The elementary theory of finite fields*

By JAMES AX**

CONTENTS

Central results and methods

0. Introduction

In this paper we prove the decidability of the theory of finite fields and of the theory of p-adic fields. This generalizes our algorithm, given in [8], for determining whether a system of diophantine equations has, for all primes p, a solution modulo p (or a p-adic solution).

In our proof the crucial properties of finite fields are Weil's Riemann hypothesis for curves and Čebotarev's density theorem.

The decidability of related theories is also obtained. These include the theory of almost all finite fields, the theory of prime finite fields, the theory of finite fields of a fixed characteristic and the theory of unramified extensions of p-adic fields. All the conjectures of [8] are established.

Let R_q denote the field with q elements and let E be an elementary statement about rings. The basic metamathematical result is a determination of the set $\Delta(E)$ of q such that E holds in R_q. It turns out that the sets of

* This research was in part performed while the author was supported by NSF Grant GP-3665.

** Sloan Fellow.

prime powers of the form $\Delta(E)$ have a simple characterization. If n is a positive integer and W is a set of divisors of n, we set

$$a(n, W) = \{m \mid \gcd(n, m) \in W\} .$$

MAIN THEOREM. *Given E and a prime p we can find α_p, n_p, W_p, such that for $m > \alpha_p$,*

$$E \text{ holds in } R_{p^m} \longleftrightarrow m \in a(n_p, W_p) .$$

This implies, for example, that *if E holds in R_{p^m} whenever $m \equiv 1 \bmod 3$, then E holds in R_{p^m} for all but a finite set of $m \equiv 2 \bmod 3$.*

To describe the dependence of α_p, n_p and W_p on p we have the following.

SUPPLEMENT. *We can find an integer π and a finite normal extension N of the rationals with the following properties. For $p > \pi$ we can take $\alpha_p = 0$ and n_p, W_p so that they depend only on the decomposition subfield of N with respect to a prime of N above p.*

Of course there are only finitely many subfields K of N; moreover, it follows from Čebotarev's theorem that a subfield K of N arises infinitely often if and only if N is a cyclic extension of K.

As another example of our characterization we have the following fact. *If E holds for all prime fields, then E holds for all finite fields of sufficiently large characteristic.*

The principal method of proof is the algebraic investigation of certain infinite fields which are "like" finite fields. We recall that a field F is said to be *quasi-finite* if F shares with finite fields the properties of being perfect and of having precisely one extension of each degree. We call F *pseudo-finite* if in addition,

(*) every (absolutely irreducible) variety defined over F has an F-valued point.

It follows from the Riemann hypothesis that every infinite algebraic extension of a finite field satisfies (*) and that every non-principal ultraproduct $\mathcal{R}$ of the R_q is pseudo-finite. We will prove that *pseudo-finite fields are precisely those infinite-fields having every elementary property shared by all finite fields*; i.e., *pseudo-finite fields are the infinite models of the theory of finite fields.*

Actually the ultraproducts $\mathcal{R}$ satisfy a certain infinite dimensional analogue of (*):

(**) for every regular extension field F of a subfield E of $\mathcal{R}$ such that $\sharp F < \sharp\mathcal{R}$, there exists an E-monomorphism $F \to \mathcal{R}$.

We call an uncountable quasi-finite field $\mathcal{R}$ satisfying (**), *hyper-finite.*

Our basic algebraic result is that two hyper-finite fields having the same cardinality and the same absolute numbers are isomorphic. It turns out that the hyper-finite fields are precisely the uncountable saturated pseudo-finite fields; in particular every pseudo-finite field is elementarily equivalent to a hyper-finite field. Thus two pseudo-finite fields are elementarily equivalent if and only if they have the "same" absolute numbers. (An element α of a field F is called an *absolute number* $\leftrightarrow \alpha$ is algebraic over the prime field of F.) This implies that if E is an elementary statement, then there exists a simple one variable elementary systement λ (i.e., an assertion about the absolute numbers) such that $[E \leftrightarrow \lambda]$ holds in every finite field. Moreover we can, in principle, find λ using the fact the statement $[E \leftrightarrow \lambda]$ is, by the Completeness Theorem, provable from the (recursive) axioms for pseudo-finite fields. This yields the Main Theorem and its Supplement.

While the decision procedures obtained are somewhat unorthodox, this may be regarded as a syntactical reflection of the fact that the theories considered are not model complete, as is shown by example at the end of § 8.

Diverse applications. While we have found no striking number-theoretic applications of our results, certain instances of the Main Theorem and its p-adic analogue are not without arithmetic interest. A field is said to be $C_i(d) \leftrightarrow$ every form of degree d in more than d^i variables has a non-trivial zero over the field.

THEOREM A. *Let i, d be positive integers, and let p be a prime. For each m, let $\mathbf{Q}_{p^m}$ be the unramified extension of the p-adic numbers of degree m. Then the set of m such that $\mathbf{Q}_{p^m}$ is $C_i(d)$ differs by a finite set from some $a(n, W)$.*

A purely algebraic statement which follows from our methods is the following.

THEOREM B. $\prod_p R_p/\bigoplus R_p \approx \prod R_{p^p}/\bigoplus R_{p^p}$ *as rings, assuming the continuum hypothesis.*

This statement, although intrinsically uninteresting, is notable in that its proof seems to defy existing methods of pure algebra.

Another discovery made during the course of this investigation is the following rather fundamental property of algebraic varieties.

THEOREM C. *An injective morphism of an algebraic variety into itself is surjective.*

This fact seems to have been noticed only in special case (e.g. for affine space by Białynicki-Birula and Rosenlicht [18]).

THEOREM D. *Let F be a perfect field with abelian Galois group such that every absolutely irreducible variety over F has an F-valued point. Then F is C_1.*

The author is grateful to T. McLaughlin for a stimulating and profitable conversation on this subject.

Notation. We continue to use R_q, $\Delta(E)$, $a(n, W)$, $\mathbf{Q}_{p^m}$ as above. In addition we denote the integers by $\mathbf{Z}$ and the rationals by $\mathbf{Q}$. If $a \in \mathbf{Z}$ then $\mathbf{Z}_{>a}$ denotes the $m \in \mathbf{Z}$ such that $m > a$. $\mathcal{P}$ = set of primes, $\mathcal{Q}$ = set of prime powers. We list below certain symbols. The non-standard ones are defined more completely when they first occur:

$\mathbf{Z}_*$ = set of supernatural numbers, defined in § 1;

(a, b) = gcd (a, b) = greatest common divisor of a, b and $a \mid b$ means a divides b for $a, b \in \mathbf{Z}_*$;

$\delta(m)$ = the set of divisors of $m \in \mathbf{Z}_{>0}$.

If K is a field then:

$[K]$ = set of $f \in \mathbf{Z}[X_1]$ having a root in K;

Abs (K) = $\{\alpha \in K \mid \alpha$ algebraic over the prime field of $K\}$;

$\tilde{K}$ = an algebraic closure of K;

$\mathcal{G}(N/K)$ = the compact group of automorphisms of an algebraic extension N/K;

K_s denotes the unique extension of K of degree $s \in \mathbf{Z}_*$ if there is such ($(R_p)_s$ is written as R_{p^s});

$A \underset{K}{\approx} B$ means A and B are K-isomorphic K-algebras.

Π = the axioms for pseudo-finite fields.

$T \equiv T'$ means T and T' are elementarily equivalent.

$\mathfrak{A}$ = Boolean algebra on $\mathbf{Z}_{>0}$ consisting of the $a(n, W)$ for $n \in \mathbf{Z}_{>0}$ and $W \subseteq \delta(n)$.

$\mathfrak{B}$ = Boolean algebra on $\mathcal{Q}$ generated by the finite sets and the $\Delta(E)$ for E a (one variable) statement.

$\#M$ denotes the cardinality of the set M.

1. Quasi-finite fields

We recall [3, Ch. XIII, § 2] that a field F is called *quasi-finite* if F is perfect and has precisely one extension of each degree (in a fixed algebraic closure $\tilde{F}$). It then follows that every finite extension F'/F is cyclic. If $n \in \mathbf{Z}_{>0}$, the unique extension of F of degree n will be denoted by F_n. For later purposes it is convenient to extend this notation to infinite algebraic extensions of F. Let $\mathbf{Z}_*$ denote the set of *supernatural numbers* [4, Ch. I, § 1.3], i.e.,

the set of formal infinite products $\prod_{p \text{ prime}} p^{n(p)}$ where $n(p) \in \mathbf{Z}_{>0} \cup \{\infty\}$. If F'/F is algebraic and p is a prime, let $n(p) = \sup\{m \mid F_{p^m} \subset F'\}$. Then $F' \to \prod_p p^{n(p)}$ defines a one-to-one correspondence between algebraic extensions of F and supernatural numbers s. For $s \in \mathbf{Z}_*$, we denote the field corresponding to s by F_s. Identifying natural numbers with their image under the obvious map $\mathbf{Z}_{>0} \to \mathbf{Z}_*$, this notation is consistent with the previous one. Moreover if we define multiplicative notions on $\mathbf{Z}_*$ in the obvious way then for $s, t \in \mathbf{Z}_*$ we have that $s \mid t \leftrightarrow F_s \subset F_t$ and $(s, t) = 1 \leftrightarrow F_s \cap F_t = F$. If $s, t \in \mathbf{Z}_{>0}$, then F_{st} is the unique extension of F_s of degree t; so F_s is quasi-finite. More generally if $s = \prod_p p^{n(p)} \in \mathbf{Z}_*$, then F_s is quasi-finite $\leftrightarrow n(p) \neq \infty$ for all p.

If E is a field and A, B are E-algebras then $A \approx_E B$ means they are E-isomorphic.

LEMMA 1. *Let $E \subset F$ be quasi-finite fields such that E is relatively algebraically closed in F. Then*

$$\tilde{F} \approx_F \tilde{E} \otimes_E F .$$

PROOF. Since E is perfect and relatively algebraically closed in F, $\tilde{E} \otimes_E F$ is a field algebraic over F and containing an extension of each degree n over F, namely $E_n \otimes_E F$.

LEMMA 2. *Let $E_1 \subset E_2 \subset F$ be quasi-finite with E_1 relatively algebraically closed in F. Then $\tilde{F} \approx_F \tilde{E}_2 \otimes_{E_2} F$; in particular E_2 is relatively algebraically closed in F.*

PROOF. The first and last isomorphisms of the following sequence follow from Lemma 1.

$$\tilde{E}_2 \otimes_{E_2} F \approx_F (\tilde{E}_1 \otimes_{E_1} E_2) \otimes_{E_2} F \approx_F \tilde{E}_1 \otimes_{E_1} F \approx_F \tilde{F} .$$

LEMMA 3. *If F is quasi-finite there exists a countable subfield E of F such that E is relatively algebraically closed in F and E is quasi-finite.*

PROOF. For each $n \in \mathbf{Z}_{>0}$ let $f_n \in F[X_0]$ be irreducible of degree n. Then any countable relatively algebraically closed subfield E of F containing the coefficients of the f_n works.

LEMMA 4. *Let E be a quasi-finite subfield of a quasi-finite field F. Suppose for each prime p there exists $m(p) \in \mathbf{Z}_{>0}$ and there exists an $f_p \in E_{m(p)}[X_1]$ such that f_p is irreducible over $F_{m(p)}$ of degree p and $(p, m(p)) = 1$. Then E is relatively algebraically closed in F.*

PROOF. If E is not relatively algebraically closed in F then for some prime p, $E_p \subset F$. Then

$$F_{m(p)} \supseteq E_p F_{m(p)} \supseteq E_p E_{m(p)} F_{m(p)} = E_{pm(p)} F_{m(p)} .$$

Our hypothesis shows that $E_{pm(p)}F_{m(p)} \supseteq F_{pm(p)}$ and this yields a contradiction.

Remark. Without going through the details it will be convenient for later purposes to note that the analogues of the facts presented in this section remain valid if we "forget about" some primes. More precisely if S is a set of primes then we define a field F to be S-quasi-finite $\leftrightarrow$ F has one extension of each degree n for which $p \mid n \rightarrow p \in S$. Then the analogues of this section are valid for S-quasi-finite fields.

2. Absolutely entire algebras

Let K be a field and R a (commutative) K-algebra. The following lemma is well-known.

LEMMA 1. *$\tilde{K} \otimes_K R$ is an integral domain $\leftrightarrow$ $A \otimes_K R$ is an integral domain for every extension field A of K.*

Definition. R is *absolutely entire over* $K \leftrightarrow \tilde{K} \otimes_K R$ is an integral domain. If R is a field we shall follow standard terminology [6, Ch. IV, end of §10] and say that R is a *regular extension* of K.

COROLLARY 1. *R is absolutely entire over $K \leftrightarrow A \otimes_K R$ is absolutely entire over A for some (resp. every) extension field A of K.*

COROLLARY 2. *If E and F are quasi-finite and E is relatively algebraically closed in F then F is a regular extension on E.*

COROLLARY 3. *R is absolutely entire over $K \leftrightarrow R$ is an integral domain and its quotient field is a regular extension of K.*

Now let $\aleph$ be a cardinal and let $S = K[X_\nu : \nu < \aleph]$ be the ring of polynomials over K in variables index by the ordinals $\nu < \aleph$.

The following lemma is a direct consequence of the definitions.

LEMMA 2. *Let I be an ideal of S. Then $\tilde{K} \otimes_K I$ is a prime ideal of $\tilde{K} \otimes_K S \leftrightarrow S/I$ is an absolutely entire K-algebra.*

Definition. I is an *absolutely prime ideal* of $S \leftrightarrow S/I$ is an absolutely entire K-algebra.

