j and A_j depend only on Ψ_j and hence only on ϕ; which μ_j applies depends also on $\mathfrak{k}$ and $x \in \mathfrak{k}^m$. From (7) and (8):

$$(9) \qquad |\operatorname{card}(\mathscr{F}) - (r_1\mu_1 + \ldots + r_e\mu_e)q^d| \leqq C \cdot q^{d-(1/2)},$$
$$\text{with} \quad C := |r_1|A_1 + \ldots + |r_e|A_e.$$

From (6) we conclude that $r_1\mu_1 + \ldots + r_e\mu_e \geqq \mu/e > 0$, at least for sufficiently large $q = \operatorname{card}(\mathfrak{k})$. Since $r_1, \ldots, r_e$ are determined by e alone and there are only finitely many possibilities for $\mu_1, \ldots, \mu_e$ this finishes the proof. □

As before we have important additional information:

(3.8) Proposition. *Let C and D be as in the Main Theorem, and let $(d, \mu) \in D$. Then the set of $x \in \mathfrak{k}^m$ such that $|\operatorname{card}(\phi(x, \mathfrak{k}^n)) - \mu q^d| \leqq Cq^{d-(1/2)}$ is defined in the field $\mathfrak{k}$ by a formula $\phi_{d,\mu}(X)$ that is independent of $\mathfrak{k}$.*

This is easily traced back to the existence of similar formulas for the Ψ_j's in the proof of the Main Theorem. However, in the beginning of this proof we replaced certain constants c_i by extra parametric variables X_i', which is fortunately harmless, since the c_i''s are only subject to *definable* restrictions, see (2.6).

(3.9) Another interesting fact that emerges from the proof is that the denominators of the rationals μ can be bounded in terms of the "quantified variable complexity" of ϕ alone: the complexity with which the free variables $X_1, \ldots, X_m, Y_1, \ldots, Y_n$ occur in ϕ does not matter. We leave a precise statement of this fact and its proof to the reader.

(3.10) We now extend our Main Theorem to cardinalities of "quotients". Let $\phi(X, Y)$ and $\Psi(X, Y, Z)$ be formulas where $X = (X_1, \ldots, X_m)$ is a tuple of parametric variables and $Y = (Y_1, \ldots, Y_n)$ and $Z = (Z_1, \ldots, Z_n)$ have the same length.

Let $\mathfrak{k} = \mathbb{F}_q$ and $x \in \mathfrak{k}^m$, and suppose the set $\phi(x, \mathfrak{k}^n)$ is nonempty and $\Psi(x, \mathfrak{k}^n \times \mathfrak{k}^n)$ is an equivalence relation on $\phi(x, \mathfrak{k}^n)$. Denote the set of equivalence classes by

$$(\phi/\Psi)(x, \mathfrak{k}^n) \quad \text{(the quotient set)}.$$

Then we have the following estimates holding for all pairs $(\mathfrak{k}, x)$ that satisfy these assumptions.

(3.11) Corollary. *There is a positive constant $A = A(\phi, \Psi)$ and a finite set $B = B(\phi, \Psi)$ of pairs (f, ϱ) with $f \in \{0, \ldots, n\}$ and ϱ a positive rational such that*

$$|\operatorname{card}(\phi/\Psi)(x, \mathfrak{k}^n) - \varrho q^f| \leqq Aq^{f-(1/2)} \text{ for some } (f, \varrho) \in B.$$

The constant A and the set B can be taken independent of (ℓ, x).

Proof. The Main Theorem gives us a positive constant C and a finite set D of pairs (d, μ) with $d \in \{0, \ldots, n\}$ and $0 < \mu \in \mathbb{Q}$, such that for each equivalence class S we have

$$|\operatorname{card}(S) - \mu q^d| \leqq C q^{d-(1/2)} \tag{1}$$

for some pair $(d, \mu) \in D$. Here C and D depend only on ϕ and Ψ, not on (ℓ, x).

Fix a pair $(d, \mu) \in D$, and write $\operatorname{card}(S) \sim \mu q^d$, if estimate (1) holds. Let $U = U(d, \mu)$ be the union of the equivalence classes S for which $\operatorname{card}(S) \sim \mu q^d$. Keeping in mind that we have fixed (d, μ) it follows from (3.8) that the set U is definable, uniformly for all relevant pairs (ℓ, x). Then another application of the Main Theorem provides a positive constant $C' = C'(d, \mu)$ and a finite set $D' = D'(d, \mu)$ of pairs (e, ν) with $e \in \{0, \ldots, n\}$ and $0 < \nu \in \mathbb{Q}$ such that if $U \neq \emptyset$, then

$$|\operatorname{card}(U) - \nu q^e| \leqq C' q^{e-(1/2)} \tag{2}$$

for some $(e, \nu) \in D'$. (Again C' and D' depend on ϕ, Ψ, d and μ but not on (ℓ, x).)

