ISRAEL JOURNAL OF MATHEMATICS 117 (2000), 311–333

# NON-STANDARD FINITE FIELDS OVER $I\Delta_0 + \Omega_1$

BY

PAOLA D'AQUINO

*Dipartimento di Matematica, Seconda Universitá di Napoli*
*Via Vivaldi, Caserta 81100, Italy*
*e-mail: paola.daquino@unina2.it*

AND

ANGUS MACINTYRE

*Department of Mathematics and Statistics, University of Edinburgh*
*JCM Building, Mayfield Road, Edinburgh EH9 3JZ, Scotland*
*e-mail: angus@maths.ed.ac.uk*

ABSTRACT

We consider residue fields of primes in the well-known fragment of arithmetic $I\Delta_0 + \Omega_1$. We prove that each such residue field has exactly one extension of each degree. The standard proofs use counting and the Frobenius map. Since little is known about these topics in fragments, we looked for, and found, another proof using permutation groups and the elements of Galois cohomology. This proof fits nicely into $I\Delta_0 + \Omega_1$ using, instead of exponentiation, exponentiation modulo a prime.

## 1. Introduction

The importance of finite fields in both practical and theoretical computer science is well established, and there is a huge literature on algorithmic aspects of this ([Sh]).

Model theoretic aspects impinge on this, starting with Ax's [Ax] deep work on the decidability of the elementary theory of finite fields. Ax isolated crucial axioms for non-principal ultraproducts $K$ of finite fields:

(i) $K$ is perfect;

Received October 28, 1998

(ii) $K$ has exactly one extension of each degree;

(iii) every absolutely irreducible curve over $K$ has a $K$-rational point.

(Such fields are now called pseudofinite.)

Finite fields satisfy (i) and (ii). Both properties are proved by counting, and there is in particular no very explicit way of exhibiting, given a finite field $K$ and an integer $n$, an irreducible polynomial of degree $n$ over $K$.

Residue fields $\mathbf{F}_p$ of non standard primes $p$ in models $\mathcal{M}$ of Peano Arithmetic ($PA$) are pseudofinite [M1]. Moreover, such $\mathbf{F}_p$ are equipped with an exponentiation $x^k$ with $x \in \mathbf{F}_p$, $k \in \mathcal{M}$, and it is easy to prove Fermat's Little Theorem, and the cyclicity of the multiplicative group of $\mathbf{F}_p$.

Note that the abstract notion of a field with such an exponentiation has hardly been investigated. Also, Ax's axioms involve no reference to exponentiation, though proofs of the corresponding facts in finite fields do use exponentiation and counting.

In this paper we consider much weaker systems of arithmetic, where exponentiation is not total, but exponentiation modulo a prime is. For the well known example $I\Delta_0+\Omega_1$ we succeed in proving, for residue fields $\mathbf{F}_p$, that $\mathbf{F}_p$ has exactly one extension of each degree. Our proof does not use (conventional) counting, and does not give a proof of Fermat's Little Theorem. Counting is replaced by permutation group theory and Galois cohomology.

Following Kreisel we ask (but do not answer) the question:

What more does the new proof tell us, beyond the mere truth of the result for original setting of finite fields?

We will be working in a somewhat exotic category, that of non-standard rings with exponentiation. Regarding exponentiation, the point of departure is Bennett's [B], where he gave a $\Delta_0$-definition of the graph of the exponential function on $\mathbf{N}$. Exponentiation is not a total function in our models (see [Pa]). In fact there is in each model of $I\Delta_0$ a unique partial $\Delta_0$-definable function $exp$ satisfying certain basic [GD] properties of the function $x^y$. One writes $Exp$ for the axiom that $exp$ is total. The system $I\Delta_0 + Exp$ is surely strong enough to derive all the results in Hardy and Wright [HW]. From a different perspective, it is far too strong for its proof theory to be relevant for hardcore complexity theory.

In some rare cases one has been able to replace $Exp$ by a (provably weaker) combinatorial principle of pigeon hole type. This happened for the cofinality of primes, and for Lagrange's Theorem, proved, respectively, in $I\Delta_0+\Omega_1$, by Woods [W] and Berarducci–Intrigila [BI]. They used $\Delta_0$-WPHP, which prohibits $1-1$ $\Delta_0$-maps from $2a$ to $a$ for $a > 0$. In [PWW] $\Delta_0$-WPHP is derived in $I\Delta_0 + \Omega_1$,

where $\Omega_1$ naturally expresses the totality of the function

$$x \longrightarrow x^{|x|},$$

where $|x|$ is the binary length of $x$. See [WP] for background on this system. Sometimes the function $\#(x,y) = x^{|y|}$ is taken as primitive. Note that in contrast to $x^y$ this is a polynomial time computable function.

The inclusions

$$I\Delta_0 \subset I\Delta_0 + \Omega_1 \subset I\Delta_0 + Exp$$

are known to be strict [HP]. Little is known about elementary arithmetic in $I\Delta_0$, whereas one is gradually accumulating non trivial results for $I\Delta_0 + \Omega_1$.

In 1975 Pratt [Pr] showed that **prime** is in NP∩co-NP. While it is trivial that **prime** is in co-NP, it requires considerable effort to show **prime** is in NP. Pratt used Fermat Little Theorem and the cyclicity of $\mathbf{F}_p^*$. It is believed that **prime** is in P, and Miller [Mi] proved this under an Extended Riemann Hypothesis.

The connection to $I\Delta_0 + \Omega_1$ is the following. In [Bu] Buss isolated a natural subsystem $S_2^1$ of $I\Delta_0 + \Omega_1$, and showed that any predicate provably in NP∩co-NP over $S_2^1$ is in fact in P (in the real world). So there is a clear incentive to put Pratt's proof, and in particular Fermat Little Theorem, into $I\Delta_0 + \Omega_1$.

In $I\Delta_0$ (as opposed to the weaker *IOpen* [MM]) the notions **prime, irreducible, maximal** coincide. For $\mathcal{M}$ model of $I\Delta_0$, and $p$ prime in $\mathcal{M}$, let $\mathbf{F}_p$ be the residue field. For $p$ standard, $\mathbf{F}_p$ is as in $\mathbf{N}$. For $p$ non standard, $\mathbf{F}_p$ has characteristic 0.

One wants to understand in $I\Delta_0 + \Omega_1$ the analogues of the following facts from the real world:

1) The multiplicative group of $\mathbf{F}_p$ and its finite extensions are cyclic;

2) $\mathbf{F}_p$ has a unique extension $\mathbf{F}_{p^n}$ of dimension $n$, the splitting field of $x^{p^n} - x$;

3) The automorphism group of $\mathbf{F}_{p^n}$ over $\mathbf{F}_p$ is cyclic generated by the Frobenius map $\sigma : x \mapsto x^p$.