COROLLARY. *I is absolutely prime $\leftrightarrow$ AI is an absolutely prime ideal of $A[X_\nu : \nu < \aleph]$ for some (resp. every) extension field A of K.*

PROOF. Corollary 1 to Lemma 1 together with Lemma 2.

It follows from the finite-dimensional case [14, Ch. I, § 7, Lem. 2], that there exists a smallest subfield k of K such that there exists an ideal J of $k[X_\nu : \nu < \aleph]$ with $I = KJ$. Then $J = k[X_\nu : \nu < \aleph] \cap I$. Moreover if G is any set of automorphisms of K which transform I into itself then $k \subset$ fixed

field of G.

3. Pseudo-finite fields

Definition. A field F is *pseudo-finite* $\leftrightarrow$ F is quasi-finite and for every finitely generated absolutely entire F-algebra R there exists an F-algebra homomorphism $R \rightarrow F$.

Examples. Let k be a finite field. Then k is quasi-finite. In the terminology of § 1, let $s = \prod_p p^{n(p)}$ be a supernatural number such that $n(p) \neq \infty$ for all p. Then k_s is quasi-finite. If in addition $n(p) \neq 0$ for infinitely many p, then k_s is infinite. As we shall see, it is an easy consequence of the Riemann hypothesis for curves that k_s is pseudo-finite. Similarly any non-principal ultra-product of (non-isomorphic) finite fields is pseudo-finite. On the other hand no finite field k is pseudo-finite. Indeed if $q = \sharp k$ then

$$R = k[X_0, X_1]/\langle 1 - X_0(X_1^q - X_1)\rangle$$

is an absolutely entire k-algebra and there are no k-homomorphisms $K \rightarrow k$.

LEMMA 1. *Let E be a subfield of a pseudo-finite field F and let R be a finitely generated absolutely entire E-algebra. Then there exists an E-algebra homomorphism $R \rightarrow F$.*

PROOF. By Corollary 1 to Lemma 1 of § 2, $F \otimes_E R$ is an absolutely entire F-algebra. Hence there exists an F-homomorphism $F \otimes_E R \rightarrow F$. Then $R \rightarrow F \otimes_E R \rightarrow F$ is an E-algebra homomorphism.

LEMMA 2. *F is pseudo-finite $\leftrightarrow$ F is quasi-finite and every absolutely irreducible variety V defined over F has an F-valued point (over F).*

PROOF. Since every variety V defined over F contains an affine (open) subvariety defined over F, we may assume V is affine. If R is the ring of regular functions on V defined over F, then R is a finitely generated F-algebra. Moreover by definition [7, Ch. II, § 6, Def. 1], an F-valued point of V is precisely an F-homomorphism $R \rightarrow F$. The lemma follows.

LEMMA 3. *Let F be a quasi-finite field such that for every finitely generated absolutely entire E-algebra R, where E is a countable (or finite) subfield of F, there exists an E-algebra homomorphism $R \rightarrow F$. Then F is pseudo-finite.*

PROOF. Let S be a finitely generated absolutely entire F-algebra. We must show that there exists an F-algebra homomorphism $S \rightarrow F$. Now there exists a positive integer n and an ideal I in $F[X_1, \cdots, X_n] = F[X]$ such that $S \approx_F F[X]/I$. Let $g_1, \cdots, g_m \in F[X]$. Then the subfield E of F generated over the prime field of F by the coefficients of $g_1, \cdots, g_m$ is countable or finite.

Set $R = E[X]/J$ where J is the ideal of $E[X]$ generated by $g_1, \cdots, g_m$. Then $S \approx_F R \otimes_E F$. By Corollary 1 to Lemma 1 of § 2, R is an absolutely entire E-algebra. By hypothesis there exists an E-algebra homomorphism $R \to F$. Tensoring this with the identity map $F \to F$ we therefore obtain the desired F-homomorphism

$$S \approx R \otimes_E F \to F .$$

4. Hyper-finite fields

Definition. A field F is *hyper-finite* $\leftrightarrow$ F is uncountable, quasi-finite and for every absolutely entire E-algebra R, where E is a subfield of F and $\sharp R < \sharp F$, there exists an E-algebra homomorphism $R \to F$.

Remarks. It follows from Lemma 3 of § 3 that every hyper-finite field is pseudo-finite. The non-principal ultraproducts of (non-isomorphic) finite fields turn out to be hyper-finite. The main fact we shall eventually establish is the converse of this statement for hyper-finite fields of cardinality $2^{\aleph_0}$.

LEMMA 1. *If E is a subfield of a hyper-finite field F and if R is an absolutely entire E-algebra such that $\sharp R < \sharp F$ then there exists an E-algebra monomorphism $R \to F$.*

PROOF. By Corollary 3 to Lemma 1 of § 2, the quotient field V of R is an absolutely entire E-algebra. Since $\sharp V \leqq \aleph_0 \sharp R < \sharp F$ there exists an E-algebra homomorphism $V \to F$. The composed map $R \to V \to F$ is an E-algebra monomorphism.

LEMMA 2. *Let E be quasi-finite and let F, F' be extension of E such that*

(a) *F is quasi-finite and F' is hyper-finite;*

(b) *E is relatively algebraically closed in F and F';*

(c) *$\sharp F' > \sharp F$.*

Then there exists an E-monomorphism $F \xrightarrow{\varphi} F'$ and for any such φ, $\varphi(F)$ is relatively algebraically closed in F'.

PROOF. The last assertion follows from Lemma 2 of § 1. That φ exists follows from the definition of hyper-finite since F is absolutely entire over E by Corollary 2 to Lemma 1 of § 2.

PROPOSITION 1. *Let E be quasi-finite and let F, F' be extensions of E such that*

(a) *E is relatively algebraically closed in F and F';*

(b) *F and F' are hyper-finite;*

(c) *$\sharp F = \sharp F' > \sharp E$.*

Then $F \approx_E F'$.

PROOF. Let $B = \{t_\lambda : 1 \leqq \lambda < \aleph\}$, $B' = \{t'_\lambda : 1 \leqq \lambda < \aleph\}$ be transcendence bases for F and F' over E, well-ordered by the ordinals $\lambda < \aleph = \#F$. For $0 \leqq \rho < \aleph$ we will recursively define subfields F_ρ of F, F'_ρ of F' containing E and E-isomorphisms $\varphi_\rho : F_\rho \rightarrow F'_\rho$ satisfying the following conditions

(i) $F_0 = F'_0 = E$, $\varphi_0 = 1_E$;

(ii) $\#F_\rho \leqq \#\rho + \aleph_0 \#K \quad \forall\, \rho < \aleph$;

(iii) if $\rho < \rho' < \aleph$ then $F_\rho \subset F_{\rho'}$ and $\varphi_{\rho'} \mid F_\rho = \varphi_\rho$;

(iv) if ρ is an odd positive integer plus a limit ordinal (possibly 0) $F_\rho =$ relative algebraic closure of $F_{\rho-1}(t_\sigma)$ in F where σ is smallest such that $t_\sigma \notin F_{\rho-1}$;

(v) if ρ is an even positive integer plus a limit ordinal, $F'_\rho =$ relative algebraic closure of $F'_{\rho-1}(t'_\sigma)$ where σ is smallest ordinal such that $t'_\sigma \notin F'_{\rho-1}$;

(vi) if $\rho \neq 0$, is a limit ordinal $F_\rho = \bigcup_{\lambda<\rho} F_\lambda$.

Suppose $0 < \lambda < \aleph$ and we have defined F_ρ, F'_ρ for $0 \leqq \rho < \lambda$ satisfying (i)–(vi) with $\aleph$ replaced by λ. Suppose first that λ is an odd positive integer plus a limit ordinal. Then $\exists\, \sigma$ as in (iv) since $\#F_\rho \leqq \#\rho + \aleph_0 \#K \leqq \#\lambda + \aleph_0 \#K < \aleph$. Then F_λ as defined by (iv) is such that $F_{\lambda-1}$, F_λ and $\varphi_{\lambda-1}^{-1}(F'_{\lambda-1})$ satisfy the hypothesis of Lemma 2. Hence $\exists$ a monomorphism $\varphi_\lambda : F_\lambda \rightarrow F'$ extending $\varphi_{\lambda-1}$ and such that $F'_\lambda = \varphi_\lambda(F_\lambda)$ is relatively algebraically closed in F'. Thus we have constructed F_λ, F'_λ, φ_λ. The case where λ is an even positive integer plus a limit ordinal is similar and the limit ordinal case is even easier. Now set $V = \bigcup_{\rho<\aleph} F_\rho$. Then $\{\rho \mid t_\rho \in V\}$ is a segment of the ordinals $< \aleph$ and $\#\{\rho \mid t_\rho \in V\} = \aleph$. Thus $\{\rho \mid t_\rho \in V\} = \{\rho \mid \rho < \aleph\}$ and so F is algebraic/V. Since V is relatively algebraically closed in F because each F_ρ is so, $V = F$. Similarly $\bigcup_{\rho<\aleph} F'_\rho = F'$ and if we define $F \xrightarrow{\varphi} F'$ by $\varphi \mid F_\rho = \varphi_\rho$, we have the desired isomorphism.

Definition. If F is a field, $\mathrm{Abs}(F) = \{\alpha \in F \mid \alpha$ is algebraic over the prime field of $F\}$.

COROLLARY. *If F and F' are hyper-finite of the same cardinality then $F \approx F' \leftrightarrow \mathrm{Abs}(F) \approx \mathrm{Abs}(F')$, provided* Abs (F) *is quasi-finite.*

This last proviso will be removed in the next section.

5. The isomorphism theorem for hyper-finite fields

The purpose of this section is to establish the following isomorphism theorem on which all our results are based.

THEOREM 1. *Let F, F' be extensions of a field E such that*

(a) *E is relatively algebraically closed in F and F':*

(b) *F and F' are hyper-finite;*

(c) $\#F = \#F' > \#E$.

Then $F \approx_E F'$.

Remark. Theorem 1 differs from Proposition 1 only in that we no longer require E to be quasi-finite.

As an immediate consequence of Theorem 1 we obtain the following fact.

THEOREM 2. *If F, F' are hyper-finite of the same cardinality, then* $F \approx F' \leftrightarrow \mathrm{Abs}(F) \approx \mathrm{Abs}(F')$.

It follows from Lemma 3 of §1 that there exists a quasi-finite relatively algebraically closed subfield E_1 of F containing E and such that $\#E_1 < \#F$. Moreover by Lemma 1 of § 4, there exists an E-monomorphism $E_1 \xrightarrow{\varphi} F'$. If we knew $\varphi(E_1)$ was relatively algebraically closed in F', then by Proposition 1 of § 4 could extend φ to an E-isomorphism $F \to F'$ and so establish Theorem 1. We have thus reduced Theorem 1 to the following fact whose proof is unfortunately rather complicated.

PROPOSITION 2. *Let E, F be regular extensions of a field K such that*

(a) *E is quasi-finite, F is hyper-finite;*

(b) $\#E < \#F$.

Then there exists a K-monomorphism $E \xrightarrow{\varphi} F$ such that $\varphi(E)$ is relatively algebraically closed in F.

We need some preliminary considerations. If L is any field with at most one extension of each degree then we can assign as in § 1 to each algebraic extension L'/L a supernatural number s and write $[L' : L] = s$. Let A be the set of primes p such that $p \nmid [\tilde{K} : K]$. For each $p \in A$ let ζ_p be a generator of the group of all p^{th} roots of unity in $\tilde{K}$ and set $l(p) = [K(\zeta_p) : K] - 1$. Until further notice we assume $\mathrm{char}\, K \notin A$. This restriction will be removed later. Thus for each $p \in A$, $F(\zeta_p)_p$ is a Kummer extension of $F(\zeta_p)$ and so there exists $\beta_p \in F(\zeta_p)_p$ such that $F(\zeta_p)_p = F(\zeta_p, \beta_p)$ and $\alpha_p = \beta_p^p \in F(\zeta_p)$. Now there exist unique $a_0^{(p)}, \cdots, a_{l(p)}^{(p)} \in F$ such that

$$\alpha_p = \sum_{\lambda=0}^{l(p)} a_\lambda^{(p)} \zeta_p^\lambda.$$

This follows from the fact that

$$[F(\zeta_p) : F] = [K(\zeta_p) : K] = l(p) + 1$$

by disjointness. Let D be any relatively algebraically closed quasi-finite subfield of F containing $K(a_\lambda^{(p)} : p \in A, \lambda = 0, \cdots, l(p))$ such that $\#D < \#F$. Let δ denote the supernatural number $\prod_{p \in A} p^1$. Since $(\delta, [\tilde{K} : K]) = 1$, D_δ and $D(\zeta_p : p \in A)$ are linearly disjoint over D. For each $p \in A$ let $D_\delta(\zeta_p) \ni \gamma \to M_p(\gamma)$ denote the matrix representation with respect to the basis $1, \zeta_p, \cdots, \zeta_p^{l(p)}$

of the regular representation of $D_\delta(\zeta_p)$ over D_δ. Explicitly we have for all $u_0, \cdots, u_{l(p)}, v_0, \cdots, v_{l(p)} \in D_\delta$ and $\gamma \in D_\delta(\zeta_p)$ that

$$(u_0 \cdots u_{l(p)})M_p(\gamma) = (v_0 \cdots v_{l(p)}) \longleftrightarrow \gamma \sum_{\lambda=0}^{l(p)} u_\lambda \zeta_p^\lambda = \sum_{\lambda=0}^{l(p)} v_\lambda \zeta_p^\lambda .$$

Moreover $M_p(\gamma)$ has entries in any subfield D' of D_δ such that $D' \supseteq K$ and $\gamma \in D'(\zeta_p)$. In particular, $M_p(\zeta_p)$ has entries in K.