Let $\bar{U} = \bar{U}(d, \mu)$ be the set of equivalence classes S with $\operatorname{card}(S) \sim \mu q^d$, so U is the union of the elements of $\bar{U}$. Assume that $U \neq \emptyset$ and let $(e, \nu) \in D'$ be such that estimate (2) holds. The idea is now that since each $S \in \bar{U}$ has cardinality roughly μq^d and their union U has cardinality roughly νq^e, there must be roughly $\nu q^e / \mu q^d = (\nu/\mu) q^{e-d}$ sets $S \in \bar{U}$. In fact we claim there is a positive constant C'' such that

$$|\operatorname{card}(\bar{U}) - (\nu/\mu) q^{e-d}| \leqq C'' \cdot q^{e-d-(1/2)}. \tag{3}$$

To show the existence of such a constant C'' we may as well assume that q is large, so that $e \geqq d$: $e < d$ would imply, by (1) and (2), that $\operatorname{card}(U) < \operatorname{card}(S)$ for large q and S an equivalence class contained in U, contradiction. Let $K = \operatorname{card}(\bar{U})$, and let $S_1, \ldots, S_K$ be the distinct elements of $\bar{U}$. Taking their union and using (1) we get

$$|\operatorname{card}(U) - K\mu q^d| \leqq KC q^{d-(1/2)},$$

hence

$$|\operatorname{card}(U)/\mu q^d - K| \leqq K \cdot (C/\sqrt{q}),$$

so that

$$\operatorname{card}(U)/\mu q^d = K(1-\varepsilon) \quad \text{with} \quad |\varepsilon| \leqq C/\sqrt{q} \leqq 1/2 \text{ for large } q.$$

Using this equality in (2) and dividing by μq^d we get

$$|K(1-\varepsilon) - (\nu/\mu) q^{e-d}| \leqq (C'/\mu) q^{e-d-(1/2)},$$

hence

$$|K - (\nu/\mu) q^{e-d}(1/1-\varepsilon)| \leqq \big(C'/\mu(1-\varepsilon)\big) q^{e-d-(1/2)}.$$

Since $1/(1-\varepsilon) = 1+\delta$ with $|\delta| \leqq 2C/\sqrt{q}$ for large q this implies an estimate

$$|K - (v/\mu)q^{e-d}| \leqq C'' q^{e-d-(1/2)} \text{ for large } q$$

for some positive constant C'' which depends only on ϕ and Ψ. This establishes (3). The desired result now follows by combining the estimate (3) for $\operatorname{card}(\bar{U}(d,\mu))$ with the fact that, for q sufficiently large, $(\phi/\Psi)(x, \mathcal{K}^n)$ is the *disjoint* union of the sets $\bar{U}(d,\mu)$ where (d,μ) varies over D. □

§ 4. Further applications of the Main Theorem

(4.1) Until this point we needed little of the existing body of logical results on finite and pseudo-finite fields. In particular, we simply *defined* a pseudo-finite field to be a perfect PAC-field that has for each $n > 0$ a unique extension field of degree n inside its algebraic closure. It then follows from Weil's theorem that each infinite model of the theory of finite fields is a pseudo-finite field. In this section and the next two we shall also freely use the converse, and some other results from Ax [1].

(1) *The pseudo-finite fields are exactly the infinite models of the theory of finite fields.* (Usually this is taken as the definition of "pseudo-finite field".)

(2) *The pseudo-finite fields of characteristic* 0 *are exactly the infinite models of the theory of finite prime fields* $\mathbb{F}_p$ (p prime).

(The proof of these results needs besides Weil's theorem another deep arithmetic fact, namely Cebotarev's density theorem.)

(4.2) Using (1) and (2) one can answer once more Felgner's original question, without using our Main Theorem: Suppose $\phi(Y)$ is a formula in the language of rings defining in each finite field of the form $\mathbb{F}_{q^2}$ the subfield $\mathbb{F}_q$. Let F be a characteristic 0 model of the theory of the fields $\mathbb{F}_{q^2}$. Then $\phi(Y)$ defines in F a proper subfield, but F is also a model of the theory of finite prime fields $\mathbb{F}_p$ by (2), so $\phi(Y)$ must define for infinitely many prime numbers p a proper subfield of $\mathbb{F}_p$, which is absurd. However, this kind of argument cannot prove the stronger assertion (*) mentioned in the introduction to this paper. What the argument does prove is the following:

There is no formula $\phi(Y)$ that defines in infinitely many finite fields of infinitely many different characteristics a proper subfield.

(This is of course also clear from our Main Theorem.)

(4.3) Lemma. *Let the set $S \subseteq F^{m+n}$ be definable (using constants) in the pseudo-finite field F. Then there is $M = M(S) \in \mathbb{N}$ such that for all $x \in F^m$:*

$$\text{if } S_x \text{ is finite, then } \operatorname{card}(S_x) \leqq M.$$

Proof. Replacing the constants in the defining formula for S by extra variables we may as well assume that S is defined by a formula $\phi(X, Y)$ in the language of rings, where $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_n)$. Let the constant C, the finite set D of pairs (d, μ), and the formulas $\phi_{d,\mu}(X)$ be as in (3.7) and (3.8).