In the extreme cases of $PA$ and of *IOpen*, one knows the $\mathbf{F}_p$ up to elementary equivalence. As already mentioned Macintyre showed in [M1] that for $PA$ and nonstandard $p$ the $\mathbf{F}_p$ are up to elementary equivalence the characteristic 0 pseudo-finite fields of Ax. We believe that, with little more effort, one can replace $PA$ by $I\Delta_0 + exp$.

For *IOpen*, Macintyre and Marker showed in [MM] that up to elementary equivalence there is no restriction beyond characteristic 0. In particular, a residue field may have infinitely many extensions of each dimension.

*Notation:* For $L$ a field, $L^*$ is its multiplicative group, and $L^{alg}$ its algebraic closure.

## 2. Exponentiation over non-standard finite rings

Gödel [G] showed that in any model $\mathcal{M}$ of $PA$ there is a well defined exponential function $x^y$ satisfying the usual recursion laws, and unique modulo being first order definable from $+$ and $\cdot$. Striking as this is, it has no computational significance, and Godel's Incompleteness owes none of its importance to this fact.

Thirty years later Bennett [B] found a $\Delta_0$-definition of the relation $x^y = z$ (Godel's is $\Sigma_1$) and later it was shown [GD] that on any model $\mathcal{M}$ of $I\Delta_0$ there is a partial function $(x, y) \mapsto x^y$ satisfying the usual recursion laws and for fixed $x$ having domain an initial segment. Again, there is uniqueness subject to $\Delta_0$-definability. The (minor) computational significance is that the function $2^y$ is not in general total, since on $\mathbf{N}$ $2^n$ is not of polynomial growth.

However, the function

$$(x, y, n) \mapsto \text{ remainder of } x^y \text{ mod } n$$

is polynomial time computable (folklore by repeated squaring). So one naturally asks if every model $\mathcal{M}$ of $I\Delta_0$ carries a unique (subject say to $\Delta_0$-definability) total map

$$\mathcal{M}/n\mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{M}/n\mathcal{M}$$
$$(x, y) \mapsto x^y$$

for all $n$ (even non standard) in $\mathcal{M}$, satisfying the obvious algebraic laws for exponentiation mod $n$. This question has not been answered. There is however a positive answer (again folklore) if one moves up to $I\Delta_0 + \Omega_1$, [HP]. Here by uniqueness we mean that there exists a $\Delta_0$-formula $G(x, y, n, t)$ defining the graph of a function $g(x, y, n)$ (where $t$ codes the computation) which is total if we assume $\Omega_1$, and there is a total $\Delta_0$-function $\theta$ such that $\theta(g(x, y, n))$ is the remainder of $x^y$ modulo $n$. A precise formulation of these facts need not concern the uninitiated.

Let us record, for future use, that we have checked the following for $I\Delta_0 + \Omega_1$:

For any ring $R$ $\Delta_0$-interpretable in a model $\mathcal{M}$ of $I\Delta_0 + \Omega_1$, with the underlying set of $R$ some $[0, a]$, there is a natural $\Delta_0$-definable total $(r, n) \mapsto r^n$ for $r \in R$ and $n \in \mathcal{M}$, satisfying the usual algebraic laws of exponentiation. In this paper we apply this observation to $L$ which is a standard-finite-dimensional extension of $\mathcal{M}/p$, for $p$ a prime in $\mathcal{M}$. The essential point is that henceforward we can use these exponentiations freely in $\Delta_0$-induction arguments.

### 3. Fermat Little Theorem

When we work in a weak fragment of arithmetic such as $I\Delta_0$ or $I\Delta_0 + \Omega_1$ in order to reproduce some classical number theoretical results we may face two problems:

1) give a **meaning** to the objects we are working with;

2) find a proof which can be formalized in the fragment.

In this section we will study Fermat's Little Theorem in $I\Delta_0 + \Omega_1$. Because of the totality of exponentiation modulo an integer in $I\Delta_0 + \Omega_1$, problem 1) does not exist in this case. We can at least express the following

$$(flt) \quad \text{if } p \text{ is a prime and } (a,p) = 1 \text{ then } a^{p-1} \equiv 1(\mathrm{mod}\, p).$$

It is now clear why we need to work in $I\Delta_0 + \Omega_1$ rather than in $I\Delta_0$. In $I\Delta_0$ we do not even know how to state Fermat's Little Theorem. This still leaves the problem of formalizing a proof of it in $I\Delta_0 + \Omega_1$. One of the classical proofs of $(flt)$ is group-theoretic: the multiplicative group $\mathbf{Z}_p^*$ has order $p-1$ and the order of every element $a \in \mathbf{Z}_p^*$ divides $p-1$. So

$$a^{p-1} \equiv 1(\mathrm{mod}\, p) \quad \text{for every } a \in \mathbf{Z}_p^*.$$

$\mathbf{Z}_p^*$ is a cyclic group of order $p-1$ (and a generator is called a primitive root). The above proof involves a counting argument which we do not know how to formalize in $I\Delta_0 + \Omega_1$. Berarducci and Intrigila in [BI] also considered the provability of $(flt)$ in subsystems of arithmetic. They formalized the group theoretic proof of $(flt)$ in the theory $I\mathcal{E}_*^2$, where induction is applied to $\mathcal{E}_*^2$-predicates (we recall that $\mathcal{E}_*^2$ is the class of predicates defined by Grzegorczyk, see [HP]). The proof goes smoothly in $I\mathcal{E}_*^2$ since a good notion of cardinality is here available. The full $\Delta_0$-pigeon hole is provable in $I\mathcal{E}_*^2$, so it is easy to carry on the proof that the order of an element divides the order of the group. They did not consider the further property of cyclicity of $\mathbf{Z}_p^*$. The crucial step in the classical proof seems to be the fact that a polynomial of degree $n$ has at most $n$ roots in a field. This is known as Lagrange's Theorem and it is proved by induction on the degree of the polynomial (see [L]). Clearly, there are obstacles in carrying on the induction in $I\Delta_0 + \Omega_1$ since the polynomials may be too long to be coded.

Although for cyclicity of $\mathbf{F}_p^*$ we need only that the polynomial $x^r - 1$ has at most $r$ roots in any field (for $r$ a divisor of $p-1$), the proof for such sparse polynomials seems inextricably bound in an induction to that for nonsparse polynomials (like $x^{r-1} + x^{r-2} + \cdots + x + 1$) in general too long to be coded.

*Remark:* If $r \in \mathbf{N}$ then the polynomial $x^r - 1$ has at most $r$ roots in $\mathbf{F}_p$ since this is a purely algebraic fact. This property will play a crucial role in the following sections.