LEMMA 1. *For each $p \in A$, $\mathcal{G}(D_\delta/D_{\delta/p})$ is cyclic of order p. If σ_p is a generator then D is the fixed field of $\{\sigma_p : p \in A\}$.*

PROOF. $[D_\delta : D_{\delta/p}] = p$ which implies the first assertion. The second assertion now follows from the fact that $D = \bigcap_{p \in A} D_{\delta/p}$.

LEMMA 2. *For $p \in A$, there exists a unique*

$$\tau_p \in \mathcal{G}\big(D_\delta(\zeta_q : q \in A)/D_{\delta/p}(\zeta_q : q \in A)\big)$$

such that $\tau_p \mid D_\delta = \sigma_p$.

PROOF. This follows from the linear disjointness of D_δ and $D(\zeta_q : q \in A)$ over D.

LEMMA 3. $\tau_p M_p(\beta_p) = M_p(\tau_p \beta_p)$ *for* $p \in A$.

PROOF. If $u_0, \cdots, u_{l(p)} \in D$, then

$$(u_0 \cdots u_{l(p)})\tau_p M_p(\beta_p) = \tau_p\big((u_0 \cdots u_{l(p)})M_p(\beta_p)\big) .$$

Now there exist $v_0, \cdots, v_{l(p)} \in D_\delta$ such that

$$\beta \sum_{\lambda=0}^{l(p)} u_\lambda \zeta_p^\lambda = \sum_{\lambda=0}^{l(p)} v_\lambda \zeta_p^\lambda .$$

Thus

$$\tau_p \beta \sum_{\lambda=0}^{l(p)} u_\lambda \zeta_p^\lambda = \sum_{\lambda=0}^{l(p)} \tau_p(v_\lambda)\zeta_p^\lambda .$$

Thus

$$\begin{aligned}(u_0 \cdots u_{l(p)})M_p\big(\tau_p(\beta)\big) &= \tau_p(v_0 \cdots v_{l(p)}) \\ &= \tau_p\big((u_0 \cdots u_{l(p)})M_p(\beta_p)\big) = (u_0 \cdots u_{l(p)})\tau_p M_p(\beta_p) .\end{aligned}$$

It follows that $\tau_p M_p(\beta_p) = M_p(\tau_p \beta_p)$.

Recall that $M_p(\beta_p)$ has entries in D_δ.

LEMMA 4. $\sigma_p M_p(\beta_p) = M_p(\zeta_p)^i M_p(\beta_p)$ *for some* $i = i(p) \in \mathbf{Z}$, *for* $p \in A$.

PROOF. By Lemma 3, $\sigma_p M_p(\beta_p) = \tau_p M_p(\beta_p) = M_p(\tau_p \beta_p)$. Now $(\tau_p \beta_p)^p = \tau_p \beta_p^p = \tau_p \alpha_p = \alpha_p \in D(\zeta_p)$ so $\exists i \in Z$ such that $\tau_p \beta_p = \zeta_p^i \beta_p$ and the lemma follows.

Now as above there exist, for each $p \in A$,

$$x_0^{(p)}, \cdots, x_{l(p)}^{(p)} \in E, \; z_0^{(p)}, \cdots, z_{l(p)}^{(p)} \in E_p$$

such that $U^p - \sum_{\lambda=0}^{l(p)} x_\lambda^{(p)} \zeta_p^\lambda$ is irreducible over $E(\zeta_p)$ and such that

$$\Big(\sum_{\lambda=0}^{l(p)} z_\lambda^{(p)} \zeta_p^\lambda\Big)^p = \sum_{\lambda=0}^{l(p)} x_\lambda^{(p)} \zeta_p^\lambda .$$

Let $\aleph = \#E$. Then there exist $y_\nu \in E$ for $\nu < \aleph$ such that

$$E = K[x_\lambda^{(p)}, y_\nu : p \in A, \lambda = 0, \cdots, l(p), \nu < \aleph] .$$

Set $S = K[X_\lambda^{(p)}, Y_\nu, Z_\lambda^{(p)} : p \in A, \lambda = 0, \cdots, l(p), \nu < \aleph]$. Let I be the kernel of the K-surjection

$$S \xrightarrow{\psi} E[z_\lambda^{(p)} : p \in A, \lambda = 0, \cdots, l(p)] = B$$

where $\psi(X_\lambda^{(p)}) = x_\lambda^{(p)}$, $\psi(Y_\nu) = y_\nu$, $\psi(Z_\lambda^{(p)}) = z_\lambda^{(p)}$. Since E is a regular extension of K and since $([B : E], [\tilde{K} : K]) = 1$, B is a regular extension of K. Thus I is an absolutely prime ideal of S.

LEMMA 5. *For each* $p \in A$,

$$E_{\delta/p}(z_0^{(p)}, \cdots, z_{l(p)}^{(p)}) = E_\delta$$

and the natural restriction map $\mathcal{G}(E_\delta(\zeta_p)/E_{\delta/p}(\zeta_p)) \to \mathcal{G}(E_\delta/E_{\delta/p})$ *is an isomorphism.*

PROOF. $E_{\delta/p}(z_0^{(p)}, \cdots, z_{l(p)}^{(p)}, \zeta_p) \supseteq E_{\delta/p}(\zeta_p, \sum_{\lambda=0}^{l(p)} z_\lambda^{(p)} \zeta_p^\lambda)$ and so

$$[E_{\delta/p}(z_0^{(p)}, \cdots, z_{l(p)}^{(p)}, \zeta_p) : E] = \delta(l(p) + 1) .$$

The lemma follows.

LEMMA 6. *There exists*

$$\rho_p \in \mathcal{G}(E(z_\lambda^{(q)} : q \in A, \lambda = 0, \cdots, l(q))/E(z_\lambda^{(q)} : q \in A \sim p, \lambda = 0, \cdots, l(q))$$

such that

$$\rho_p(z_0^{(p)} \cdots z_0^{l(p)}) = (z_0^{(p)} \cdots z_0^{l(p)}) M_p(\zeta_p) \qquad \text{for } p \in A .$$

PROOF. $E(z_\lambda^{(q)} : q \in A \sim p, \lambda = 0, \cdots, l(q)) = E_{\delta/p}$ and $E_\delta = E(z_\lambda^{(q)} : q \in A, \lambda = 0, \cdots, l(q))$. By Lemma 5 there exists $\rho_p \in \mathcal{G}(E_\delta/E_{\delta/p})$ such that

$$\rho_p \sum_{\lambda=0}^{l(p)} z_\lambda^{(p)} \zeta_p^\lambda = \zeta_p \sum_{\lambda=0}^{l(p)} z_\lambda^{(p)} \zeta_p^\lambda .$$

The lemma follows.

COROLLARY. *I is transformed into itself under the substitutions of S defined by*

$$(Z_0^{(p)}, \cdots, Z_{l(p)}^{(p)}) = Z^{(p)} \longrightarrow Z^{(p)} M_p(\zeta_p) = (Z_0^{(p)} \cdots Z_{l(p)}^{(p)}) M_p(\zeta_p) \quad \text{for all } p \in A .$$

Now let $S = K[X, Y, Z] \xrightarrow{\mu} D_\delta[X, Y, Z]$ be the K-monomorphism obtained by substituting for every $p \in A$, $Z^{(p)} \to Z^{(p)} M_p(\beta_p)$.

LEMMA 7. *For each $g \in I$ and each $p \in A$ there exists $h \in I$ such that* $\sigma_p \mu(g) = \mu(h)$.

PROOF. $\sigma_p \mu(g)$ is obtained from $\mu(g)$ by the substitution $Z^{(p)} \to Z^{(p)} M_p(\zeta_p)^i$ for some $i \in \mathbf{Z}$, according to Lemma 4. By the Corollary to Lemma 6 there exists $h \in I$ such that $g \to h$ under the substitution $Z^{(p)} \to Z^{(p)} M_p(\zeta_p)^i$. Then

$\sigma_p\mu(g) = \mu(h)$.

COROLLARY. *$\mu(I)$ is transformed into itself by $\{\sigma_p : p \in A\}$.*

LEMMA 8. *There exists an ideal J of $D[X, Y, Z]$ such that*

$$D_\delta J = D_\delta[X, Y, Z]\mu(I) .$$

J is absolutely prime.

PROOF. By the remarks at the end of § 2 and the Corollary to Lemma 1, J exists. Now there exists a unique D_δ-automorphism λ of $D_\delta[X, Y, Z]$ extending μ. λ transforms $D_\delta I$ into $D_\delta J$. Since I is absolutely prime we have that $D_\delta I$ and hence $D_\delta J$ is absolutely prime. Thus J is absolutely prime.

PROOF OF PROPOSITION 2 (char $K \notin A$). $D[X, Y, Z]/J$ is absolutely entire over D. Since F is hyper-finite and $\#D[X, Y, Z] \leqq \aleph_0\aleph(\#D) < \#F$, there exists, by Lemma 1 of § 4, a D-homomorphism $D[X, Y, Z] \xrightarrow{\xi} F$ with kernel J. Since μ fixes $K[X, Y]$,

$$I \cap K[X, Y] = \mu(I) \cap K[X, Y] \subseteq J \cap K[X, Y] .$$

Now $K[X, Y]/I \cap K[X, Y] \approx_K E$ so that $I \cap K[X, Y]$ is a maximal ideal of $K[X, Y]$. Thus $I \cap K[X, Y] = J \cap K[X, Y]$. It follows that $K(\xi(X), \xi(Y)) \approx_K E$ and that there is a unique K-monomorphism $E \xrightarrow{\varphi} F$ such that $\varphi(x_\lambda^{(p)}) = \xi(X_\lambda^{(p)})$ and $\varphi(y_\nu) = \xi(Y_\nu)$. We now claim that for $p \in A$,

$$U^p - \sum_{\lambda=0}^{l(p)} \varphi(x_\lambda^{(p)})\zeta_p^\lambda$$

is irreducible over $F(\zeta_p)$. There exist $\Gamma_\lambda^{(p)}(Z^{(p)}) \in K[Z_0^{(p)}, \cdots, Z_{l(p)}^{(p)}]$ such that

$$\Big(\sum_{\lambda=0}^{l(p)} Z_\lambda^{(p)}\zeta_p^\lambda\Big)^p = \sum_{\lambda=0}^{l(p)} \Gamma_\lambda^{(p)}(Z^{(p)})\zeta_p^\lambda \qquad \text{for } p \in A,\ \lambda = 0, \cdots, l(p) .$$

Then for $p \in A$,

$$\sum_{\lambda=0}^{l(p)} x_\lambda^{(p)}\zeta_p^\lambda = \Big(\sum_{\lambda=0}^{l(p)} z_\lambda^{(p)}\zeta_p^\lambda\Big)^p = \sum_{\lambda=0}^{l(p)} \Gamma_\lambda^{(p)}(z^{(p)})\zeta_p^\lambda .$$

Since $x_\lambda^{(p)}, z_\lambda^{(p)} \in E_\delta$ and $1, \zeta_p, \cdots, \zeta_p^{l(p)}$ are linearly independent over E_δ we have $x_\lambda^{(p)} = \Gamma_\lambda^{(p)}(z^{(p)})$, i.e., $X_\lambda^{(p)} - \Gamma_\lambda^{(p)}(Z^{(p)}) \in I$. Thus

$$X_\lambda^{(p)} - \Gamma_\lambda^{(p)}\big(Z^{(p)}M_p(\beta_p)\big) \in \mu(I) \subseteq D_\delta J .$$

Now in $D_\delta(\zeta_p)[X, Y, Z]$ we have

$$\Big(\beta_p \sum_{\lambda=0}^{l(p)} Z_\lambda^{(p)}\zeta_p^\lambda\Big)^p = \Big(\sum_{\lambda=0}^{l(p)} V_\lambda\zeta_p^\lambda\Big)^p$$

where V_λ is the λ^{th} entry of $Z^{(p)}M_p(\beta_p)$. Thus

$$\beta_p^p\Big(\sum_{\lambda=0}^{l(p)} Z_\lambda^{(p)}\zeta_p^\lambda\Big)^p = \sum_{\lambda=0}^{l(p)} \Gamma_\lambda^{(p)}\big(Z^{(p)}M_p(\beta_p)\big)\zeta_p^\lambda .$$

Hence

$$u = \alpha_p\Big(\sum_{\lambda=0}^{l(p)} Z_\lambda^{(p)}\zeta_p^\lambda\Big)^p - \sum_{\lambda=0}^{l(p)} X_\lambda^{(p)}\zeta_p^\lambda \in D_\delta(\zeta_p)J .$$

Since $u \in D(\zeta_p)[X, Y, Z]$, we conclude $u \in D(\zeta_p)J$. As ξ extends uniquely to a

$D(\zeta_p)$-homomorphism, $D(\zeta_p)[X, Y, Z] \to F(\zeta_p)$ with kernel $D(\zeta_p)J$, we have

$$\alpha_p\left(\sum_{\lambda=0}^{l(p)} \xi(Z_\lambda^{(p)})\zeta_p^\lambda\right)^p = \sum_{\lambda=0}^{l(p)} \xi(X_\lambda^{(p)})\zeta_p^\lambda = \sum_{\lambda=0}^{l(p)} \varphi(x_\lambda^{(p)})\zeta_p^\lambda$$

in $F(\xi_p)$. Since $\left(\sum_{\lambda=0}^{l(p)} \xi(Z_\lambda^{(p)})\zeta_p^\lambda\right)^p$ is a p^{th} power in $F(\zeta_p)$ and, since $U^p - \alpha_p$ is irreducible over $F(\zeta_p)$, our claim that $U^p - \sum_{\lambda=0}^{l(p)} \varphi(x_\lambda^{(p)})\zeta_p^\lambda$ is irreducible over $F(\zeta_p)$ is established.