Suppose $(d, \mu) \in D$ with $d > 0$. Clearly, for finite fields $\mathbb{k}$ and $x \in \mathbb{k}^m$ such that $\mathbb{k} \models \phi_{d,\mu}(x)$ we have card $\phi(x, \mathbb{k}^n) >$ (positive constant) $\cdot$ card $(\mathbb{k})$, where the constant does not depend on $(\mathbb{k}, x)$; hence by (4.1) (1), if $x \in F^m$ and $F \models \phi_{d,\mu}(x)$, the set S_x must be infinite. Similarly, for $(0, \mu) \in D$, finite fields $\mathbb{k}$ and $x \in \mathbb{k}^m$ such that $\mathbb{k} \models \phi_{0,\mu}(x)$, we have card $\phi(x, \mathbb{k}^n) \leqq M$, where the constant $M \in \mathbb{N}$ does not depend on $(\mathbb{k}, x)$. Hence, for $x \in F^m$, the set S_x is finite if and only if S_x is empty or $F \models \phi_{0,\mu}(x)$ for some pair $(0, \mu) \in D$, and in that case card $(S_x) \leqq M$. □

(4.4) We gave this proof in detail to show how (4.1) (1) can be used to draw conclusions for pseudo-finite fields from facts about finite fields. Below we will leave such routine verifications to the reader. After all, such results about pseudo-finite fields are just elegant recastings of more complicated statements on *families* of finite fields. Here is an example which shows that pseudo-finite fields behave much like stable structures (according to Cherlin and Hrushovski).

(4.5) Proposition. *Let the set $S \subseteq F^{m+1}$ be definable (using constants) in the pseudo-finite field F. Then there is no infinite set $A \subseteq F^m$ such that all sets S_a with $a \in A$ are infinite and all intersections $S_a \cap S_b$ with $a \neq b$, $a, b \in A$, are finite.*

Proof. By the previous lemma there is a uniform bound $B \in \mathbb{N}$ on the size of finite sets of the form $S_a \cap S_b$. Therefore it suffices to prove the following result on formulas $\phi(X, Y)$ in the language of rings, $X = (X_1, \ldots, X_m)$, Y a single variable:

There are positive integers K, M and N with the property that there is no finite field $\mathbb{k}$ of size $\geqq K$ and finite set $A \subseteq \mathbb{k}^m$ of size $\geqq M$, such that all sets $\phi(a, \mathbb{k})$ with $a \in A$ have size $\geqq N$ and all intersections $\phi(a, \mathbb{k}) \cap \phi(b, \mathbb{k})$ with $a, b \in A$, $a \neq b$, have size $\leqq B$.

To see this, note that by the Main Theorem there is a positive integer N and a rational $\mu > 0$, such that if $|\phi(a, \mathbb{k})| \geqq N$, then $|\phi(a, \mathbb{k})| \geqq \mu q$, where $\mathbb{k} = \mathbb{F}_q$.

Hence, if $M > 1/\mu$, there cannot be M distinct sets $\phi(a, \mathbb{k})$ all whose pairwise intersections are "small" of size $\leqq B$, provided q is sufficiently large. □

(4.6) Proposition. *Let $\phi(X, Y)$ with $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_n)$ be a formula. Then there is $M(\phi) \in \mathbb{N}$ such that for each finite field $\mathbb{k}$ there is no strictly increasing chain of sets $\phi(x^1, \mathbb{k}^n) \subset \ldots \subset \phi(x^M, \mathbb{k}^n)$ of length M, $x^i \in \mathbb{k}^m$.*

Remark. It follows that for pseudo-finite F and set $S \subseteq F^{m+n}$ definable in F using constants, there is $M \in \mathbb{N}$ such that there is no strictly increasing chain

$$S_{a(1)} \subset S_{a(2)} \subset \ldots \subset S_{a(M)} \text{ of length } M,\ a(i) \in F^m.$$

Proof. It suffices to prove the proposition for sufficiently large finite fields, and below we assume tacitly that $\mathbb{k}$ is a "large" finite field. Consider a strictly increasing chain

$\phi(x^1, \mathfrak{k}^n) \subset \ldots \subset \phi(x^M, \mathfrak{k}^n)$, $x^i \in \mathfrak{k}^m$. We have to bound M. Let us write $S_i := \phi(x^i, \mathfrak{k}^n)$ for convenience. Of course we may as well assume that $S_1 \neq \emptyset$. Our Main Theorem associates to ϕ a finite set D of pairs (d, μ), and to each S_i exactly one of those pairs, say (d_i, μ_i). Since $\mathfrak{k}$ is large, we have $(d_1, \mu_1) \leqq \ldots \leqq (d_M, \mu_M)$, where D is lexicographically ordered. Our argument is now by induction on $d_M = \max(d_i)$. Since D is finite, we may (in order to bound M) as well assume all (d_i, μ_i) are equal, say $(d_i, \mu_i) = (d, \mu)$ for all i. We now look at the differences $S_i \setminus S_1$ for $i > 1$, which form themselves a strictly increasing chain $S_2 \setminus S_1 \subset \ldots \subset S_M \setminus S_1$ of length $M - 1$. Again our Main Theorem associates a finite set of pairs (e, ν) to nonempty sets of the form $\phi(a, \mathfrak{k}^n) \setminus \phi(b, \mathfrak{k}^n)$. Since $\mathfrak{k}$ is large, and the S_i have all approximately μq^d elements, where $q = \operatorname{card}(\mathfrak{k})$, the sets $S_i \setminus S_1$ are much smaller than the S_i's, so the pairs (e, ν) associated to them must have $e < d = d_M$. Then the inductive hypothesis gives us a bound on $M - 1$, hence we get a bound on M. □

Interpretation of the numbers d and μ: dimension and measure.