*Note:* Fermat Little Theorem can be stated also as follows: consider the map $\sigma : \mathbf{F}_p \longrightarrow \mathbf{F}_p$ defined as $\sigma(x) = x^p$. Then $\sigma = identity$, i.e. $\sigma(x) = x$ for all $x \in \mathbf{F}_p$.

The above statement can be proved easily by induction on $x$. But also in this case we cannot formalize the proof in $I\Delta_0 + \Omega_1$: in the inductive step the expression

$$(x+1)^p = x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{1}x + 1$$

can be too long to be coded. Using the definition of exponentiation modulo $n$ we can express in $I\Delta_0 + \Omega_1$ also this version of $(flt)$.

A third proof of Fermat Little Theorem uses the complete set of residues and it is a corollary of a more general result, the Fermat–Euler Theorem, which says that

$$\text{if} \quad (n,a) = 1 \quad \text{then} \quad a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$$

where $\varphi$ is the Euler function. It is shown that if $U(n)$ denotes the set of invertible elements in $\mathbf{Z}_n$ and $a \in \mathbf{Z}_n$ then $aU(n) = U(n)$. So, if $U(n) = \{y_1, \ldots, y_{\varphi(n)}\}$ then $aU(n) = \{ay_1, \ldots, ay_{\varphi(n)}\} = \{y_1, \ldots, y_{\varphi(n)}\}$. It follows that

$$(\bullet) \quad ay_1 \cdots ay_{\varphi(n)} \equiv y_1 \cdots y_{\varphi(n)} (\mathrm{mod}\, n)$$

and so $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$. In this proof there is the problem of expressing the products in $(\bullet)$. As far as we know there is no $\Delta_0$-formula, even in $\#$, defining the product of a $\Delta_0$-function for which the totality of the product function modulo an integer is provable. In particular, no $\Delta_0$-definition of the graph of factorial is known for which the totality of factorial modulo an integer is provable in $I\Delta_0 + \Omega_1$. This is connected with the fact that we cannot reduce the computation of $n!$ to a computation in a logarithmic number of steps as for exponentiation (see [BCSS]).

## 4. Quasi-cyclicity of $\mathbf{F}_p^*$

Even if the classical result of the cyclicity of $\mathbf{F}_p^*$ seems not to be provable in $I\Delta_0 + \Omega_1$ we can prove for $\mathbf{F}_p^*$ the classical decomposition for abelian groups.

First of all we show that any element of $\mathbf{F}_p^*$ has an order (see also [KP]) and among the orders of all elements there is a maximal one.

LEMMA 4.1: *Every element $a$ of $\mathbf{F}_p^*$ has an order which is less than $2p$.*

*Proof:* Fix an element $a$ of $\mathbf{F}_p^*$ and consider the map $\phi$: $[1, 2p] \longrightarrow [1, p]$ defined as $\phi(x) = a^x (\mathrm{mod}\, p)$. From the discussion in section 2 it is clear that $\phi$ is $\Delta_0$ and so by the $\Delta_0$-weak pigeon hole principle there are $x, y < p$ such that $a^x \equiv a^y (\mathrm{mod}\, p)$, hence $a^{x-y} \equiv 1 (\mathrm{mod}\, p)$. So the set $\{z : 0 < z < 2p, a^z \equiv 1 (\mathrm{mod}\, p)\} \neq \emptyset$ and $\Delta_0$-definable, so it has a minimal element $x$ which is the order of $a$. ∎

We will use the standard notation $o(a)$ to denote the order of $a$.

We need to recall the following general fact about $\Delta_0$-definable sets in a model $\mathcal{M}$ of $I\Delta_0$.

LEMMA 4.2: *Let $A$ be a bounded non-empty $\Delta_0$-definable subset of $\mathcal{M}$. Then $A$ has a maximal element.*

*Proof:* See [D'A]. ∎

We recall that for any $d \in \mathcal{M}$ there exists $s \in \mathcal{M}$ with $s = [\log d]$ in $\mathcal{M}$, and there is a $1 - 1$ map from the set of primes which divide $d$ into $s$, giving $d = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ (for a more precise treatment see the details in [D'A] or [W]).

LEMMA 4.3: *There exists a maximal order $d$ among the orders of the elements of $\mathbf{F}_p^*$, and the order of each element of $\mathbf{F}_p^*$ divides $d$.*

*Proof:* Consider the set of all orders, $A = \{x < 2p : o(a) = x \text{ for some } a < p\}$. $A$ is $\Delta_0$-definable and bounded by $2p$, hence by Lemma 4.2 it has a maximal element $d$.

Let $\alpha$ be an element of order $d$ and $d = m_1 m_2 \cdots m_s$, where the $m_i$'s are powers of distinct primes $p_i$. Suppose that there exists an element $x \in \mathbf{F}_p^*$ whose order $n$ does not divide $d$. There are two cases:

(i) Every prime dividing $n$ divides also $d$. Let $n = n_1 n_2 \cdots n_s$, where the $n_i$'s are powers of distinct primes, and $n_i$ does not divide $m_i$ for some $i = 1, \ldots, s$. Let $w = \alpha^{m_i}$ and $z = x^{n/n_i}$. It is clear that $o(w)$ and $o(z)$ are coprime, hence the order of $wz$ is $o(w)o(z)$ which is strictly bigger than $d$, and this gives a contradiction with the maximality of $d$.

(ii) There exists a prime $r$ such that $r$ divides $n$ but $r$ does not divide $d$. Let $n_i = r^k$ where $k$ is the higher power of $r$ which divides $n$. If $z = x^{n/n_i}$ then $o(z)$ is coprime with $d$ and so $\alpha z$ has order greater than $d$, and again we get a contradiction with the maximality of $d$. ∎

The maximal order $d$ will play the role of $p-1$. We cannot prove that $d$ is equal to $p-1$ (a counting argument seems needed). Using a sharpened version of the $\Delta_0$-weak pigeon hole principle (see [PWW]) we can only show that $d \leq (1+\epsilon)(p-1)$ for any (standard) rational $\epsilon > 0$.

*Note:* Even assuming that $\mathbf{F}_p^*$ is cyclic we cannot prove that $d = p-1$ in $I\Delta_0 + \Omega_1$. We have only the following estimates on $d$,

$$\frac{p-1}{1+\epsilon} \leq d \leq (1+\epsilon)(p-1).$$

It seems that the whole $\Delta_0$-pigeon hole is needed in order to show that $d = p-1$.

*Note:* If we assume that $d \geq p-1$ then $\mathbf{F}_p^*$ is cyclic. Suppose $\mathbf{F}_p^*$ is not cyclic and consider two different cosets modulo the subgroup $< \alpha >$, with $\alpha$ of order $d$. There is an injection of $2d$ into $p-1$, contradicting the weak pigeon hole principle.