If $q \in A$, let $f_q = U^q - \sum_{q=0}^{l(q)} \varphi(X_\lambda^{(q)})\zeta_q^\lambda$, and if $q \notin A$ is a prime, let f_q be the irreducible polynomial in $K[U]$ defining an extension of K of degree q and let $m(q) = 1$. Then for all primes q, $f_q \in \varphi(E)_{m(q)}[U]$ is irreducible over $F_{m(q)}$ and $q \nmid m(q)$. By Lemma 4 of §1, $\varphi(E)$ is relatively algebraically closed in F. This completes the proof of Proposition 2 if char $K \notin A$.

We now briefly indicate the modifications necessary to remove the restriction that char $K \notin A$. Suppose $r = \text{char } K \in A$. Then set $l(r) = 0$. There exists by Artin-Schreier theory $\alpha_r \in F$ and $\beta_r \in F_r$ such that $U^r - U - \alpha_r$ is irreducible over F and $\beta_r^r - \beta_r = \alpha_r$. Instead of using linear transformations $Z^{(r)} \to Z^{(r)}M_r(\beta_r)$ and $Z^{(r)} \to Z^{(r)}M_r(\zeta_r)$ we use the affine transformations $Z_0^{(r)} \to Z_0^{(r)} + \beta_r$ and $Z_0^{(r)} \to Z_0^{(r)} + 1$. The proof carries through as before; we omit the details. We have therefore established Proposition 2 and thereby proved Theorem 1.

6. The Riemann hypothesis for curves

The Riemann hypothesis for curves as proved by Weil asserts [1, 2nd Part, § IV, Th. 13, Cor. 3] that if k is a finite field with q elements, and if C is a complete non-singular curve of genes g defined over k, then the number N of k-valued points of C satisfies $|N - q - 1| \leqq 2gq^{1/2}$.

LEMMA 1. *Let $M \in \mathbf{Z}_{>0}$ then we can find $\alpha(M) \in \mathbf{Z}_{>0}$ with the following property. For all fields k such that $\#k > \alpha(M)$ and for all*

$$f_1, \cdots, f_M \in k[X_1, \cdots, X_M]$$

such that the ideal $I = \langle f_1, \cdots, f_M \rangle$ in $k[X_1, \cdots, X_M]$ is absolutely prime, $\deg f_1, \cdots, \deg f_M \leq M$ *and* $\text{trans deg}_k\, k[X]/I \geqq 1$, *there exist*

$$g_1, \cdots, g_{\alpha(M)} \in k[X_1, \cdots, X_M]$$

of degree at most $\alpha(M)$ such that $I' = \langle I, g_1, \cdots, g_{\alpha(M)} \rangle$ is absolutely prime and $\text{trans deg}_k\, k[X]/I' = 1$.

The principle of a demonstration of this lemma can be found in [8, § 2; 17]. An exact proof would be tedious though trivial and so is omitted.

LEMMA 2. *With the notation of Lemma* 1, *we can find $\beta(M) \in \mathbf{Z}_{>0}$ such that if $\#k \geqq \beta(M)$, then V has a k-valued point.*

PROOF. The genus of the projective normalization C' of a projective

completion of C can be bounded by a function of M and $\alpha(M)$. Also the number of k-rational points of C' minus the number of k-rational points of C can be bounded by a function of M and $\alpha(M)$. The existence of $\beta(M)$ now follows from the Riemann hypothesis.

COROLLARY. *If* $s = \prod p^{n(p)} \in \mathbf{Z}_*$ *is such that* $n(p) \neq \infty$ *for all* p *and* $n(p) \neq 0$ *for infinitely many* p, *then for any finite field* k, k_s *is pseudo-finite.*

7. Ultraproducts of finite fields

A proof of the following lemma can be found in [9].

LEMMA 1. *Let* $f_1(U, X), \cdots, f_M(U, X) \in \mathbf{Z}[U_1, \cdots, U_L, X_1, \cdots, X_N]$. *Then we can find an elementary formula* $E(U)$ *with* $U_1, \cdots, U_M$ *as its free variables such that if* k *is a perfect field and* $u_1, \cdots, u_L \in k$, *then* $\langle f_1(u, X), \cdots, f_M(u, X)\rangle$ *is an absolutely prime ideal of* $k[X_1, \cdots, X_N] \leftrightarrow E(u)$ *is true in* k.

Now let $k(\nu)$ be finite fields for $\nu \in \mathbf{Z}_{>0}$ such that $\sharp k(\nu) \to \infty$ as $\nu \to \infty$. Let $f_1, \cdots, f_M \in \mathbf{Z}[U_1, \cdots, U_L, X_1, \cdots, X_N]$. Let D be a non-principal ultrafilter D on $\mathbf{Z}_{>0}$ and let $\mathcal{K} = \prod k(\nu)/D$ be the corresponding ultraproduct. Suppose $c_\lambda(\nu) \in k(\nu)$ are such that if c_λ^* denote the element of $\mathcal{K}$ represented by $(c_\lambda(\nu))_{\nu \in Z>0}$ for $\lambda = 1, \cdots, L$, then

$$\langle f_1(c_1^*, \cdots, c_L^*, X_1, \cdots, X_N), \cdots, f_M(c^*, X)\rangle$$

is absolutely prime in $\mathcal{K}[X_1, \cdots, X_N]$. It follows from Lemma 1 that $d = \{\nu \mid \langle f_1(c(\nu), X), \cdots, f_M(c(\nu), X)\rangle$ is absolutely prime in $k(\nu)[X]\} \in D$. It follows from Lemma 2 of § 6 that there exists a finite subset s of $\mathbf{Z}_{>0}$ such for $\nu \in d - s$ there exist $x_j(\nu) \in k(\nu)$ for $j = 1, \cdots, N$ such that $f_1(c(\nu), x(\nu)) = \cdots = f_M(c(\nu), x(\nu)) = 0$ in $k(\nu)$. Thus $f_1(c^*, x^*) = \cdots = f_M(c^*, x^*) = 0$ in $\mathcal{K}$. We have proved the following fact, since $\mathcal{K}$ is quasi-finite (cf. § 8).

LEMMA 2. $\mathcal{K}$ *is pseudo-finite.*

For the remainder of this paper we assume the continuum hypothesis $2^{\aleph_0} = \aleph_1$.

All of our decidability and arithmetic applications can be freed of this assumption in several ways as in [11, § 3] even though our proofs of isomorphisms of ultraproducts (from which these applications are deduced) depend on the continuum hypothesis.

PROPOSITION 3. *Every non-principal ultraproduct of non-isomorphic finite fields is hyper-finite.*

PROOF. Let $\mathcal{K}$ be as above. Let E be a countable subfield of $\mathcal{K}$ and let I be an absolutely prime ideal of $S = E[X_j : j \in \mathbf{Z}_{>0}]$. For $n \in \mathbf{Z}_{>0}$ let $I_n = I \cap E[X_1, \cdots, X_n]$. Let $I_n = \langle f_1^{(n)}, \cdots, f_{M(n)}^{(n)}\rangle$. Then $I = \bigcup_n I_n$. It suffices

to prove that there exist $x_j \in \mathcal{K}$ for $j \in \mathbf{Z}_{>0}$ such that $f_\mu^{(n)}(x_1, \cdots, x_n) = 0$ for $n \in \mathbf{Z}_{>0}$, $\mu = 1, \cdots, M(n)$. Since I_n is absolutely prime, it follows from Lemma 2 and Lemma 1 of § 3 that for all $n \in \mathbf{Z}_{>0}$ there exist $x_1^{(n)}, \cdots, x_n^{(n)} \in \mathcal{K}$ such that $f_\mu^{(j)}(x_1^{(n)}, \cdots, x_n^{(n)}) = 0$ for $j = 1, \cdots, n$, $\mu = 1, \cdots, M(j)$. By the saturation property of $\mathcal{K}$ [16, Ch. IX, Th. 3] there exist $x_j \in \mathcal{K}$ for $j \in \mathbf{Z}_{>0}$ such that $f_\mu^{(n)}(x_1, \cdots, x_n) = 0$ for $n \in \mathbf{Z}_{>0}$, $\mu = 1, \cdots, M(n)$. (Usually the saturation property is formulated only for formulas with one free variable. But then we can find x_1 such that for all n there exist $x_2^{(n)}, \cdots, x_n^{(n)}$ such that $f_\mu^{(j)}(x_1, x_2^{(n)}, \cdots, x_n^{(n)}) = 0$ for $j = 1, \cdots, n$ and $\mu = 1, \cdots, M(j)$. Then applying the one variable saturation property again we get that there exists x_2 such that for all n there exist $x_3^{(n)}, \cdots, x_n^{(n)}$ etc.) This completes the proof.

THEOREM 3. *If $\mathcal{K}$, $\mathcal{K}'$ are non-principal ultraproducts of non-isomorphic finite fields, then $\mathcal{K} \approx \mathcal{K}' \leftrightarrow \mathrm{Abs}(\mathcal{K}) \approx \mathrm{Abs}(\mathcal{K}')$.*

PROOF. This follows from Proposition 3 and Theorem 2 of § 5 since we have $\#\mathcal{K} = \#\mathcal{K}' = 2^{\aleph_0}$.

PROPOSITION 4. *An uncountable saturated pseudo-finite field is hyper-finite.*

PROOF. The proof is similar to the proof of Proposition 3.

Remark. It is easy to prove Lemma 1 with "absolutely prime ideal" replaced by "ideal with an absolutely prime radical". Moreover it would be possible to use the lemma in this form at the expense of certain tedious complications.

8. Elemenary equivalence of pseudo-finite fields

As in [8, § 4, Th. 5], there exists an elementary statement C_n such that a field F has precisely one extension of degree $n \leftrightarrow C_n$ holds in F for all $n \in \mathbf{Z}_{>0}$. Clearly there exist for all primes q an elementary statement P_q such that either $q \neq 0$ in F or every element in F is a q^{th} power. Thus F is quasi-finite $\leftrightarrow C_n$ and P_q hold in F for all n and q. For each $D, M, N \in \mathbf{Z}_{>0}$ there exist $L = L(D, M, N)$ and

$$f_1, \cdots, f_M \in \mathbf{Z}[U_1, \cdots, U_L, X_1, \cdots, X_N]$$

comprising the "general" sequence of M polynomials of degree at most D in $X_1, \cdots, X_N$. By Lemma 1 of § 7 there exists an elementary formula $B(D, M, N)(U_1, \cdots, U_L)$ in the free variables $U_1, \cdots, U_L$ such that if F is a field and $u_1, \cdots, u_L \in F$, then $\langle f_1(u, X), \cdots, f_M(u, X)\rangle$ is absolutely prime in $F[X_1, \cdots, X_N] \leftrightarrow B(D, M, N)(u_1, \cdots, u_L)$ is true in F. Let $E(D, M, N)$ be the elementary statement

$$\forall U_1, \cdots, U_L[B(D, M, N)(U_1, \cdots, U_L) \longrightarrow \exists X_1, \cdots, X_n f(U, X) = \cdots = f_M(U, X) = 0] .$$

Let $\Pi = \{C_n, P_q, B(D, M, N) : \text{all } n, q, D, M, N\}$. Then F is pseudo-finite $\leftrightarrow$ Π holds in F. We have thus elementarily axiomatized pseudo-finite fields in a recursive way. Moreover each C_n and P_q are true in every finite field while by Lemma 2 of § 6 and Lemma 1 of § 7 each $B(D, M, N)$ holds in R_q for all but a finite set of q which we can explicitly find.

PROPOSITION 5. *Every pseudo-finite field is elementarily equivalent to a hyper-finite field.*

PROOF. Every field is elementarily equivalent to a saturated field (for example take a countable elementarily equivalent subfield and then take a non-principal countable ultrapower). Proposition 4 of § 7 now implies Proposition 5 since the axioms for being pseudo-finite are elementarily expressible.

LEMMA 1. *If F, F' are algebraic extensions of a field E, then*

$$\{f \in \mathbf{E}[X_1] \mid f \text{ has a root in } F\} = \{f \in E[X_1] \mid f \text{ has a root in } F'\} \longleftrightarrow F \approx_E F' .$$

PROOF. The proof is easy and is carried out in [8, § 3, Lemma 5].

$A \equiv B$ means A is elementarily equivalent to B.

LEMMA 2. *Let E and F be fields. Then*

$$E \equiv F \longrightarrow \text{Abs}(E) \approx \text{Abs}(F) .$$

PROOF. Assume $E \equiv F$. Then Char E = Char F. Let R be the prime field of E which we may regard as a common subfield of E and F. Moreover

$$\{f \in Z[X_1] \mid f \text{ has a root in } E\} = \{f \in Z[X_1] \mid f \text{ has a root in } F\} .$$

It follows from Lemma 1 that Abs $(E) \approx$ Abs (F).

THEOREM 4. *Let F, F' be pseudo-finite. Then*

$$F \equiv F' \longleftrightarrow \text{Abs}(F) \approx \text{Abs}(F') .$$

PROOF. ($\rightarrow$) follows from Lemma 2. To prove the reverse implication we may assume F, F' are saturated of cardinality $\aleph_1$. Then $F \approx F'$ by Theorem 2 of § 5 and Proposition 4 of § 7. This proves the theorem.