(4.7) Given an infinite field F we define the *algebraic dimension* $\operatorname{algdim}(S)$ of a nonempty set $S \subseteqq F^n$ to be the usual dimension of its Zariski closure in the affine space $\tilde{F}^n$, or equivalently, the Krull dimension of the ring $F[Y]/I$ where the ideal I is given by $I := \{f \in F[Y] : f \text{ vanishes identically on } S\}$. By convention, $\operatorname{algdim}(\emptyset) = -\infty$.

(4.8) Fix a pseudo-finite field F and a nonempty set $S \subseteqq F^n$ definable in F using constants, say $S = \phi(x, F^n)$ for a formula $\phi(X, Y)$ and $x \in F^m$. In section 3 we associated to ϕ a finite set D of pairs (d, μ), and to each such pair a formula $\phi_{d,\mu}(X)$; there is a unique pair $(d, \mu) \in D$ such that $F \models \phi_{d,\mu}(x)$. (If F were a large finite field of size q this would mean that S has roughly μq^d elements.) One checks easily, by arguing with large finite fields, that this pair (d, μ) associated to S via ϕ does not depend on the choice of the defining formula $\phi(x, Y)$ for S. Here is an algebraic interpretation of the integer d.

(4.9) Proposition. *With S and d as above we have*: $d = \operatorname{algdim}(S)$.

Proof. Suppose first that $S = V(F)$ for an F-algebraic set $V \subseteqq \tilde{F}^n$. Then the proof of (3.3) shows that $d = \dim(V^*)$. Since F is pseudo-finite it follows, cf. [6], 10.1, that $S = V(F) = V^*(F)$ is Zariski-dense in V^*. Hence $d = \operatorname{algdim}(S)$.

We now reduce the general case to the special case just discussed: by Lemma (2.9) we may as well assume that for some $e, k \in \mathbb{N}$ we have $S = \pi(V(F))$ where $V \subseteqq \tilde{F}^{n+k}$ is an F-algebraic set, $\pi : \tilde{F}^{n+k} \to \tilde{F}^n$ is the projection on the first n coordinates, and each fiber V_y $(y \in \tilde{F}^n)$ has at most e points. In particular, each $y \in S$ has at most e inverse images under π in $V(F)$. Hence, by considering what this would mean if F were a "large" finite field, we see that for the pair (d', μ') associated to $V(F)$ we have $d = d'$. Now V^* is the Zariski-closure of $V(F)$ in $\tilde{F}^{n+k}$, so by the special case already done we have $d = d' = \dim(V^*)$, and $S = \pi(V(F))$ is Zariski-dense in $\pi(V^*)$, hence Zariski-dense in the Zariski-closure $\pi(V^*)^Z$ of $\pi(V^*)$. Each fiber V_y^* $(y \in \tilde{F}^n)$ has at most e elements, so

$$\operatorname{algdim}(S) = \dim(\pi(V^*)^Z) = \dim(V^*) = d. \quad \square$$

(4.10) We now give a "measure theoretic" interpretation to the rational number μ associated by our Main Theorem to a definable set.

With F, S and (d, μ) as before, let $\mathrm{Def}(S)$ be the boolean algebra of subsets of S that are definable in F using constants. Let $\mu_S : \mathrm{Def}(S) \to [0,1]$ be given as follows:

for any nonempty $A \in \mathrm{Def}(S)$ with associated pair (e, v), put

$$\mu_S(A) = 0 \quad \text{if } e < d \text{ (and also } \mu_S(\emptyset) = 0),$$
$$\mu_S(A) = v/\mu \quad \text{if } e = d.$$

One easily checks that μ_S is then a finitely additive probability measure taking only rational values, such that if there is a bijection between elements A and B of $\mathrm{Def}(S)$ definable in F using constants, then $\mu_S(A) = \mu_S(B)$.

Using the properties of this measure on $\mathrm{Def}(F^n)$ we easily obtain the following extension of Proposition (4.5). We leave the proof to the reader.

(4.11) Proposition. *Let the set $S \subseteq F^{m+n}$ be definable using constants in the pseudo-finite field F. Then there is no infinite set $A \subseteq F^m$ such that $\dim(S_a) = n$ for all $a \in A$ and $\dim(S_a \cap S_b) < n$ for all distinct $a, b \in A$.*

§ 5. Algebraic boundedness

(5.1) An infinite field E is called *algebraically bounded* if for each set $S \subseteq E^m$ that is definable in E using constants there are polynomials $f_1, \ldots, f_r \in E[X, T]$ such that if S_x is finite, $x \in E^m$, then $S_x \subseteq \{t \in E : f_i(x, t) = 0\}$ for some $i \in \{1, \ldots, r\}$ with $f_i(x, T) \neq 0$.

The importance of this property stems from the fact that if E is algebraically bounded, then algebraic dimension behaves very well for sets $S \subseteq E^m$ that are definable in E using constants, cf. [2]; for instance, $\mathrm{algdim}(f(S)) \leq \mathrm{algdim}(S)$ when $f : S \to E^n$ is a map definable in E using constants; also, if $R \subseteq E^{m+n}$ is definable in E using constants, then for each $d \in \{0, \ldots, n\}$ the set $\{x \in E^m : \mathrm{algdim}(R_x) = d\}$ is definable in E using constants. Below we prove that pseudo-finite fields are algebraically bounded, by first proving a general property of perfect PAC-fields. In this proof we shall freely make use of known facts on PAC-fields, cf. [6]. First a purely model-theoretic notion.