We are now going to extend in a formal way the decomposition of abelian groups working with $d$ instead of $p-1$. We need to recall the following result due to Paris, Wilkie and Woods which says that we can formalize in $I\Delta_0$ the notion of sum of a $\Delta_0$-definable function over a logarithmic segment. Let $\mathcal{M}$ be a model of $I\Delta_0$.

THEOREM 4.4 ([PWW]): *Let $a, b, d \in \mathcal{M}$, $d \leq (\log a)^k$ for some $k \in \mathbf{N}$ and $F$: $d \to b$, $\Delta_0$-definable. Then there is a $\Delta_0$-definable function $G : d \to \mathcal{M}$ (uniformly) such that $G(0) = F(0)$ and for all $i < d$, $G(i+1) = G(i) + F(i+1)$, i.e. the sum of the function $F$ exists.*

Clearly, this result can be extended in a natural way to models of $I\Delta_0 + \Omega_1$.

*Definition 4.5:* Let $d = m_1 m_2 \cdots m_s$ where $m_i = p_i^{k_i}$. Define for each $i \leq s$

$$A(p_i) = \{x \in \mathbf{F}_p^* : \text{ order of } x \text{ is a power of } p_i\}.$$

THEOREM 4.6: *$\mathbf{F}_p^*$ is the direct sum of $A(p_1)$, $A(p_2), \ldots, A(p_s)$ in the following sense, each element of $\mathbf{F}_p^*$ can be written in a unique way as a product of $s$ elements each belonging to the $A(p_i)$'s, for $i = 1, \ldots, s$.*

For the interpretation of non standard finite product see [BD'A].

*Proof:* Let $u \in \mathbf{F}_p^*$ and $o(u) = n_1 n_2 \ldots n_s$ where each $n_i$ divides $m_i$, for $i = 1, \ldots, s$. Let $h_i = n/n_i$ for $i = 1, \ldots, s$. So $h_1, \ldots, h_s$ are coprime elements. Hence there are $c_1, \ldots, c_s$ such that

$$(\star) \quad c_1 h_1 + \cdots + c_s h_s = 1.$$

This argument can be formalized in $I\Delta_0+\Omega_1$ since we are dealing with a sequence of logarithmic length and whose elements are bounded in size. The coefficients $c_i$ can be chosen less than $\prod_{j\neq i} n_j$, and so $c_i < n^{\log d}$. More precisely, consider the $\Delta_0$-function $f\colon s \longrightarrow n^{\log d}$ defined as $f(i) = c_i h_i$. From Theorem 4.4 it follows that there is a $\Delta_0$-definable function $F\colon s \longrightarrow M$ such that $F(1) = h_1 c_1$ and $F(i+1) = F(i) + h_{i+1}c_{i+1}$, so $F(s) = 1$.

We can now write

$$u = u^1 = u^{c_1h_1+\cdots+c_sh_s} = u^{c_1h_1}u^{c_2h_2}\cdots u^{c_sh_s}$$

where $u^{c_ih_i} \in A(p_i)$ for $i = 1,\ldots,s$ and the product of the sequence $u^{c_1h_1}, u^{c_2h_2}, \ldots, u^{c_sh_s}$ is in the sense of [BD'A]. ∎

*Notation:* We will use the standard multiplicative notation of the decomposition of abelian groups, i.e. we will write

$$\mathbf{F}_p^* = A(p_1) \times A(p_2) \times \cdots \times A(p_s).$$

We will use the above decomposition in order to determine the index of the $r$-powers of $\mathbf{F}_p^*$ for $r$ prime in $\mathbf{N}$. In fact, it will be sufficient to decompose $\mathbf{F}_p^*$ into two parts, an $r$-part where all the elements have order a power of $r$, and a part in which all the elements have order coprime with $r$. To be more precise, we can decompose $\mathbf{F}_p^*$ as follows,

$$\mathbf{F}_p^* = A(r) \times \prod_{\substack{q \text{ prime} \\ q\neq r}} A(q).$$

LEMMA 4.7: *$A(r)$ is cyclic.*

*Proof:* It is straightfoward to adapt the proof of Lang, see [L].

In [BI] Berarducci and Intrigila proved in $I\Delta_0 + \Omega_1$ the classical result that the subgroup $(\mathbf{F}_p^*)^2$, of the squares of $\mathbf{F}_p^*$, has index 2 in $\mathbf{F}_p^*$. The classical proof involves a counting argument which is avoided in [BI]. From this result follows immediately the existence of an extension of degree 2 of $\mathbf{F}_p$. It is enough just to add the square root of a non-square.

In order to construct normal extensions of higher degree $r \in \mathbf{N}$ we will calculate the index of the $r$-powers in $\mathbf{F}_p^*$. The notion of splitting field of a polynomial does not seem to have a meaning in a model of $I\Delta_0 + \Omega_1$ for the reasons we discussed in section 2, and we will avoid it.

Denote the set of $r$-powers of $\mathbf{F}_p^*$ by $(\mathbf{F}_p^*)^r$.

THEOREM 4.8: *Let $r \in \mathbf{N}$. The index of $(\mathbf{F}_p^*)^r$ in $\mathbf{F}_p^*$ is either $r$ or 1, depending on whether $\mathbf{F}_p$ contains the primitive $r$-roots of unity or not.*

*Proof:* Consider the decomposition of $\mathbf{F}_p^*$ as

$$A(r) \times \prod_{\substack{q \text{ prime} \\ q \neq r}} A(q).$$

All elements of

$$\prod_{\substack{q \text{ prime} \\ q \neq r}} A(q)$$

are $r$ powers. Let $u \in \prod_{q \neq r} A(q)$, where $q$ is a prime and let $k$ be the order of $u$. Since $r$ and $k$ are coprime there exist $\lambda$ and $\mu$ such that $1 = \lambda r + \mu k$. Hence $u = u^{\lambda r + \mu k} = u^{\lambda r} u^{\mu k} = u^{\lambda r}$, and so $u$ is a power of $r$. The function $x \mapsto x^r$ is surjective restricted to $\prod_{q \neq r} A(q)$, where $q$ is a prime.

If $r$ does not divide the maximal order $d$ then $A(r)$ is trivial, there are no primitive $r$-roots of unity, and

$$\mathbf{F}_p^* = \prod_{\substack{q \text{ prime} \\ q \neq r}} A(q).$$

In this case all elements of $\mathbf{F}_p^*$ are $r$ powers, hence the map $x \mapsto x^r$ is surjective on $\mathbf{F}_p^*$ and so the index of $(\mathbf{F}_p^*)^r$ in $\mathbf{F}_p^*$ is 1.