Definition. If F is a field, $[F] = \{f \in Z[X_1] \mid f \text{ has a root in } F\}$.

THEOREM 5. *Let F be pseudo-finite. Then*

$$\Pi_F = \Pi \cup \{[\exists X_1 f(X_1) = 0] : f \in [F]\} \cup \{\forall X_1 f(X_1) \neq 0 : f \in \mathbf{Z}[X_1] - [F]\}$$

is a complete set of axioms for F, i.e., F' satisfies $\Pi_F \leftrightarrow F \equiv F'$.

PROOF. Theorem 5 is an immediate consequence of Lemma 1, 2, and Theorem 4.

Remark. These axioms are not model-complete. To verify this assertion, let D be a non-principal ultrafilter on $\mathcal{P}$ such that if $\mathcal{R} = \prod_p R_p/D$ then $\mathrm{Abs}(\mathcal{R}) \approx \tilde{Q}$. This is possible by Theorem 7 of § 10; it is also easy to verify directly. Now set $\mathcal{R}' = \prod_p R_{p^2}/D$. Then $\mathcal{R} \subset \mathcal{R}'$ so that $\mathrm{Abs}(\mathcal{R}') = \tilde{Q}$. It follows from Theorem 4, that $\mathcal{R} \equiv \mathcal{R}'$ (in fact by Theorem 3 of § 7, $\mathcal{R} \approx \mathcal{R}'$). On the other hand $[\mathcal{R}' : \mathcal{R}] = 2$, so there exists $r \in \mathcal{R}$ such that $[\exists X_1 X_1^2 = r]$ is true in $\mathcal{R}'$ but not in $\mathcal{R}$. Similar examples can be given in any characteristic.

The results of the rest of this section are not used in the sequel.

LEMMA 3. *Let S_i, S_i' be rings of cardinality at most the continuum for $i \in \mathbf{Z}_{>0}$. Suppose that for every non-principal ultrafilter D on $\mathbf{Z}_{>0}$ we have*

$$\prod S_i/D \equiv \prod S_i'/D \ .$$

Then $\mathcal{S} = \prod S_i/\bigoplus S_i \approx \prod S_i'/\bigoplus S_i = \mathcal{S}'$.

PROOF. The standard proof [16, Ch. IX, Th. 3] that the non-principal ultraproduct of the S_i are saturated is easily modified to show that $\mathcal{S}$ and $\mathcal{S}'$ are saturated. Since elementarily equivalent saturated systems of the same cardinality are isomorphic [16, Ch. IX, Th. 2], it suffices to prove that $\mathcal{S} \equiv \mathcal{S}'$. Now if E is any elementary statement about rings, then $\{i \mid E \text{ holds in } S_i\}$ and $\{i \mid E \text{ holds in } S_i'\}$ differ by a finite set; otherwise we could find an ultrafilter D such that E holds in precisely one of $\prod S_i/D$ and $\prod S_i'/D$. It now follows from [10, Th. 3.1] that $\mathcal{S} \equiv \mathcal{S}'$. This completes the proof.

LEMMA 4. *Let k_i for $i \in \mathbf{Z}_{>0}$ be pairwise non-isomorphic finite fields. For each $i \in \mathbf{Z}_{>0}$, let k_i' be a finite extension of k_i. Suppose that for all $d \in \mathbf{Z}_{>1}$, $\{i : d \mid [k_i' : k_i]\}$ is finite. Then for every non-principal ultrafilter D on $\mathbf{Z}_{>0}$,*

$$\mathcal{K} = \prod k_i/D \approx \prod k_i'/D = \mathcal{K}' \ .$$

PROOF. Let $f \in \mathbf{Z}[X_1]$ be monic. Then f has a root in $\mathcal{K} \leftrightarrow h = \{i : f \text{ has a root in } k_i\} \in D$. If f has a root in k_i' but not in k_i, then $[k_i' : k_i]$ has a divisor d with $1 < d \leqq \deg(f)$. By our hypothesis this can happen for only finitely many $i \in \mathbf{Z}_{>0}$. Thus $h' = \{i : f \text{ has a root in } k_i'\}$, and h differ by a finite set. It follows that f has a root in $\mathcal{K} \leftrightarrow f$ has a root in $\mathcal{K}'$.

By Theorem 5, $\mathcal{K} \equiv \mathcal{K}'$ and so $\mathcal{K} \approx \mathcal{K}'$.

COROLLARY. $\prod k_i/\bigoplus k_i \approx \prod k_i'/\bigoplus k_i'$.

PROOF. Combine Lemmas 3 and 4.

Example. $\prod R_p/\bigoplus R_p \approx \prod R_{p^p}/\bigoplus R_{p^p}$.

This is Theorem B of the introduction.

9. The decision procedure for one variable statement.

Definition. For $n \in \mathbf{Z}_{>0}$, we set $\delta(n) = \{m \in \mathbf{Z}_{>0} : m \mid n\}$.

Definition. If $n \in \mathbf{Z}_{>0}$ and $W \subset \delta(n)$, then we set

$$a(n, W) = \{m \in \mathbf{Z}_{>0} \mid \gcd(n, m) \in W\}$$

The proof of the following properties of $a(n, W)$ is omitted.

LEMMA 1. (i) *If* $n \mid n'$, *then* $a(n, W) = a(n', W')$ *where*

$$W' = \{d \in \mathbf{Z}_{>0} : d \mid n' \text{ and } \gcd(n, d) \in W\} .$$

(ii) $\sim a(n, W) = a(n, \delta(n) \sim W)$.

(iii) $a(n, W) \cup a(n, W') = a(n, W \cup W')$.

Definition. $\mathfrak{A} = \{a(n, W) \mid n \in \mathbf{Z}_{>0}, W \subseteq \delta(n)\}$.

COROLLARY. $\mathfrak{A}$ *is a boolean algebra. If* $\varphi(X_1, \cdots, X_s)$ *is an explicit boolean polynomial, if* $n_1, \cdots, n_s$ *are given positive integers, and if* $W_\sigma \subset \delta(n_\sigma)$ *for* $\sigma = 1, \cdots, s$. *Then we can compute in a finite number of steps* $m \in \mathbf{Z}_{>0}$ *and* $V \subset \delta(m)$ *such that*

$$\varphi\big(a(n_1, W_1), \cdots, a(n_s, W_s)\big) = a(m, V) .$$

Moreover, we can decide in a finite number of steps whether $a(m, V)$ *is* $\mathbf{Z}_{>0}$ *or is cofinite in* $\mathbf{Z}_{>0}$ *since*

$$a(m, V) = \mathbf{Z}_{>0} \longleftrightarrow V = \delta(m) \longleftrightarrow a(m, V)$$

is cofinite in $\mathbf{Z}_{>0}$.

Remark. If $\alpha \in \mathfrak{A}$, then α is the finite union of (infinite) arithmetic progressions, but not conversely. For example, if $\alpha \in \mathfrak{A}$ contains

$$\{m \in \mathbf{Z}_{>0} \mid m \equiv 1 \bmod 3\} \text{ then } \alpha \supseteq \{m \in \mathbf{Z}_{>0} \mid m \equiv 2 \bmod 3\} .$$

We use a bar to denote residue class.

For convenience of language we pretend from now on that there is precisely one field R_q of each prime power order q.

LEMMA 2. *Let* $f \in \mathbf{Z}[X_1]$ *be monic and let* N *be a finite normal extension of* $\mathbf{Q}$ *in which* f *factors completely. Suppose* p *is a prime such that* $p \nmid \operatorname{Disc}(f)$ *and that* K *is the decomposition subfield of* N *with respect to some prime* $\mathfrak{p}$ *of* N *above* p. *Let* $n = [N : K]$ *and*

$$W = \{[L : K] \mid K \subset L \subset N, f \text{ has a root in } L\} .$$

Then for $m \in \mathbf{Z}_{>0}$, $\bar{f}$ *has a root in* $R_{p^m} \leftrightarrow m \in a(n, W)$.

PROOF. ($\leftarrow$). Let $w = \gcd(n, m) \in W$.

Since $\operatorname{Disc}(N) \mid \operatorname{Disc}(f)$, p is unramified in N and so $\mathcal{G}(N/K)$ is cyclic of degree n. Thus f has a root $\alpha \in L$ where $[L : K] = w$. Since α is an algebraic

integer, its residue class $\bar{\alpha}$ with respect to the prime $(\mathfrak{p} \cap L)$ of L is in R_{p^w}. Thus $\bar{f}$ has a root in R_{p^w} and hence in R_{p^m}.

$(\rightarrow)$. Let $N_{\mathfrak{p}}$ be the completion of N with respect to $\mathfrak{p}$. Since $p \nmid \mathrm{Disc}(f)$, the monic irreducible factors of $\bar{f}$ over R_p are in one-to-one correspondence with the monic irreducible factors of f over $\mathbf{Q}_p$. Since $\bar{f}$ has a root in R_{p^m}, f has a monic irreducible factor g over $\mathbf{Q}_p$ of degree w where $w \mid m$. But g factors completely in $N \subset N_{\mathfrak{p}}$ and $[N_{\mathfrak{p}} : \mathbf{Q}_p] = n$. Thus $w \mid n$. Now $\mathcal{G}(N/K)$ is identified with $\mathcal{G}(N_{\mathfrak{p}}/\mathbf{Q}_p)$ by letting $\mathcal{G}(N/K)$ act on the first factor of $N \otimes_K \mathbf{Q}_p \approx_{\mathbf{Q}_p} N_{\mathfrak{p}}$. Therefore the coefficients of g (which are in N) are fixed by $\mathcal{G}(N/K)$, i.e., $g \in K[X_1]$ and g is irreducible over K. If L is the extension of K defined by a root α of g, then $\alpha \in L$, $[L : K] = w$ and $f(\alpha) = 0$. It follows that $w \in W$. As $w \mid \gcd(n, m)$, $\gcd(n, m) \in W$. Thus $m \in a(n, W)$.

COROLLARY 1. *Let f, N, p and K be as in the lemma. Then $\bar{f}$ has a root in $R_p \leftrightarrow f$ has a root in K.*

PROOF. $\bar{f}$ has a root in $R_p \leftrightarrow 1 \in a(n, W) \leftrightarrow$ there exists L such that $K \subset L \subset N$, $([L : K], n) = 1$, and f has a root in L. Since $[L : K] \mid n$, the corollary is established.

COROLLARY 2. *Let $f_1, \cdots, f_s \in \mathbf{Z}[X_1]$ be monic and let N be a finite normal extension of $\mathbf{Q}$ in which each f_σ factors completely. For each subfield K of N such that $\mathcal{G}(W/K)$ is cyclic, let*

$$W_\sigma(K) = \{[L : K] \mid K \subset L \subset N, f_\sigma \text{ has a root in } L\} \qquad \text{for } \sigma = 1, \cdots, s .$$

Then for each prime p such that $p \nmid \prod_{\sigma=1}^{s} \mathrm{Disc}(f_\sigma)$ we have for $\sigma = 1, \cdots, s$ that $\bar{f}_\sigma$ has a root in $R_{p^m} \leftrightarrow m \in a([N : K^{(p)}], W_\sigma(K^{(p)}))$ where $K^{(p)}$ is the decomposition subfield of N with respect to any prime of N above p.

COROLLARY 3. *Let $\varphi(X_1, \cdots, X_s)$ be a boolean polynomial and let $p \nmid \prod_{\sigma=1}^{s} \mathrm{Disc}(f_\sigma)$. Then*

$$\{m \mid \varphi([\exists X_1 f_1(X_1) = 0], \cdots, [\exists X_1 f_s(X_1) = 0]) \text{ holds in } R_{p^m}\}$$
$$= \varphi(a([N : K^{(p)}]), W_1(K^{(p)})), \cdots, a([N : K^{(p)}], W_s(K^{(p)})) .$$

COROLLARY 4. *Set $\lambda = \varphi([\exists X_1 f_1(X_1) = 0], \cdots, [\exists X_1 f_s(X_1) = 0])$. Then the following conditions are equivalent.*

(A) *λ holds in R_{p^m} for all $p \nmid \prod_{\sigma=1}^{s} \mathrm{Disc}(f_\sigma)$ and for all m;*

(B) *λ holds in R_{p^m} for all but a finite set of $p \nmid \prod_{\sigma=1}^{s} \mathrm{Disc}(f_\sigma)$ and all m;*

(C) *$\varphi(a([N : K], W_1(K)), \cdots, a([N : K], W_s(K))) = \mathbf{Z} > 0$ for all $K \subset N$ such that $\mathcal{G}(N/K)$ is cyclic.*

PROOF. The corollary follows from the fact that every $K \subset N$ such that $\mathcal{G}(N/K)$ is cyclic is of the form $K^{(p)}$ for infinitely many primes p.

PROPOSITION 6. *Let* $f_1, \cdots, f_s \in \mathbf{Z}[X_1]$ *be given monic polynomials and let* $\varphi(X_1, \cdots, X_s)$ *be a given boolean polynomial. Then we can decide in a finite number of steps whether or not*

$$\lambda = \varphi\big([\exists X_1 f_1(X_1) = 0], \cdots, [\exists X_1 f_s(X_1) = 0]\big)$$

holds in R_{p^m} *for all but a finite set of* p *and all* m. *If so, we can compute the precise exceptional set of* p.