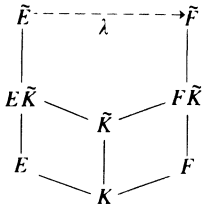
(5.2) Definition. A subfield K of a field E is said to be *finitely closed in E* if for each $L(K)$-formula $\phi(T)$ such that $\phi(E)$ is finite we have $\phi(E) \subseteq K$.

In pure model theory this is also called "algebraically closed in", but this terminology is to be avoided here for obvious reasons.

(5.3) Proposition. *Let K be a relatively algebraically closed subfield of a perfect* PAC-*field E. Then K is finitely closed in E.*

Proof. Given an $L(K)$-formula $\phi(T)$ such that $\phi(E)$ is finite we have to show that $\phi(E) \subseteq K$. Suppose that $b \in \phi(E) \setminus K$. To derive a contradiction it clearly suffices to construct an element b' in an elementary extension E' of E such that $b' \in \phi(E') \setminus \phi(E)$. The idea is to get E' as a sort of free amalgam of two copies of E over K, and b' as the

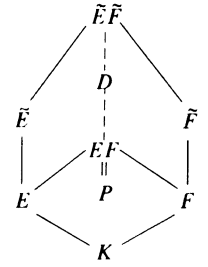
element that corresponds to b in the other copy. The details are as follows. Since $E|K$ is regular, the K-algebra $E \otimes_K E$ is a domain. Let $P := \mathrm{Frac}(E \otimes_K E)$, and identify E with $E \otimes 1 \subseteq P$ via $e \to e \otimes 1$, and put $F := 1 \otimes E \subseteq P$, so F is just a second copy of E over K but linearly disjoint from E inside P. The K-isomorphism $e \to 1 \otimes e : E \to F$ extends to an isomorphism $E\tilde{K} \to F\tilde{K}$ that is the identity on $\tilde{K}$, and then further to an isomorphism $\lambda : \tilde{E} \to \tilde{F}$ that is the identity on $\tilde{K}$, see the following diagram of subfields of $\tilde{P}$.



Note that λ induces an isomorphism $\Phi : G(F) \to G(E)$ of absolute Galois groups:

$$\Phi(\sigma) = \lambda^{-1} \circ \sigma \circ \lambda .$$

Next we consider the following diagram of subfields of $\tilde{P}$.



We now construct a field D between P and its Galois extension $\tilde{E}\tilde{F}$ such that the restriction maps $\mathrm{Gal}(\tilde{E}\tilde{F}|D) \to G(E)$ and $\mathrm{Gal}(\tilde{E}\tilde{F}|D) \to G(F)$ are isomorphisms. First define an embedding $\sigma \to \sigma' : G(F) \to \mathrm{Gal}(\tilde{E}\tilde{F}|P)$ by:

$$\sigma'(x) = \sigma(x) \qquad \text{for } x \in \tilde{F},$$
$$\sigma'(x) = (\Phi\sigma)(x) \quad \text{for } x \in \tilde{E}.$$

(Then σ' is well-defined since $\tilde{E}$ and $\tilde{F}$ are linearly disjoint over $\tilde{K}$, and $\sigma(x) = (\Phi\sigma)(x)$ for $x \in \tilde{K}$.) In the same way we define an embedding

$$\tau \to \tau'' : G(E) \to \mathrm{Gal}(\tilde{E}\tilde{F}|P) :$$

$\tau''(x) = \tau(x)$ for $x \in \tilde{E}$, $\tau''(x) = (\Phi^{-1}\tau)(x)$ for $x \in \tilde{F}$. These two embeddings have the same image in $\mathrm{Gal}(\tilde{E}\tilde{F}|P)$ since $\sigma' = (\Phi\sigma)''$ for $\sigma \in G(F)$.

Let $D :=$ fixed field of this image. Then clearly the restriction maps

$$\mathrm{Gal}(\tilde{E}\tilde{F}|D) \to G(E) \quad \text{and} \quad \mathrm{Gal}(\tilde{E}\tilde{F}|D) \to G(F)$$

are isomorphisms, as desired. Now we take a regular PAC-field extension Q of D, cf. [6], p. 155, so that the restriction map $G(Q) \to \mathrm{Gal}(\tilde{E}\tilde{F}|D)$ is surjective. Since $G(Q)$ is projective, cf. [6], p. 137, it has a closed subgroup N that maps isomorphically onto

$\mathrm{Gal}(\tilde{E}\tilde{F}|D)$ by this restriction map. Put $E' :=$ fixed field of N (inside $\tilde{Q}$). Then E' is a perfect PAC-field, cf. [6], p. 132, and $G(E') = N$ maps isomorphically onto $G(E)$ and onto $G(F)$ by restriction. Hence E' is an elementary extension of E and of F, cf. [6], p. 254.

Put $b' := 1 \otimes b \in \phi(F) \setminus K$. Then clearly $b' \in \phi(E') \setminus \phi(E)$. □

(5.4) Remark. The construction of D in the proof is like the "field crossing argument" in [6], p. 250.

(5.5) It is useful at this point to extend the notion of algebraic boundedness from individual fields to theories of fields.