If $r$ divides $d$ from Lemma 4.7 we have $A(r) =< \alpha >$ for some $\alpha$ in $\mathbf{F}_p^*$ and $o(\alpha) = r^k$ for some $k$. Notice that $k$ can be non standard. In this case $\mathbf{F}_p^*$ contains all the $r$-roots of unity, and these are

$$1, \alpha^{r^{k-1}}, \alpha^{2r^{k-1}}, \ldots, \alpha^{(r-1)r^{k-1}}.$$

Moreover, the image of the function $x \mapsto x^r$ restricted to $A(r)$ is generated by $\alpha^r$.

CLAIM: *The coset representatives of $(\mathbf{F}_p^*)^r$ are*

$$1, \alpha, \alpha^2, \ldots, \alpha^{r-1}.$$

We show first that $\alpha^i$ and $\alpha^j$ identify different cosets for $0 \leq i, j < r$ and $i \neq j$. Notice that all elements in $\prod_{q \neq r} A(q)$, where $q$ is a prime are in the same coset modulo $(\mathbf{F}_p^*)^r$. Suppose that $\alpha^i < \alpha^r >= \alpha^j < \alpha^r >$ for some $i, j < r$, this is equivalent to say $\alpha^{i-j} \in < \alpha^r >$ and this happens if and only if $i - j = 0$.

It is left to show that $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ are the only cosets representatives of $(\mathbf{F}_p^*)^r$. If $j \geq r$ then $j = rq + \rho$ for some $q, \rho$ such that $0 \leq \rho < r$, and $\alpha^j < \alpha^r >= \alpha^\rho < \alpha^r >$.

So the index of $(\mathbf{F}_p^*)^r$ in $\mathbf{F}_p^*$ is $r$. ∎

Notice that in the above proof we have avoided any counting argument, by exhibiting coset representatives of the $r$ powers in $\mathbf{F}_p^*$.

*Notation:* In the following we will use the more compact notation $A(r')$ to denote the set of all elements of $\mathbf{F}_p^*$ whose order is coprime with $r$.

## 5. Normal extensions

In this section we will consider normal extensions of $\mathbf{F}_p$ of finite degree, i.e. the degree is a natural number. As we have recalled in the introduction, in the classical case any finite field has a unique extension of each degree $n$ and this is the splitting field of the polynomial $x^{p^n} - x$. All extensions are Galois, i.e. normal and separable. In our case since $\mathbf{F}_p$ has characteristic 0 the separability of any extension follows. So it is left to establish the existence and uniqueness of normal extensions of $\mathbf{F}_p$ of degree $n$, for $n \in \mathbf{N}$. We will use the result established in the previous section on the index of $r$ powers in $\mathbf{F}_p^*$, and some classical results of Galois theory.

We need to recall the following result in Kummer theory about abelian extensions (see [L]).

THEOREM 5.1: *Let $K$ be a field of characteristic 0 and with primitive $n$ roots of unity. There is a one to one correspondence between the subgroups $B$ of $K^*$ containing $(K^*)^n$ and the abelian extensions of $K$ of exponent $n$. Moreover, if $K_B$ is the abelian extension corresponding to the subgroup $B$ then the dimension of $K_B$ over $K$ is equal to the index of $(K^*)^n$ in $B$.*

We apply now Theorem 5.1 to $\mathbf{F}_p$ in our setting.

COROLLARY 5.2: *Let $r \in \mathbf{N}$ be a prime which divides $d$, the maximal order. Then there exists a unique normal extension of $\mathbf{F}_p$ of degree $r$.*

*Proof:* Theorem 4.8 guarantees the existence of a normal extension of degree $r$. It is enough to add an $r$-root of an element which is not an $r$ power. Using Theorem 5.1 we get the uniqueness of an abelian (hence normal) extension of $\mathbf{F}_p$ of degree $r$. ∎

We can extend the result of Corollary 5.2 also to any $n \in \mathbf{N}$ with $n$ dividing $d$.

COROLLARY 5.3: *Let $n \in \mathbf{N}$ divide the maximal order $d$. Assume that $\mathbf{F}_p$ contains a primitive $n$-root of unity. Then there exists a unique normal extension of $\mathbf{F}_p$ of degree $n$.*

*Proof:* Decompose $\mathbf{F}_p^*$ as follows,

$$\mathbf{F}_p^* = \prod_{r|n} A(r) \times \prod_{s\nmid n} A(s).$$

As before all elements of $\prod_{s\nmid n} A(s)$ are $n$ powers and so they are all in the same coset modulo $(\mathbf{F}_p^*)^n$. As in the classical case, we have that $\prod_{r|n} A(r)$ is cyclic since the $A(r)$'s, $r$ dividing $n$, are cyclic (see Lemma 4.7). The image of the map $x \mapsto x^n$ restricted to $\prod_{r|n} A(r)$ is then generated by $\alpha^n$, and so the cosets representative of $(\mathbf{F}_p^*)^n$ are

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

Hence the index of $(\mathbf{F}_p^*)^n$ in $\mathbf{F}_p^*$ is $n$. We then get a normal abelian extension of degree $n$ and this is unique by Theorem 5.1. Notice that contrary to the case $r$ prime, there can be proper subgroups of $\mathbf{F}_p^*$ containing $(\mathbf{F}_p^*)^n$ but there is a unique one, namely $(\mathbf{F}_p^*)^n$, that has index $n$. ∎

We have then obtained the classical result on existence and uniqueness of an extension of degree $n$ for each standard $n$ which divides $d$. We will show later the uniqueness of a normal extension of degree $n$ for each $n$, leaving open the problem of the existence which will be solved in the last section.

*Remark:* The results of Corollary 5.2 and Corollary 5.3 can be extended to any finite extension $K$ of $\mathbf{F}_p$.

Using now some Galois theory we show a very sharp upper bound on the number of normal extensions of degree a power of a standard prime, with no assumption if the prime divides $d$ or not. We will prove it for any finite extension $K$ of $\mathbf{F}_p$.