PROOF. We can assume that $\prod_{\sigma=1}^{s} \mathrm{Disc}\,(f_\sigma) \neq 0$. We then find a finite normal extension N of $\mathbf{Q}$ such that f_σ factors completely in N. Then we can find all subfields K of N such that $\mathcal{G}(N/K)$ is cyclic. For each such K we can find $W_\sigma(K) = \{[L : K]\colon K \subset L \subset N,\ f_\sigma \text{ has a root in } L\}$. By Corollary 3 to Lemma 2, λ holds in R_{p^m} for all but a finite set of p and all $m \leftrightarrow$

$$\mu = \varphi\big(a([N : K], W_1), \cdots, a([N : K], W_s)\big) = \mathbf{Z}_{>0}$$

for such K. By the Corollary to Lemma 1, we can decide in a finite number of steps whether or not $\mu = \mathbf{Z}_{>0}$. This proves the first assertion. If λ holds for all but a finite set of p and all m, it follows that λ holds for all $p \nmid \prod_{\sigma=1}^{s} \mathrm{Disc}\,(f_\sigma) = D$ and all m. Now let $p \mid D$. Then we can find monic $f_1^{(p)}, \cdots, f_s^{(p)} \in \mathbf{Z}[X_1]$ such that $p \nmid \mathrm{Disc}\,(f_\sigma^{(p)})$ and such that $\overline{f_\sigma^{(p)}} \mid \overline{f_\sigma}$ and $\overline{f_\sigma} \mid (f_\sigma^{(p)})^l$ for some l where the bar denotes residue class module p. Then as above we can decide in a finite number of steps whether or not

$$\nu_p = \varphi\big([\exists X_1 f_1^{(p)}(X_1) = 0], \cdots, [\exists X_1 f_1^{(p)}(X_1) = 0]\big)$$

holds in R_{p^m} for all m. Since $\nu_p \leftrightarrow \lambda$ in each R_{p^m}, this completes the proof.

COROLLARY. *The proposition holds if some of the* f_σ *are in* $\mathbf{Z}$ *instead of being monic.*

PROOF. If $f_\sigma \in \mathbf{Z}$, we define $\mathrm{Disc}\,(f_\sigma) = f_\sigma$. Then again we can assume $D = \prod_{\sigma=1}^{s} f_\sigma \neq 0$. For the case where $p \nmid D$ we replace X_σ in φ for f_σ constant by $\sim X_\sigma$ and obtain a new boolean polynomial φ'. Then

$$\lambda \longleftrightarrow \varphi'\big([\exists X_1 g_1(X_1) = 0], \cdots, [\exists X_1 g_s(X_1) = 0]\big)$$

where $g_\sigma = f_\sigma$ if f_σ is monic and $g_\sigma(X_1)$ if f_σ is constant. If $p \mid D$, the modification is similar except that X_σ is left alone and f_σ is replaced by X_1 if f_σ is constant and $p \mid f_\sigma$.

Definition. By a *one variable statement* we mean a statement of the form

$$\varphi\big([\exists X_1 f_1(X_1) = 0], \cdots, [\exists X_1 f_s(X_1) = 0]\big)$$

where $\varphi(X_1, \cdots, X_s)$ is a boolean polynomial and $f_1, \cdots, f_s \in \mathbf{Z}[X_1]$ are monic or constant.

We have therefore proved

THEOREM 6. *Given a one variable statement E we can decide in a finite number of steps whether or not E holds in R_{pm} for all but a finite set of p and all m. If so, we can compute the precise exceptional set of p. If for some fixed p, E holds for all but a finite set of R_{pm} then E holds for all R_{pm}.*

A more complete statement is obtained by combining the corollary to Lemma 1 with the following.

THEOREM 6′. *Let $\lambda = \varphi([\exists X_1 f_1(X_1) = 0], \cdots, [\exists X_1 f_s(X_1) = 0])$ be a given one variable statement and let p be a given prime. Then we can find $m_p \in \mathbf{Z}_{>0}$ and $V_p \subset \delta(m_p)$ such that*

$$a(m_p, V_p) = \{m \mid \lambda \text{ holds in } R_{pm}\} .$$

If N is a finite normal extension of $\mathbf{Q}$ in which each f_σ factors completely, then for $p \neq \prod_{\sigma=1}^{s} \mathrm{Disc}(f_\sigma)$, m_p and V_p depend only on the decomposition subfield of a prime of N above p.

10. The absolute numbers of pseudo-finite fields

The purpose of this section is to show that the obvious necessary conditions for a field to be of the form $\mathrm{Abs}(L)$ for some non-principal ultraproduct L of finite fields are also sufficient. This implies that we get no additional fields of the form $\mathrm{Abs}(L)$ if we allow L to be an arbitrary pseudo-finite field. As we will see, this entails that every pseudo-finite field is elementarily equivalent to a non-principal ultraproduct of finite fields.

We recall that the following conditions on a perfect field K are equivalent.

(A) K has at most one extension of each degree;

(B) every finite extension L/K is cyclic;

(C) $\mathcal{G}(\tilde{K}/K)$ is procyclic.

PROPOSITION 7. *Let K be a subfield of $\tilde{\mathbf{Q}}$ such that K has at most one extension of each degree. Then there exists a non-principal ultraproduct $\mathcal{R}$ of the R_p, $p \in \mathcal{P}$ such that $K \approx \mathrm{Abs}(\mathcal{R})$.*

PROOF. For each $f \in [K]$, set $\alpha(f) = \Delta([\exists X_1 f(X_1) = 0]) \cap \mathcal{P}$; for each $g \in \mathbf{Z}[X_1] - [K]$, set $\beta(g) = \Delta([\sim \exists X_1 g(X_1) = 0]) \cap \mathcal{P}$. It suffices to show that there is a non-principal ultrafilter D on $\mathcal{P}$ such that for each $f \in [K]$, $\alpha(f) \in D$ and for each $g \in \mathbf{Z}[X_1] - [K]$, $\beta(g) \in D$. For then $[\mathcal{R}] = [K]$ and so by Lemma 1 of § 8, $\mathrm{Abs}(\mathcal{R}) \approx \mathrm{Abs}(K) = K$. Thus it suffices to establish the finite intersection property for the set

$$V = \{\alpha(f) \mid f \in [K]\} \cup \{\beta(g) \mid g \in \mathbf{Z}[X_1] - [K]\} \cup C$$

where C is the set of cofinite subsets of $\mathcal{P}$.

We claim that if $f_1, f_2 \in [K]$, then there exists $f \in [K]$ such that

$\alpha(f) - (\alpha(f_1) \cap \alpha(f_2))$ is finite. Let $\alpha_i \in K$ be a root of f_i and $\alpha \in K$ be an algebraic integer such that $\alpha_i \in \mathbf{Q}(\alpha)$, $i = 1, 2$. Let f be the monic irreducible for α over $\mathbf{Q}$. There exists a finite subset T of $\mathcal{P}$ such that if $p \in \mathcal{P} - T$, then $p \nmid \mathrm{Disc}(f)$ and α_1, α_2 are $\mathbf{Q}$-linear combinations of the powers of α with denominators prime to p. Let N be a finite normal extension of $\mathbf{Q}$ containing $\mathbf{Q}(\alpha)$. It follows from that if $p \in \alpha(f) - T$ and H is the decomposition field of a suitable prime $\mathfrak{p}$ of N above p then $\mathbf{Q}(\alpha) \subseteq H$. Taking residue classes modulo $\mathfrak{p}$ we obtain a root $\bar{\alpha}_i \in R_p$ of f_i, $i = 1, 2$. Thus $\alpha(f) - T \subseteq \alpha(f_1) \cap \alpha(f_2)$ which establishes our claim.

Also if $g_1, g_2 \in \mathbf{Z}[X_1] - [K]$, then $g_1 g_2 \in \mathbf{Z}[X_1] - [K]$ and $\beta(g_1 g_2) = \beta(g_1) \cap \beta(g_2)$.

Hence to show V has the finite intersection property we need only show that if $f \in [K]$ and $g \in \mathbf{Z}[X_1] - [K]$, then $\alpha(f) \cap \beta(g)$ is infinite.

Let H be a finite normal extension of $\mathbf{Q}$ containing all roots of g. By our hypothesis on K, KH/K is a cyclic extension. It follows that there exists a subfield K_1 of K finite over $\mathbf{Q}$ such that K_1 contains a root of f and $K_1 H/K_1$ is cyclic. Let N be a finite normal extension of $\mathbf{Q}$ containing $K_1 H$. A generator of $\mathcal{G}(K_1 H/K_1)$ extends to an automorphism τ of N. If M is the fixed field of τ, then N/M is cyclic and $K_1 H \cap M = K_1$. Suppose g has a root in M. Since g has all its roots in $K_1 H \supseteq H$, g has a root in $K \supseteq K_1 = K_1 H \cap M$, a contradiction. Thus g has no roots in M. Let A be the set of p such that M is the decomposition subfield of N of a prime above p. By Čebotarev's density theorem, A is infinite. Since $M \supseteq K_1$ and K_1 contains a root of f, it follows that $A - \alpha(f)$ is finite. As M has no root of g, it follows that $A - \beta(g)$ is finite. Thus $A - \alpha(f) \cap \beta(g)$ is finite and so $\alpha(f) \cap \beta(g)$ is infinite. This completes the proof.

A more complicated proof of this result was given in [8, § 4, Th. 5].

PROPOSITION 7′. *Every algebraic extension K of a finite field of characteristic p is isomorphic to* $\mathrm{Abs}(\mathcal{K})$ *for some non-principal ultraproduct $\mathcal{K}$ of the R_{p^m}.*

PROOF. Let $[K : R_p] = s \in \mathbf{Z}_*$. For each $n \in \mathbf{Z}_{>0}$ let $f_n \in R_p[X_1]$ be irreducible of degree n. For each $n \in \mathbf{Z}_{>0}$, let

$$b_n = \{m \in \mathbf{Z}_{>0} : \gcd(n, m) = \gcd(n, s)\} .$$

In the notation of Lemma 1 of § 9, $b_n = a(n, \{\gcd(n, s)\})$. It follows from that lemma that any finite intersection of the b_n is infinite so that there exists a non-principal ultrafilter D on $\mathbf{Z}_{>0}$ containing each b_n. Set $\mathcal{K} = \prod_n R_{p^n}/D$. If $n \in \mathbf{Z}_{>0}$ then

$R_{p^n} \subset K \longleftrightarrow n \mid s \longleftrightarrow b_n = \{m \in \mathbf{Z}_{>0} : n \mid m\} \longleftrightarrow \{m \in \mathbf{Z}_{>0} : n \mid m\} \in D \longleftrightarrow f_n$

has a root in $\mathcal{K} \leftrightarrow R_{p^n} \subset \mathcal{K}$. This proves $\mathrm{Abs}(\mathcal{K}) = K$.

We combine these results.

THEOREM 7. *A field K of absolute numbers is isomorphic to* $\mathrm{Abs}(\mathcal{K})$ *for some non-principal ultrapower $\mathcal{K}$ of the $R_q \leftrightarrow K$ has at most one extension of each degree. If* $\mathrm{char}\, K = 0$ *we may take $\mathcal{K}$ to be a non-principal ultraproduct of the R_p, $p \in \mathcal{P}$. If* $\mathrm{char}\, K = p$ *we may take $\mathcal{K}$ to be a non-principal ultraproduct of the R_{p^m}, $m \in \mathbf{Z}_{>0}$.*

11. The decidability of the theory of finite fields

THEOREM 8. *A field F is pseudo-finite $\leftrightarrow F \equiv \mathcal{K}$ for some non-principal ultrapower $\mathcal{K}$ of the R_q.*

PROOF. ($\leftarrow$) follows from Proposition 3 of § 7. Conversely assume F is pseudo-finite. Then $K = \mathrm{Abs}(F)$ has at most one extension of each degree. By Theorem 6 of § 9 there exists a non-principal ultrapower $\mathcal{K}$ of the R_q such that $\mathrm{Abs}(\mathcal{K}) \approx K$. By Theorem 4 of § 8, $F \equiv \mathcal{K}$.

We can similarly establish the following results.

THEOREM 8′. *Let p be a prime. Then a field F of characteristic p is pseudo-finite $\leftrightarrow F \equiv$ some non-principal ultraproduct of the R_{p^m}, $m \in \mathbf{Z}_{>0}$.*

THEOREM 8″. *A field F of characteristic 0 is pseudo-finite $\leftrightarrow F \equiv$ some non-principal ultraproduct of the R_p, $p \in \mathcal{P}$.*

THEOREM 9. *The following conditions on a field F are equivalent.*

(i) *F is pseudo-finite.*

(ii) *$F \equiv$ some non-principal ultraproduct of the R_q.*

(iii) *Every elementary statement true in all but a finite set of finite fields is true in F.*

(iv) *F is infinite and every elementary statement true in all finite fields is true in F.*

PROOF. (i) $\leftrightarrow$ (ii) is Theorem 8. (ii) $\rightarrow$ (iii) by the basic property of ultraproducts. (iii) $\rightarrow$ (iv) since for each $q \in \mathcal{Q}$, $[\exists X_0 X_0^q \neq X_0]$ is true in all but finitely many finite fields which implies F is infinite. Now suppose F satisfies (iv) and let $\pi \in \Pi$. Then π is true in all but a finite set $\{R_{q_1}, \cdots, R_{q_m}\}$ of finite fields. Thus $\pi \vee \bigvee_{\mu=1}^{m} [\forall X_1 X_1^{q_\mu} = X_1]$ is true in all finite fields and hence in F. Since F is infinite, π is true in F so that F is pseudo-finite. This shows (iv) $\rightarrow$ (i) and completes the proof.