Definition. Let $\mathscr{T}$ be an L-theory of fields (i.e., all its models are fields). Then we call $\mathscr{T}$ *algebraically bounded* if for each formula $\phi(X, T)$ there are polynomials

$$f_1(X, T), \ldots, f_k(X, T) \in \mathbb{Z}[X, T]$$

such that for each $\mathscr{T}$-model E and each $a \in E^m$ for which $\phi(a, E)$ is finite there is $i \in \{1, \ldots, k\}$ such that $f_i(a, T) \neq 0$ and $\phi(a, E) \subseteqq \{t \in E : f_i(a, t) = 0\}$.

Clearly, if $\mathscr{T}$ is algebraically bounded, each infinite model of $\mathscr{T}$ is algebraically bounded, in the sense defined earlier in (5.1). We do not know if the converse holds. The significance of the algebraic boundedness of $\mathscr{T}$ is that "algebraic dimension" is definable *uniformly* in all models of $\mathscr{T}$: given any formula $\phi(X, Y)$ and $d \in \{-\infty, 0, \ldots, n\}$ there is a formula $\phi_d(X)$ such that for each infinite model E of $\mathscr{T}$ we have

$$\{x \in E^m : \mathrm{algdim}\,(\phi(x, E^n)) = d\} = \phi_d(E^m)\,.$$

(This follows by adapting the proof of [2], 1.4.) A simple example of an algebraically bounded theory of fields is the theory of algebraically closed fields. Here is a useful model-theoretic test for algebraic boundedness of theories.

(5.6) Lemma. *Let $\mathscr{T}$ be an L-theory of fields. Then $\mathscr{T}$ is algebraically bounded if and only if the following conditions are satisfied*:

(i) *For each L-formula $\phi(X, T)$ there is an integer $M \in \mathbb{N}$ such that if $E \models \mathscr{T}$, $x \in E^m$ and $\phi(x, E)$ is finite, then* $\mathrm{card}\,(\phi(x, E)) \leqq M$.

(ii) *Each relatively algebraically closed subfield of a $\mathscr{T}$-model E is finitely closed in E.*

Proof. That algebraic boundedness of $\mathscr{T}$ implies (i) and (ii) follows by a simple argument that we leave to the reader. Conversely, assume (i) and (ii) hold for each $\mathscr{T}$-model E. Let $\phi(X, T)$ be a formula, and let M be as in (i). By (ii) there is for each $\mathscr{T}$-model E and $x \in E^m$ with finite $\phi(x, E)$ a polynomial $f(X, T) \in \mathbb{Z}[X, T]$ such that $f(x, T) \neq 0$ and $\phi(x, E) \subseteqq \{t \in E : f(x, t) = 0\}$. Hence by a simple compactness argument we obtain polynomials $f_1, \ldots, f_k$ in $\mathbb{Z}[X, T]$ with the desired property. □

(5.7) Corollary. *The theory of pseudo-finite fields is algebraically bounded. In particular, each pseudo-finite field is algebraically bounded.*

(5.8) This follows from the proof of Lemma (4.3), and Proposition (5.3), in view of Lemma (5.6). Initially we had a different (shorter) argument proving (5.7), but we took the longer route via (5.3), since (5.3) seems interesting in its own right.

§ 6. Axioms for quadratic extensions of finite fields

(6.1) We recall from the introduction that Psf denotes the theory of pseudo-finite fields, which has a familiar axiomatization, cf. (4.1), and that Psf^2 denotes the theory of pseudo-finite fields satisfying the sentences true in all finite fields of the form $\mathbb{F}_{q^2}$, with q a prime power >1. We also let $\mathrm{Psf}(p)$ (for $p=0$ or p a prime number) denote the theory of pseudo-finite fields of characteristic p, and $\mathrm{Psf}^2(p)$ the theory of models of Psf^2 of characteristic p.

Below we use that the absolute Galois group $G(F)$ of a pseudo-finite field F is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of the group of integers $\mathbb{Z}$.

(6.2) Lemma. *Let $F \models \mathrm{Psf}(0)$, and embed $\tilde{\mathbb{Q}}$ into $\tilde{F}$, so that we have a restriction map $G(F) \to G(\mathbb{Q})$. Let σ be a generator of the profinite group $G(F)$. Then*

$$F \models \mathrm{Psf}^2 \Leftrightarrow \sigma | \tilde{\mathbb{Q}} \text{ is a square in } G(\mathbb{Q}).$$

Proof. Suppose $F \models \mathrm{Psf}^2$. Replacing F by an elementary extension (and lifting σ accordingly) we may as well assume that F is an ultraproduct of fields $\mathbb{F}_{q^2}$, so that F contains a pseudo-finite subfield E over which it is of degree 2, namely the corresponding ultraproduct of the $\mathbb{F}_q$'s. Then $G(E)$ has generator τ with $\sigma = \tau^2$, hence $\sigma|\tilde{\mathbb{Q}} = (\tau|\tilde{\mathbb{Q}})^2$, so that $\sigma|\tilde{\mathbb{Q}}$ is a square in $G(\mathbb{Q})$.