LEMMA 5.4: *For no $r, k \in \mathbf{N}$, $r$ prime, does $K$ have two distinct normal extensions of degree $r^k$.*

*Proof:* We proceed by induction on $k$. Let $k = 1$. The case when $K$ contains the $r$-roots of unity has been dealt in Corollary 5.2. Suppose that $K$ does not contain primitive $r$-roots of unity and assume that $K$ has two distinct normal extensions $L_1$ and $L_2$ of degree $r$. Let $K(\mu_r)$ be the extension of $K$ obtained by adding the

primitive $r$-roots of unity. The dimension of $K(\mu_r)$ over $K$ is $h$, a divisor of $r-1$. Clearly, the three extensions $L_1, L_2$ and $K(\mu_r)$ are all abelian. We can embed $L_2$ and $K(\mu_r)$ into a common normal extension $N$ and consider the composite field $L_2K(\mu_r)$. From properties of the composite field it follows that since $L_2$ and $K(\mu_r)$ are both Galois extensions of $K$ then also $L_2K(\mu_r)$ is Galois over $K$, and hence normal. From $L_2$ and $K(\mu_r)$ being abelian it follows that $L_2K(\mu_r)$ is also abelian and the dimension of $L_2K(\mu_r)$ over $K$ is given by the product of the degree of $L_2$ over $K$ and the degree of $K(\mu_r)$ over $K$, i.e. $[L_2K(\mu_r) : L] = rh$. Hence from Corollary 5.2 it follows that $L_2K(\mu_r)$ is the unique normal extension of $K(\mu_r)$ of degree $r$. The extension $K(\mu_r)$ is also unique over $K$, being the splitting field of $x^r - 1$, hence $L_2K(\mu_r)$ is the unique normal extension of $K$ of degree $rh$. From elementary Galois theory the Galois group $G = G(L_2K(\mu_r)/K)$ has a unique subgroup $H$ of index $r$, since $r$ and $h$ are coprime, and so $H$ is normal in $G$. The fixed field of $H$ is a normal extension of $K$ of degree $r$, and so it has to coincide with $L_2$. If we repeat the argument with $L_1$ and $K(\mu_r)$ the field $L_1K(\mu_r)$ coincides necessarily with $L_2K(\mu_r)$. Hence the fixed field of the subgroup of $G(L_1K(\mu_r)/K)$ of index $r$ is $L_2$, and so $L_1 = L_2$.

Assume now that the result is true for $r^{k-1}$. We show it for $r^k$. Let $L_1, L_2$ be normal extensions of $K$ of degree $r^k$. The Galois group $G = G(L_1/K)$ of $L_1$ over $K$ is an $r$-group of order $r^k$, and so it has a normal subgroup $H$ of order $r^{k-1}$. If $F$ is the fixed field of $H$ then $F$ is a normal extension of $K$ of degree $r$. Repeating the argument for $L_2$ from what we proved before it follows that $F$ is the unique subfield of $L_2$ which is normal and of degree $r$ over $K$. We can now apply the inductive hypothesis to the normal extensions $L_1$ and $L_2$ of $F$ which have both degree $r^{k-1}$. ∎

We can now make significant progress towards determining the Galois theory of $\mathbf{F}_p$ and its finite extensions. This will give us further information on the number of normal extensions of any degree $n \in \mathbf{N}$. We recall the following definition of $Z$-group ($Z$ for Zassenhaus) as in [P].

*Definition 5.5:* A group $G$ is a $Z$-group if all its Sylow subgroups are cyclic.

Examples of $Z$-groups are $S_3$ and all the dihedral groups of the type $D_{2n+1}$. $Z$-groups occur naturally in our context.

THEOREM 5.6: *Let $L$ be any finite normal extension of $K$. If $G$ is the Galois group of $L$ over $K$ then $G$ is a $Z$-group.*

*Proof:* Let $H$ be an $r$-Sylow of $G$ of order $r^n$. If $L_H$ is the fixed field of $H$ in $L$ then $L$ is a normal extension of $L_H$ of degree $r^n$. So without loss of generality we

can assume that the degree of $L$ over $K$ is a power of a prime and so the Galois group is an $r$-group for some prime $r$. Let $o(G) = r^k$. We proceed by induction on $k$.

If $k = 1$ then $G$ is cyclic and there is nothing to prove. Let $o(G) = r^{k+1}$ and $Z$ be the center of $G$. $Z$ is non trivial since $G$ is an $r$-group. If $G$ is abelian but not cyclic, it has distinct normal subgroups of index $r$, giving $K$ distinct normal extensions of dimension $r$, contradicting Corollary 5.2. Hence $G$ is cyclic.

We show now that $G$ is necessarily abelian and hence complete the proof. Let $L_Z$ be the fixed field of the center $Z$. This is a normal extension of $K$ whose Galois group is isomorphic to the quotient $G/Z$, and $o(G/Z) < o(G)$. By inductive hypothesis $G/Z$ is cyclic generated by $\alpha Z$, and so $G$ is generated by $\alpha$ and $Z$. Since $\alpha^{-1} z \alpha = z$ for all $z \in Z$, $G$ is abelian, and as before $G$ is necessarily cyclic. ∎

## 6. Properties of Z-groups

Passman in [P] proves the following characterization of $Z$-groups from which the solvability of the group follows. We omit the proofs of these results and refer to [P].

THEOREM 6.1: (1) *Every $Z$-group is generated by two elements $x$ and $y$ which satisfy the following properties:*

$$x^n = y^m = 1, x^{-1}yx = y^r, (n, m) = (r - 1, m) = 1 \text{ and } r^n \equiv 1 (\mathrm{mod}\, m)$$

*and the derived group $G'$ is cyclic generated by $y$.*

(2) *Every $Z$-group is solvable.*

We get immediately the following corollaries.

COROLLARY 6.2: *The Galois group $G$ of a normal extension of $\mathbf{F}_p$, or any finite extension $K$ of it, is generated by two elements $x$ and $y$ which satisfy the following properties:*

$$x^n = y^m = 1, x^{-1}yx = y^r, (n, m) = (r - 1, m) = 1 \text{ and } r^n \equiv 1 (\mathrm{mod}\, m)$$

*and the derived group $G'$ is cyclic generated by $y$.*

In the classical case the Galois group of an extension of a finite field is generated by one element. We first prove that in our case it is generated by two elements, and later we will improve this by proving that the Galois group is cyclic.

COROLLARY 6.3: *The Galois group of a normal extension of* $\mathbf{F}_p^*$, *or any finite extension* $K$ *of it, is solvable.*

In the spirit of reproducing as much as possible of the classical results of finite fields, we clearly do not want any $S_n$ occurring as Galois group of a normal extension of $\mathbf{F}_p$. For $n \geq 5$ this follows from the above corollary. In order to exclude $S_4$ notice that the 2-Sylow in $S_4$ is $\mathbf{Z}_2 \times \mathbf{Z}_2$ and so $S_4$ cannot occur as the Galois group of a normal extension. To prove that $S_3$ cannot occur requires a more complex argument.

We consider now some properties of $Z$-groups which will be useful later, in a Galois-theoretic setting. When proofs are not given, see [P].