COROLLARY. *An elementary statement E holds for all but a finite number of $R_q \leftrightarrow E$ holds for every pseudo-finite field.*

Definition. If E is an elementary statement then

$$\Delta(E) = \{q \mid E \text{ is true in } R_q\} .$$

Let $\mathfrak{B}$ be the boolean algebra on the set $\mathfrak{Q}$ of prime powers generated by the $\Delta([\exists X_1 f(X_1) = 0])$ for monic or constant $f \in \mathbf{Z}[X_1]$ and the finite subsets of $\mathfrak{Q}$.

Thus every element of $\mathfrak{B}$ differs by a finite set from $\Delta(\beta)$ for some one variable statement β.

THEOREM 10. $\mathfrak{K} = \prod R_q/D \approx \prod R_q/D' = \mathfrak{K}' \leftrightarrow D \cap \mathfrak{B} = D' \cap \mathfrak{B}$.

PROOF. $\mathfrak{K} \approx \mathfrak{K}' \leftrightarrow \mathrm{Abs}(\mathfrak{K}) \approx \mathrm{Abs}(\mathfrak{K}') \leftrightarrow [\mathfrak{K}] = [\mathfrak{K}'] \leftrightarrow D \cap \mathfrak{B} = D' \cap \mathfrak{B}$.

THEOREM 11. *If E is an elementary statement, $\Delta(E) \in \mathfrak{B}$.*

PROOF. If $\Delta(E) \notin \mathfrak{B}$, then by Corollary 2 to the proposition of § 11a, there exist non-principal ultrafilters D and D' on $\mathfrak{Q}$ such that $\Delta(E) \in D - D'$ while $D \cap \mathfrak{B} = D' \cap \mathfrak{B}$. By Theorem 10, $\prod R_q/D \approx \prod R_q/D'$ while E is true in $\prod R_q/D$ but not in $\prod R_q/D'$, a contradiction.

We may re-word Theorem 11 as follows.

THEOREM 11′. *Let E be an elementary statement. Then for each prime p there exists $m_p \in \mathbf{Z}_{>0}$, $V_p \subset \delta(m_p)$ and finite subsets M_p, $N_p \subseteq \mathbf{Z}_{>0}$ such that E holds in $R_{p^m} \leftrightarrow m \in (a(m_p, V_p) \sim M_p) \cup N_p$.*

Moreover there exists $D \in \mathbf{Z}_{>0}$ and a finite normal extension N of $\mathbf{Q}$ such that for $p \nmid D$, we have $M_p = N_p = \varnothing$ and m_p and V_p depend only on the decomposition subfield of a prime of N above p.

THEOREM 12. *Let E be a given elementary statement. Then we can find a one variable statement λ and finite subsets M, N of $\mathfrak{Q}$ such that $\Delta(E) = (\Delta(\lambda) \sim M) \cup N$. $[E \leftrightarrow \lambda]$ is deducible from Π.*

PROOF. The existence of λ, M, N follows from Theorem 11. We want to show how to find them, in principle. Since $E \leftrightarrow \lambda$ in all but a finite set of R_q, $[E \leftrightarrow \lambda]$ is true in all pseudo-finite fields by the corollary to Theorem 9. Hence by the completeness theorem there is an elementary proof of $[E \leftrightarrow \lambda]$ from Π. This also follows from Corollary 1 to the proposition of § 11a. Thus we proceed as follows. We run through all elementary proofs from Π until we hit a proof P of a statement of the form $[E \leftrightarrow \lambda']$ where λ' is a one variable statement. The proof P involves only a finite set A of $\pi \in \Pi$ and each $\pi \in \Pi$ holds in R_q for all but a finite set B_π of q which we can explicitly find. Thus for $q \in \mathfrak{Q} \sim \bigcup_{\pi \in A} B_\pi$, E holds in $R_q \leftrightarrow \lambda'$ holds in R_q. The theorem follows since we can determine for which $q \in \bigcup_{\pi \in A} B_\pi$ we have λ or E holding in R_q. The Main Theorem in the introduction now follows from Theorem 12 and Theorem 7′ of § 10.

COROLLARY. *Let $\mathcal{F}$ be a set of finite fields. Let T (resp. T_1) be the theory of all (resp. one variable) elementary statements true for all $F \in \mathcal{F}$. Then T is decidable $\leftrightarrow$ T_1 is decidable.*

THEOREM 13. *The theory of statements true in all finite fields is decidable.*

PROOF. If E is an elementary statement we apply Theorem 12 to obtain a one variable statement λ and finite subsets M, N of $\mathcal{Q}$ such that $\Delta(E) = (\Delta(\lambda) \sim M) \cup N$. We then apply Theorem 7 to λ to find that $\Delta(E) = \mathcal{Q} \leftrightarrow \Delta(\lambda) = \mathcal{Q}$ and $M \subset N$, and that we can decide whether or not $\Delta(\lambda) = \mathcal{Q}$.

In an analogous manner we can establish the following result.

THEOREM 13′. *The theory of statements true in all but a finite set of finite fields (which is the same as the theory of statements true in all pseudo-finite fields) is decidable.*

COROLLARY. *Let S be a finite or cofinite subset of $\mathcal{P}$. Let T be a cofinite subset of $\mathcal{Q}$. Then the theory W (resp. W') of statements true in R_{p^m} for all (resp. all but a finite set of) p^m such that $p \in S$ and $p^m \in T$ is decidable. In particular the theory of statements true in all finite fields of a given characteristic is decidable.*

PROOF. First suppose $\mathcal{P}$ is cofinite and let E be an elementary statement. Then $E \in W \leftrightarrow$ the elementary statement

$$E \vee \bigvee_{p \in \mathcal{P} \sim S} [P \neq 0] \vee \bigvee_{q \in \mathcal{Q} \sim T} E_q$$

is true for all finite fields, where E_q is an elementary statement true only in R_q. For example we can take F_q to be the statement

$$[\forall X_1 X_1^q = X_1^q] \wedge \bigwedge_{\substack{q' \mid q \\ 1 \neq q' \neq q}} [\exists X_1 X_1^{q'} \neq X_1] .$$

The proofs of the other cases of the corollary are similar.

THEOREM 14. *An elementary statement E is true in R_p for all but a finite set of $p \in \mathcal{P} \leftrightarrow E$ is true in R_{p^m} for all but a finite set of $p \in \mathcal{P}$ for all $m \in \mathbf{Z}_{>0}$.*

PROOF. If E is false in R_{p^m} for an infinite set S of p, then E is false in $\mathcal{K} = \prod_{p \in S} R_{p^m}/D$ for any non-principal ultrafilter D on S. But $\mathcal{K}$ is a pseudo-finite field of characteristic zero. Thus by Theorem 6 of § 9, there exists a non-principal ultraproduct $\mathcal{K}'$ of the R_p, $p \in \mathcal{P}$, such that $\mathrm{Abs}(\mathcal{K}') \approx \mathrm{Abs}(\mathcal{K})$. Hence $\mathcal{K} \equiv \mathcal{K}'$ and so E is false in $\mathcal{K}'$ and therefore E is false in R_p for an infinite set of $p \in \mathcal{P}$. This proves the forward implication, the converse being trivial.

Remark. $[\exists X_1 X_1^2 = -1]$ is true in R_{p^2} for all $p \in \mathcal{P}$ but false in R_p for

those $p \in \mathcal{P}$ such that $p \equiv 3 \bmod 4$.

By reasoning as before we can prove the following result.

THEOREM 13''. *The theory of statements true in all (resp. all but a finite set of) prime finite fields is decidable.*

11a. Existence of ultrafilters

PROPOSITION. *Let K be a sub-boolean algebra of a boolean algebra J. Let $j \in J - K$. Then there exists ultrafilters D, D' of J such that $D \cap K = D' \cap K$ and $j \in D - D'$.*

PROOF. Let $k_\mu \subseteq -j$, $1 \leqq \mu \leqq m$ and $k'_\nu \subseteq j$, $1 \leqq \nu \leqq n$. Then

$$\bigcap_\mu (-k_\mu) \cap \bigcap_\nu (-k'_\nu) \neq \varnothing .$$

Indeed, otherwise

$$\bigcup_\mu k_\mu \cup \bigcup k'_\nu = 1$$

(where 1 is the universal element of K and J). Since $\bigcup_\mu k_\mu \subseteq -j$ and $\bigcup_\nu k'_\nu \subseteq j$, we would then have

$$\bigcup_\nu k'_\nu = j .$$

This contradicts our assumption that $j \notin K$.

Thus there exists a filter E of K containing all $-k \in K$ such that $k \subseteq j$ or $k \subseteq -j$. By Zorn's lemma, there exists an ultrafilter F of K such that $F \supseteq E$.

We claim that $f \cap j \neq \varnothing$ for all $f \in F$. If $f \in F$ and $f \cap j = \varnothing$, then $f \subseteq -j$ and so $-f \in E \subseteq F$, a contradiction. This establishes our claim.

It follows that there exists an ultrafilter D of J such that $D \supseteq F \cap \{j\}$. Similarly there exists an ultrafilter D' of J such that $D' \supseteq F \cup \{-j\}$.

COROLLARY 1. *Let H be a boolean algebra of elementary statements. Let T be a set of elementary statements such that for every two models M, M' of T the following conditions are equivalent.*

(A) *For all $h \in H$, h holds in $M \leftrightarrow h$ holds in M';*

(B) $M \equiv M'$.

Then for all elementary statements E there exists $h \in H$ such that $[E \leftrightarrow h]$ is provable from T.

PROOF. Let J be the boolean algebra of elementary statements modulo the ideal generated by $\{-t \mid t \in T\}$. Let K be the subalgebra of J corresponding to H and let j be the element of J corresponding to E. We must show $j \in K$. Assume false. By the proposition there exist ultrafilters D, D' of J such that $D \cap K = D' \cap K$ and $j \in D - D'$. By the completeness theorem, the models of T are in natural correspondence with the ultrafilters of J. If M, M' are the models of T corresponding to D, D' then E is true in M but

not in M' so that (B) does not hold. But since $D \cap K = D' \cap K$, (A) does hold; this contradiction proves the corollary.

COROLLARY 2. *Let I be an infinite set and H a boolean algebra on I containing the finite sets. Suppose $r \subseteq I$ and $r \notin H$. Then there exists non-principal ultrafilters D, D' on I such that $D \cap H = D' \cap H$ and $r \in D - D'$.*

PROOF. This corollary follows from the proposition by taking J to be the boolean algebra of subsets of I modulo finite subsets of I and using that the ultrafilters of J are in natural one-one correspondence with non-principal ultrafilters on I.

12. Applications to p-adic fields

If $p \in \mathcal{P}$ and $m \in \mathbf{Z}_{>0}$, then $\mathbf{Q}_{p^m}$ denotes the unramified extension of $\mathbf{Q}_p$ of degree m. We may now combine Theorems 8, 8', of § 11 with the results of [11, 12, 13, 15] to obtain Theorem 15 below.

Let Γ be a recursive set of elementary statements about valued fields such that F is a model of $\Gamma \leftrightarrow F$ is an henselian valued field of characteristic zero, valued in a U-group. Then for all $q \in \mathcal{Q}$, $\mathbf{Q}_q$ is a model of Γ. For each $\pi \in \Pi$ we can find an elementary statement π' about valued fields such that π' holds in $F \leftrightarrow \pi$ holds in $\bar{F}$. Let $\Pi' = \Gamma \cup \{\pi' \mid \pi \in \Pi\}$. Then Π' is a recursive axiomatization of those models F of Γ such that $\bar{F}$ is pseudo-finite. For each $\lambda \in \Pi'$ the set of $q \in \mathcal{Q}$ such that λ is false in $\mathbf{Q}_q$ is a finite set which we can explicitly find since Π has the corresponding property with respect to the R_q. Finally we set

$$\Pi_1' = \Pi' \cup \{[\operatorname{ord} p = 0 \vee \operatorname{ord} p = 1]: p \in \mathcal{P}\} .$$

THEOREM 15. *F is a model of $\Pi_1' \leftrightarrow F \equiv \prod_q \mathbf{Q}_q/D$ for some non-principal ultrafilter D on $\mathcal{Q}$. Moreover if D and D' aae non-principal ultrafilters on $\mathcal{Q}$, then*

$$\prod \mathbf{Q}_q/D \equiv \prod \mathbf{Q}_q/D' \longleftrightarrow \prod R_q/D \equiv \prod R_q/D' \longleftrightarrow$$
$$\prod \mathbf{Q}_q/D \approx \prod \mathbf{Q}_q/D' \longleftrightarrow \prod R_q/D \approx \prod R_q/D' .$$

THEOREM 16. *Given an elementary statement E about valued fields we can find a one variable statement λ and finite subsets M, N of $\mathcal{Q}$ such that for the set $\Delta'(E)$ of $q \in \mathcal{Q}$ such that E is true in $\mathbf{Q}_q$ we have*

$$\Delta'(E) = \big(\Delta(\lambda) \sim M\big) \cup N .$$

PROOF. We first prove the existence of λ, M, N, or equivalently that $\Delta'(E) \in \mathcal{B}$. If this were false then, as in the proof of Theorem 11 of § 11, there would exist non-principal ultrafilters D, D', on $\mathcal{Q}$ such that $D \cap \mathcal{B} = D' \cap \mathcal{B}$ while $\Delta'(E) \in D \sim D'$. The desired contradiction now follows from

Theorem 10 of §11 and Theorem 15. Now let λ' be the relativization of λ to valued fields, i.e., if λ is obtained from the boolean polynomial $\varphi = \varphi(X_1, \cdots, X_s)$ by replacing X_σ by $[\exists X_1 f(X_1) = 0]$ for $\sigma = 1, \cdots, s$, then λ' is obtained from φ by replacing X_σ by $[\exists X_1 \operatorname{ord} X_1 \geqq 0 \wedge \operatorname{ord} f(X_1) > 0]$ for $\sigma = 1, \cdots, s$ (where the $f_\sigma \in \mathbf{Z}[X_1]$ are constant or monic). Then $[E \leftrightarrow \lambda']$ is true for all but a finite set of $\mathbf{Q}_q$ Therefore $[E \leftrightarrow \lambda]$ is true in every non-principal ultraproduct of the $\mathbf{Q}_q$. By Theorem 15, $[E \leftrightarrow \lambda']$ is true in every model of Π_1'. By the completeness theorem we can find proof P of $[E \leftrightarrow \mu']$ from Π_1' where μ' is the relativization to valued fields of a one variable statement μ. As in the proof of Theorem 12 we can find a finite subset C of $\mathfrak{Q}$ such that for $q \in \mathfrak{Q} \sim C$, $[E \leftrightarrow \mu']$ holds in $\mathbf{Q}_q$. We then test E and μ' in $\mathbf{Q}_q$ for $q \in C$ using the decidability of $\mathbf{Q}_q$. This completes the proof.