Conversely, let $(\sigma|\tilde{\mathbb{Q}}) = \pi^2$, $\pi \in G(\mathbb{Q})$. Let $K \subseteq \tilde{\mathbb{Q}}$ be the fixed field of π. By Cebotarev's density theorem (cf. Ax [1] for the way how this is used here) there is an ultraproduct E of fields $\mathbb{F}_p$ such that, after embedding $\tilde{\mathbb{Q}}$ into $\tilde{E}$, π can be lifted to a generator ϱ of $G(E)$. Let E' be the unique quadratic extension of E inside $\tilde{E}$, so that E' is isomorphic to the corresponding ultraproduct of the fields $\mathbb{F}_{p^2}$. It follows that $E' \models \mathrm{Psf}^2$, and $G(E')$ is generated by ϱ^2. Now $\varrho^2|\tilde{\mathbb{Q}} = \pi^2 = \sigma|\tilde{\mathbb{Q}}$, so E' and F are two pseudo-finite fields such that $E' \cap \tilde{\mathbb{Q}} =$ fixed field of $\pi^2 = F \cap \tilde{\mathbb{Q}}$. Hence $F \equiv E'$ by [6], Corollary 18.10, so $F \models \mathrm{Psf}^2$. □

(6.3) Since an element of $G(\mathbb{Q})$ is a square if and only if its restriction to each finite degree Galois extension of $\mathbb{Q}$ is a square, this leads to the following considerations. For each finite degree Galois extension $K \subseteq \tilde{\mathbb{Q}}$ of $\mathbb{Q}$, take a set $S(K) \subseteq \mathrm{Gal}(K|\mathbb{Q})$ such that every square in $\mathrm{Gal}(K|\mathbb{Q})$ is conjugate to a power of σ^2 for some $\sigma \in S(K)$. For each $\sigma \in S(K)$, take $\alpha_\sigma \in K$ such that $\mathbb{Q}(\alpha_\sigma) = \mathrm{Fix}(\sigma^2)$ and α_σ is integral over $\mathbb{Z}$.

Let $f_\sigma(T) \in \mathbb{Z}[T]$ be the minimal polynomial of α_σ over $\mathbb{Q}$, and define $f_K(T) := \prod f_\sigma(T)$, σ ranging over $S(K)$. For example, if $K = \mathbb{Q}(\sqrt{n})$, where $n \in \mathbb{Z}$ is not a square, then we can take $S(K) = \{\text{identity}\}$ and $\alpha_\sigma = \sqrt{n}$, so that $f_K(T) = T^2 - n$.

(6.4) Proposition. *An axiomatization of* $\mathrm{Psf}^2(0)$ *is given by*

$$\mathrm{Psf}(0) \cup \{\exists T(f_K(T) = 0) \colon K \subseteq \tilde{\mathbb{Q}} \text{ is a finite degree Galois extension of } \mathbb{Q}\}.$$

Proof. Let $F \models \mathrm{Psf}^2(0)$, and take a generator τ of $G(F)$, and let $K \subseteq \tilde{\mathbb{Q}} \subseteq \tilde{F}$ be a finite degree Galois extension of $\mathbb{Q}$. By (6.2) the restriction $\tau | K$ is a square, hence conjugate to some power σ^{2i} with $\sigma \in S(K)$. Hence $F \cap K$ contains a subfield isomorphic to $\mathbb{Q}(\alpha_\sigma)$, and therefore $F \models \exists T(f_K(T) = 0)$.

Conversely, suppose $F \models \mathrm{Psf}(0)$ and $F \models \exists T(f_K(T) = 0)$ for each finite degree Galois extension $K \subseteq \tilde{\mathbb{Q}} \subseteq \tilde{F}$ of $\mathbb{Q}$. Let τ be a generator of $G(F)$. To show $F \models \mathrm{Psf}^2$, it suffices by (6.2) to show that $\tau | K$ is a square in $\mathrm{Gal}(K|\mathbb{Q})$ for each such K. Given such K, it follows from $F \models \exists T(f_K(T) = 0)$ that $F \cap K$ contains a subfield L isomorphic to $\mathbb{Q}(\alpha_\sigma)$ for some $\sigma \in S(K)$. By definition of α_σ, some conjugate of σ^2 generates $\mathrm{Gal}(K|L)$, so that $\mathrm{Gal}(K|L)$ is generated by a square of $\mathrm{Gal}(K|\mathbb{Q})$. Therefore

$$\tau | K \in \mathrm{Gal}(K|F \cap K) \subseteq \mathrm{Gal}(K|L)$$

is a square in $\mathrm{Gal}(K|\mathbb{Q})$. □

(6.5) As already said in the introduction, if p is a prime number, then $\mathrm{Psf}^2(p)$ is axiomatized by $\mathrm{Psf}(p) \cup \{\exists T(T^2 = n) : n \in \mathbb{Z}\}$. To see that a model F of the latter theory is a model of the former, note that F contains a copy of $\mathbb{F}_{p^2}$, so the subfield

$$F^a := \{x \in F : x \text{ is algebraic over } \mathbb{F}_p\}$$

of F is isomorphic to $\mathbb{F}_{p^{2n}}$ for some *supernatural* number n, cf. [6], 20.9. If $n \notin \mathbb{N}$, we form a nonprincipal ultraproduct of the fields $\mathbb{F}_{p^{2m}}$ with $m \in \mathbb{N}$ and $m | n$, and get a pseudo-finite field E such that $E^a \cong F^a$, hence $E \equiv F$ by [6], 18.10, and therefore $F \models \mathrm{Psf}^2$, since $E \models \mathrm{Psf}^2$. If $n \in \mathbb{N}$, we form a nonprincipal ultraproduct of the $\mathbb{F}_{p^{2mn}}$ with m ranging over the primes not dividing n, and again we get a pseudo-finite field E with $E^a \cong F^a$ and $E \models \mathrm{Psf}^2$, so that $F \models \mathrm{Psf}^2$.