LEMMA 6.4: *Let* $G$ *be a* $Z$*-group and* $H$ *a* $p$*-Sylow of* $G$ *of order* $p^k$. *If* $H$ *is not contained in* $G'$, *the derived subgroup, then* $G$ *has a normal subgroup of index* $p^k$ *(a* $p$*-complement).*

LEMMA 6.5: *If* $G$ *is a* $Z$*-group then every subgroup and every quotient of* $G$ *is a* $Z$*-group.*

*Proof:* It is clear that a subgroup $H$ of $G$ is a $Z$-group since the Sylow subgroups of $H$ are subgroups of the Sylow subgroups of $G$ and hence they are cyclic. Let $G_1 = G/H$ where $H$ is a normal subgroup of $G$, and $\pi$ the natural projection of $G$ onto $G_1$. From elementary group theory we have that if $Q$ is a $p$-Sylow of $G$ then $\pi(Q) = QH/H$ is a $p$-Sylow of $G_1$ and $\pi(Q) \cong Q/Q \cap H$. Hence $QH/H$ is cyclic. Moreover, if $S_1/H$ is a $p$-Sylow of $G/H$ then there exists a $p$-Sylow $S$ of $G$ such that $SH/H$ is a $p$-Sylow of $G/H$, and hence $S_1/H$ and $SH/H$ are conjugate, and so $S_1/H$ is cyclic. This completes the proof. ∎

Notice that $Z$-groups are not closed under direct products, for example $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not a $Z$-group.

We will use the following result due to P. Hall which is a generalization of the Sylow's theorems for solvable groups (see [H]).

THEOREM 6.6: *Let* $G$ *be a solvable group of order* $nm$, *with* $(m, n) = 1$. *Then there exists a subgroup* $H$ *of* $G$ *of order* $n$. *Moreover, any two subgroups of order* $n$ *are conjugate, and if* $K$ *is a subgroup of* $G$ *whose order is coprime with* $m$ *then* $K$ *is contained in* $H$ *or a conjugate of* $H$.

LEMMA 6.7: *If* $G$ *is a* $Z$*-group then all subgroups of the same order are conjugate.*

*Proof:* Let $o(G) = nm$, $G =< x, y >$ with $x^n = y^m = 1$, $G' =< y >$, and $H$ be a subgroup of $G$ of order $n_1 m_1$ with $n_1$ dividing $n$ and $m_1$ dividing $m$. $H$

is solvable since $G$ is solvable, hence by Theorem 6.6 there is a subgroup $J$ of $H$ of order $m_1$ and $J \subseteq G'$. So $J$ is the unique subgroup of $G'$ of order $m_1$, i.e. $J =< y^{m/m_1} >$. $G'$ is a normal cyclic subgroup of $G$ and this implies that also $J$ is normal in $G$. Indeed, for any $t \in G$ we have $t^{-1}yt = y^h$ for some $h < n$, and this implies that $t^{-1}y^{m/m_1}t = (y^h)^{m/m_1} = (y^{m/m_1})^h \in J$. So, $J$ is also a normal subgroup of $H$. Theorem 6.6 implies also the existence of a subgroup $K$ of $H$ of order $n_1$. Since $o(K)$ divides the order of the subgroup $< x >$ of $G$ we have that $K \subseteq< x >$ or $K \subseteq g^{-1} < x > g$, for some $g \in G$. From $(o(K), o(J)) = 1$, $J \lhd H$, and $o(H) = o(J)o(K)$ it follows that $H = JK =< y^{m/m_1}, g^{-1}x^{n/n_1}g >$, for some $g \in G$. Consider now the conjugate of $H$ via $g^{-1}$, i.e. $gHg^{-1} =< gy^{m/m_1}g^{-1}, x^{n/n_1} >=< y^{m/m_1}, x^{n/n_1} >$. Notice that the last equality is true since $< gy^{m/m_1}g^{-1} >=< y^{m/m_1} >$, and this follows from the uniqueness of the subgroup of order $m_1$ in $G'$. ∎

An immediate consequence of the lemma is that if a subgroup of a $Z$-group is normal then it is the unique subgroup of that order. In terms of field theory we get

COROLLARY 6.8: *Let $K$ be a finite extension of $\mathbf{F}_p$.*

(i) *$K$ has at most one normal extension of each degree $k \in \mathbf{N}$.*

(ii) *If $K$ has a normal extension of degree $k$ then all extensions of $K$ of dimension $k$ are normal, and there is a unique such.*

In general, a normal subgroup of a normal subgroup is not normal in the group. For $Z$-groups this is true as shown in the next lemma.

LEMMA 6.9: *Let $G$ be a $Z$-group and $N$ a normal subgroup of $G$. If $H$ is a subgroup of $N$ then $H$ is normal in $G$.*

*Proof:* Assume $H \lhd N \lhd G$. Let $g \in G$, clearly $g^{-1}Hg < g^{-1}Ng = N$. Moreover, $N$ is a $Z$-group, so $N$ contains a unique normal subgroup of the order of $H$, hence $H = g^{-1}Hg$. ∎

This has an immediate consequence in the context we are working in. In general, if $L$ is a normal extension of $K$ and $F$ is a normal extension of $L$ it is not true that $F$ is normal over $K$. For example, $\mathbf{Q}(\sqrt{2})$ is a normal extension of $\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2})$ is a normal extension of $\mathbf{Q}(\sqrt{2})$, but $\mathbf{Q}(\sqrt[4]{2})$ is not normal over $\mathbf{Q}$. From Lemma 6.9 it follows that in our setting the property of being a normal extension is transitive. Let $L$ be a normal extension of $K$ and $G$ be the Galois group of $L$ over $K$. By elementary Galois theory if $N \lhd G$ then $fix(N)$ is a normal extension of $K$ of degree the index of $N$ in $G$. If $H \lhd N$ then $fix(H)$ is a normal

extension of $fix(N)$ of degree the index of $H$ in $N$. Since $G$ is a $Z$-group $H$ is normal in $G$ and so $fix(H)$ is a normal extension of $K$. To summarize

LEMMA 6.10: *Let $K$ be any finite extension of $\mathbf{F}_p$. If $L$ is a normal extension of $K$ and $F$ is a normal extension of $L$ then $F$ is normal over $K$.*

Using Lemma 6.10 we can prove now the existence of normal extensions of degree $r^k$ for each prime $r$ dividing $d$ and any $k$. We construct such extensions by steps. We need to assume that $r$ divides $d$ to start the induction (see Corollary 5.2).

COROLLARY 6.11: *$K$ has a unique (hence necessarily normal) extension of degree $2^n$, for all $n \in \mathbf{N}$.*

The construction of extensions of each degree $n$ is then reduced to construct extensions of prime degree.

## 7. Existence of normal extensions of each degree

We are going to use Albert's analysis from [Al] to get normal extension of prime degree $r$ with no assumption on $r$. Pop informed us that he has an unpublished analysis which is more explicitly cohomological.

We may as well look at the problem in full generality, and at the end apply an argument specific to our arithmetical setting.