Remark. If we combine Theorem 16 with Theorem 7′ of §10 and the remark following the corollary of Lemma 1 of §10 we obtain Theorem A stated in the introduction. Another consequence of Theorem 16 is

THEOREM 17. *Let $S = \mathcal{P}, \mathfrak{Q}$, or all powers of a fixed prime. Then the theory of statements true in $\mathbf{Q}_q$ for all $q \in S$ (resp. all but a finite set of $q \in S$) is decidable.*

Let E be an elementary statement about rings. Then we can find an elementary statement E' about valued fields such that if p is a prime then E' holds in $\mathbf{Q}_p \leftrightarrow E$ holds in $\mathbf{Z}/p^t$ for all $\mathbf{Z}_{>0}$.

COROLLARY 1. *Let S be as in Theorem 17. Then the theory of statements true in $\mathbf{Z}/q$ for all $q \in S$ (resp. all but a finite set of $q \in S$) is decidable.*

COROLLARY 2. *There is an effective procedure for deciding if a polynomial $f \in \mathbf{Z}[X_1, \cdots X_n]$ has a solution modulo m for all $m \in \mathbf{Z}_{>1}$.*

PROOF. f has a solution modulo $m \leftrightarrow f$ has a solution modulo $p_i^{a_i}$, $i = 1, \cdots, k$ where $m = \prod_{i=1}^{k} p_i^{a_i}$, the p_i being distinct primes.

13. Decidable pseudo-finite fields

THEOREM 18. *Let F be a pseudo-finite field of characteristic $p \in \mathcal{P}$ Let $\nu: \mathcal{P} \to \mathbf{Z}_{\geqq 0} \cup \{\infty\}$ be such that if we set $s = \prod_{p \in \mathcal{P}} p^{\nu(p)} \in \mathbf{Z}_*$, then $\operatorname{Abs}(F) = R_{p^s}$. Then F is decidable $\leftrightarrow$ ν is recursive. More generally the degree of recursive unsolvability of F and of ν are equal.*

PROOF. A complete set of axioms for F is given by

$$\Pi \cup \{[\exists X_1 f(X_1) = 0]: f \in [F]\} \cup \{[\forall X_1 f(X_1) \neq 0]: f \in \mathbf{Z}[X_1] - [F]\},$$

according to Theorem 5 of §8. Since Π is recursive, the degree of unsolvability of F is the same as that of the characteristic function χ of the subset $[F]$ of

$\mathbf{Z}[X_1]$. But χ and ν are recursive in each other, i.e., have the same degree of recursive unsolvability. This proves the theorem.

COROLLARY. *If* $\nu: \mathcal{P} \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ *is a function and we set* $s = \prod_{p \in \mathcal{P}} p^{\nu(p)}$, *then* R_{p^s} *is decidable* $\leftrightarrow$ ν *is recursive.*

PROOF. If image $\nu \subset \mathbf{Z}_{\geq 0}$ this follows from the theorem since then R_{p^s} is pseudo-finite. In the general case let $S = \nu^{-1}(\mathbf{Z}_{\geq 0})$. Then R_{p^s} is S-pseudo-finite as explained in § 14 and the result carries through.

This gives examples of fields F of characteristic p with arbitrary degrees of unsolvability. Given such an F one can obtain fields of characteristic zero of the same degree of unsolvability by taking the quotient field of the ring of Witt vectors over F.

THEOREM 18′. *Let* F *be a pseudo-finite field. Then* F *is decidable* $\leftrightarrow$ $[F]$ *is a recursive subset of* $\mathbf{Z}[X_1]$.

PROOF. The proof is similar to the proof of Theorem 18.

COROLLARY 1. *The unique up to elementary equivalence pseudo-finite fields* F *such that* $\mathrm{Abs}(F) = \tilde{\mathbf{Q}}$ *is decidable.*

PROOF. $[F] = (\mathbf{Z}[X_1] \sim \mathbf{Z}) \cup \{0\}$.

COROLLARY 2. *The unique up to elementary equivalence pseudo-finite field* F *such that* $\mathrm{Abs}(F)$ *is the set of real algebraic numbers is decidable.*

PROOF. By Sturm's algorithm, $[F]$ is a recursive subset of $\mathbf{Z}[X_1]$.

14. Further results and open problems

In this section we discuss the effect of removing the quasi-finite condition. Let F be a field satisfying the following condition.

$(*)$ F is perfect and, for every absolutely entire F-algebra R, there exists an F-algebra homomorphism $R \to F$.

For F perfect, this is equivalent to requiring that every absolutely irreducible variety defined over F has an F-valued point.

LEMMA 1. *If* F' *is an algebraic extension of* F, *then* F' *satisfies* $(*)$.

PROOF. We may assume F'/F finite. Then the function from the category e_F of schemes over F to the category $e_{F'}$ which assigns to every $V \in e_F$, the scheme $V \otimes_F F' \in e_{F'}$ has a right adjoint B [5, p. 195–13]:

$$(V \otimes_F F', W)_{e_{F'}} \approx (V, B(W))_{e_F}$$

for all $V \in e_F$, $W \in e_{F'}$. Thus by taking $V = F$ we see that the F-valued points of $B(W)$ are in bijective correspondence with the F'-valued points of W. Moreover, W absolutely irreducible over $F' \to B(W)$ absolutely irre-

ducible over F. The lemma follows.

We now assume the basic concepts of profinite Galois cohomology as presented in [4].

LEMMA 2. *Let F satisfy (*). Then the cohomological dimension of F is at most one*, i.e., $\operatorname{cd} \mathfrak{G}(\tilde{F}/F) \leqq 1$.

PROOF. By [4, Ch. II, § 3, Prop. 5], it suffices to prove that the Brauer group of every finite extension F of F is trivial. Now if $D \neq F'$ is a central simple division algebra over F', then the reduced norm defines an absolutely irreducible variety over F' with no F'-valued point. This contradicts Lemma 1.

Let $S \subseteq \mathcal{P}$.

Definition. F is S-pseudo-finite $\leftrightarrow$ F satisfies (*) and F is S-quasi-finite, i.e., for each $n \in \mathbf{Z}_{>0}$ such that n is composed of primes of S, F has precisely one extension of degree n.

PROPOSITION 8. *If F satisfies (*) and $\mathfrak{G}(\tilde{F}/F)$ is abelian, then F is S-pseudo-finite for some $S \subseteq \mathcal{P}$.*

PROOF. A profinite abelian group of cohomological dimension $\leqq 1$ is isomorphic to $\prod_{p \in S} \mathbf{Z}_p$ for some S, and so the proposition follows from Lemma 2.

Problem 1. Is the restriction that $\mathfrak{G}(\tilde{F}/F)$ be abelian removable?

We can now extend all the results of § 1–9 about pseudo-finite fields to S-pseudo-fields, finite fields being replaced by the finite extensions of $R_{p,S}$ where $[R_{p,S}: R_p] = \prod_{r \in \mathcal{P}-S} r^{\infty}$.

For example, if $S = \varnothing$, then F is S-pseudo-finite $\leftrightarrow$ F is algebraically closed and our results reduce to the usual algebraic and metamathematical properties of algebraically closed fields.

PROPOSITION 9. *If K is an infinite field of absolute numbers of positive characteristic, then K is S-pseudo-finite, where $S = \{p : p \mid [\tilde{K} : K]\}$.*

Problem 2. Does any proper subfield of $\tilde{\mathbf{Q}}$ satisfy (*)?

Remark. There exist quasi-finite subfields K of $\tilde{\mathbf{Q}}$ which do not satisfy (*). Indeed if p is a prime let V be maximal purely ramified algebraic extension of $\mathbf{Q}_p$ then V is a quasi-finite valued field with residue class field R_p. From the fact that $\tilde{\mathbf{Q}}$ is dense in $\tilde{\mathbf{Q}}_p$ follows that $K = \operatorname{Abs}(V)$ is quasi-finite. Moreover, $(X^p - X - 1)(Y^p - Y - 1) - p \in K[X, Y]$ is absolutely irreducible and has no zeros over K since for all $z \in V$, $\operatorname{ord}(z^p - z - 1) \leqq 0$.

PROPOSITION 10. *A field F is S-pseudo-finite for some $S \leftrightarrow F$ is elementarily equivalent to a non-principal ultraproduct of algebraic extensions of finite fields.*

COROLLARY. *If F is a perfect field such that every absolutely irreducible variety defined over F has an F-valued point, and if $\mathcal{G}(\tilde{F}/F)$ is abelian then F is C_1,* i.e., *every form in more variables than its degree has a non-trivial zero over F.*

This is Theorem D.

Problem 3. Is the restriction that $\mathcal{G}(\tilde{F}/F)$ be abelian removable?

Let V be a variety (of finite type) over an S-pseudo-finite field F. Let $\varphi: V \to V$ be an F-morphism and φ_F the induced mapping of the F-valued points.

PROPOSITION 11. *If φ_F is injective then φ_F is surjective.*

PROOF. The result would clearly be true if F were finite. From this we see it is true if F is the union of finite fields, i.e., an an algebraic extension of a finite field. Since the assertion is equivalent to a set of elementary statements, it holds for any field elementarily equivalent to an ultraproduct of algebraic extensions of finite fields. By Proposition 10, this includes the S-pseudo-finite field F.

COROLLARY. *An injective morphism of an algebraic variety into itself is surjective.*

PROOF. This follows from the special case of Proposition 11 in which S is empty. Of course in this case the isomorphism theorem reduces to the well-known fact about algebraically closed fields: two algebraically closed fields of the same uncountable cardinality are isomorphic over any common subfield of smaller cardinality

The corollary is Theorem C of the introduction.

Problem 4. Does the analogue of the corollary hold for real algebraic varieties?[1]

In § 10 it was shown that the elementary theory of $\{\mathbf{Z}/q: q \in \mathcal{Q}\}$ is decidable. Also it was shown that the *existential* theory of $\{\mathbf{Z}/m: m \in \mathbf{Z}_{>1}\}$ is decidable.

Problem 5. Is the elementary theory of the rings $\mathbf{Z}/m$, $m \in \mathbf{Z}_{>1}$ decidable?

CORNELL UNIVERSITY

REFERENCES

[1] A. WEIL, Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.

[2] E. ARTIN, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Univ. Hamburg, **3-4** (1923-26), 89-108.

[3] J-P. SERRE, Corps locaux, Hermann, Paris, 1962.

[1] A. Borel has recently answered this question affirmatively for *smooth* varieties.

[4] ———, Cohomologie Galoisienne, Lecture Notes in Mathematics, No. 5, Springer-Verlag, 1964.
[5] A. GROTHENDIECK, *Technique de descente*: II, Séminaire Bourbaki, exposè 195, (1959-1960).
[6] N. JACOBSON, Lectures in Abstract Algebra: III, Van Nostrand, Princeton, 1964.
[7] D. MUMFORD, Introduction to algebraic geometry, Harvard Lecture Notes, 1966.
[8] J. AX, *Solving diophantine problems modulo every prime*, Ann. of Math. **85** (1967), 161-183.
[9] W. M. LAMBERT, Effectiveness, elementary definability and prime polynomial ideals, Doctoral Dissertation, U.C.L.A., 1965.
[10] S. FEFERMAN and R. VAUGHT, *The first order properties of products of algebraic systems*, Fund. Math. **47** (1959), 57-103.
[11] J. AX and S. KOCHEN, *Diophantine problems over local fields*: I, Amer. J. Math. **87** (1965), 605-630.
[12] ———, *Diophantine problems over local fields*: II, a complete set of axioms for p-adic number theory, Amer. J. Math. **87** (1965), 631-648.
[13] ———, *Diophantine problems over local fields*: III. Decidable fields, Ann. of Math. **83** (1966), 437-456.
[14] A. WEIL, Foundation of Algebraic Geometry, Amer. Math. Soc. Colloquium Publications, vol. 29.
[15] JU. L. ERSHOV, "On the elementary theory of maximally complete fields" (Russian), in Algebra and Logic Seminar, Novosibirsk, Vol. **4**, No. 3, pp. 31-70.
[16] J. BELL and A. SLOMSON, Introduction to Model Theory, Lecture Notes, Mathematical Institute, Oxford, 1965.
[17] S. LANG and A. WEIL, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819-827.
[18] A. BIAŁYNICKI-BIRULA and M. ROSENLICHT, *Injective morphisms of real algebraic varieties*, Bull. Amer. Math. Soc. **67** (1961), 200-203.

(Received July 19, 1967)