So for prime characteristic there is a much simpler result than (6.4), and this raises the question whether the polynomials $f_K(T) \in \mathbb{Z}[T]$ in (6.4) can be replaced by, say, the polynomials $T^2 - n$ for $n \in \mathbb{Z}$. The next results show this is not the case.

(6.6) Corollary. *Suppose each polynomial in a set* $\mathscr{F} \subseteq \mathbb{Z}[T] \setminus \mathbb{Z}$ *has solvable splitting field over* $\mathbb{Q}$. *Then* $\mathrm{Psf}(0) \cup \{\exists T(f(T) = 0) : f \in \mathscr{F}\}$ *is not an axiomatization of* $\mathrm{Psf}^2(0)$.

Proof. Let $E \subseteq \tilde{\mathbb{Q}}$ be the splitting field of $\mathscr{F}$ over $\mathbb{Q}$, so $E|\mathbb{Q}$ is a solvable Galois extension (of possibly infinite degree over $\mathbb{Q}$). Take a Galois extension $K \subseteq \tilde{\mathbb{Q}}$ of $\mathbb{Q}$ with $\mathrm{Gal}(K|\mathbb{Q}) \cong A_5$; since A_5 is a simple non-abelian group we have $E \cap K = \mathbb{Q}$, hence there is $\sigma \in G(E)$ such that $\sigma | K$ is not a square in $\mathrm{Gal}(K|\mathbb{Q})$. Now take a pseudo-finite field F such that $F \cap \tilde{\mathbb{Q}} = \mathrm{Fix}(\sigma)$ (after embedding $\tilde{\mathbb{Q}}$ into $\tilde{F}$). Then $E \subseteq F$, so

$$F \models \mathrm{Psf}(0) \cup [\exists T(f(T) = 0) : f \in \mathscr{F}],$$

but F is not a model of Psf^2, since σ lifts to a generator of $G(F)$ and $\sigma | K$ is not a square. □

(6.7) The same argument proves that if $\mathscr{F} \subseteq \mathbb{Z}[T] \setminus \mathbb{Z}$ and

$$\mathrm{Psf}(0) \cup \{\exists T(f(T) = 0) : f \in \mathscr{F}\}$$

axiomatizes $\mathrm{Psf}^2(0)$, then for each Galois extension $K \subseteq \tilde{\mathbb{Q}}$ of $\mathbb{Q}$ with simple Galois group over $\mathbb{Q}$ there must be $f \in \mathscr{F}$ such that K is contained in the splitting field of f over $\mathbb{Q}$ in $\tilde{\mathbb{Q}}$. In particular, the degrees of the polynomials in $\mathscr{F}$ cannot be bounded by a constant, since every alternating group A_m is realized as a Galois group over $\mathbb{Q}$.

(6.8) What has been said about quadratic extensions of finite fields generalizes without difficulty to n'th degree extensions of finite fields, for each fixed n. We leave this to the reader.

References

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

[2] *L. van den Dries*, Dimension of definable sets, algebraic boundedness and henselian fields, Ann. Pure Appl. Logic **45** (1989), 189–209.

[3] *L. van den Dries*, A remark on Ax's theorem on solvability modulo primes, Math. Z. **208** (1991), 65–70.

[4] *L. van den Dries* and *K. Schmidt*, Bounds in the theory of polynomial rings over fields, Invent. Math. **76** (1984) 77–91.

[5] *J.-L. Duret*, Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance, in Model theory of Algebra and Arithmetic, Lect. Notes Math. **834** (1980), 135–157.

[6] *M. Fried* and *M. Jarden*, Field Arithmetic, Erg. Math. **11**, Berlin–Heidelberg–New York 1986.

[7] *A. Grothendieck*, Elements de Géometrie Algébrique IV, Publ. Math. Inst. Hautes Etud. Sci. **11** (1961).

[8] *C. W. Henson*, A family of countable homogeneous graphs, Pac. J. Math. **38** (1971), 69–83.

[9] *C. Kiefe*, Sets definable over finite fields: Their Zeta functions, Trans. AMS **223** (1976), 45–59.

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

[11] *B. Poizat*, Une Théorie de Galois imaginaire, J. Symb. Logic **48** (1983), 1151–1170.

[12] *P. Roquette*, Nonstandard aspects of Hilbert's irreducibility theorem, in Model Theory and Algebra, Lect. Notes Math. **498** (1975), 231–275.

Université Paris VII – C.N.R.S., Equipe de Logique Mathématique, Tour 44–55 – 5^e étage –
2, Place Jussieu, 75251 Paris Cedex 05, France
Department of Mathematics, University of Illinois, Urbana, IL 61801, USA
Mathematical Institute, 24–29, St. Giles, Oxford OX1 3LB, England

Eingegangen 11. April 1991