So, for now, let $K$ be an arbitrary field of characteristic 0 and $r$ a prime. Suppose $K$ does not have a primitive $r$th root of unity and let $L = K(\mu_r)$ be the $r$-cyclotomic extension of $K$, of dimension $h$ say, where $h > 1$ and $(h, r) = 1$. If $M$ is a normal extension of $K$ of dimension $r$ then the composite field $LM$ is normal over $L$ of dimension $r$, and so by Kummer theory (see Theorem 5.1) is a radical extension of $L$. Albert shows how to detect if a radical extension of $L$ of dimension $r$ comes as above from a normal extension $M$ over $K$. We now spell out his computations in $L$. Fix a generator $\sigma$ of the Galois group of $L$ over $K$. There exists $t$ with $1 < t < r$, so that $\sigma(\mu_r) = \mu_r^t$. Choose $s$ with $1 < s < r$, $st \equiv 1 (\mathrm{mod}\, r)$ and $\delta$ with $1 < \delta < r$, $\delta h \equiv 1 (\mathrm{mod}\, r)$. For $0 \leq k \leq h$, let $s_k = \delta s^k$. Define a homomorphism $\Lambda : L^* \longrightarrow L^*$ by

$$\Lambda(\lambda) = \prod_{k=1}^{h} (\sigma^k(\lambda))^{s_k}.$$

Albert proved

THEOREM 7.1: *A field $K$ has a normal extension of dimension $r$ if and only if the image of $\Lambda$ in $L^*$ is not contained in the group of $r$th powers in $L^*$.*

Now we apply this to $K$ a residue field, or a finite extension thereof, reverting to our earlier notation and conventions. $L$ is $K(\mu_r)$, assumed to be a proper extension of $K$ (otherwise we already know $K$ has a normal extension of dimension $r$). Let $\sigma$ be as in the previous subsection. As remarked in section 2, $\sigma$ is definable in the model $\mathcal{M}$ by a $\Delta_0$-formula and it respects exponentiation ($\sigma$ is determined by its action on $r$th roots of unity). This implies that $\Lambda$ maps $A(r)$ to $A(r)$ and $A(r')$ to $A(r')$. In fact, the image of an $r$th power is sent to an $r$th power. Thus our task is to show that the image of $A(r)$ under $\Lambda$ is not included in $r$th powers, for we can then apply Albert's theorem to get a normal extension of $K$ of dimension $r$. $A(r)$ is cyclic of order $r^m$ say, with generator $\gamma$. Without loss of generality, $\mu_r = \gamma^{r^{m-1}}$. Now $\sigma(\gamma) = \gamma^\theta$ for some $\theta$ with $(\theta, r) = 1$, and $\theta^h \equiv 1 (\mathrm{mod}\, r^m)$. So,

$$\Lambda(\gamma) = \prod_{k=1}^{h} \gamma^{\delta\theta^k s^k} = \gamma^{\sum_{k=1}^{h} \delta\theta^k s^k}.$$

Now,

$$\sum_{k=1}^{h} \delta\theta^k s^k = \delta \sum_{k=1}^{h} (\theta s)^k.$$

But recall that $\gamma^{r^{m-1}} = \mu_r$, so $\sigma(\gamma)^{r^{m-1}} = \sigma(\mu_r) = \mu_r^t = \gamma^{r^{m-1}t}$, and also $\sigma(\gamma)^{r^{m-1}} = \gamma^{\theta r^{m-1}}$, so $\gamma^{r^{m-1}(\theta - t)} = 1$, i.e. $\theta \equiv t (\mathrm{mod}\, r)$. So, $\theta s \equiv ts \equiv 1 (\mathrm{mod}\, r)$, hence

$$\sum_{k=1}^{h} \delta\theta^k s^k \equiv \delta h (\mathrm{mod}\, r) \equiv 1 (\mathrm{mod}\, r).$$

Thus $\Lambda(\gamma)$ generates $< \gamma >$, so $\Lambda$ is surjective on $A(r)$. But since $L$ has a primitive $r$th root of unity, not every element of $A(r)$ is an $r$th power (see Theorem 4.8). So the image of $\Lambda$ is not contained in $(L^*)^r$, and we have proved

THEOREM 7.2: *$K$ has a normal extension of dimension $r$ for each prime $r$.*

Using the transitivity of normal extensions and previous theorem we get easily.

COROLLARY 7.3: *For each $n \in \mathbf{N}$, $K$ has a normal extension of dimension $n$.*

It is natural to ask if there are non normal extensions of $K$. The answer to this question is no. Suppose $L$ is a normal extension of $K$ of dimension $n$ and $L'$ an extension of $K$ of dimension $n$. Let $F$ be a normal extension of $L$ and $L'$. From

the trasitivity of normal extension it follows that $F$ is also a normal extension of $K$. Let $H$ and $H'$ be the subgroups of $G(F/K)$ which fix the elements of $L$ and $L'$, respectively. $H$ and $H'$ have both index $n$ and hence the same order, so by Lemma 6.7 $H$ and $H'$ are conjugates, and since $H$ is normal also $H'$ is normal. So also $L'$ is a normal extension of $K$ of dimension $n$ but this is in contradiction with the uniqueness of the normal extension of a fixed degree. We can state this as follows.

LEMMA 7.4: *If $G$ is the Galois group of a normal finite extension of $K$ then all subgroups of $G$ are normal.*

We can now prove the classical result that the Galois group of a normal extension is cyclic.

COROLLARY 7.5: *Let $L$ be a normal extension of $K$ of degree $n$. Then the Galois group $G = G(L/K)$ is cyclic.*

*Proof:* $G$ is a $Z$-group, so all $r$-Sylows of $G$ are cyclic and they are also all normal. Hence $G$ is the direct product of its $r$-Sylows and so $G$ is cyclic. ∎

## 8. Appendix

In this section we show how to construct a cyclic extension of dimension 3. We will use an idea from [S2], where the author investigates the groups which can occur as the Galois groups of an extension of the rationals. We only need some ideas used in the case of the Galois group being $\mathbf{Z}_3$. Serre considers the following polynomial in $X$ over $\mathbf{Q}(T)$,

$$(\star) \quad X^3 - TX^2 + (T-3)X + 1 = 0,$$

with discriminant $\Delta = (T^2 - 3T + 9)^2$. If $\Delta$ is not 0 and $\lambda$ is a root and is not 0 or 1, then the other two roots are $\frac{1}{1-\lambda}$ and $\frac{\lambda-1}{\lambda}$. Notice that neither one nor zero is a root. We will consider specializations $t$ of the variable $T$, $t$ ranging through our field $L$. Note first that if $\Delta(t) = 0$ then $t = \frac{3 \pm 3\sqrt{-3}}{2}$, so if $t \in L$ then $\sqrt{-3} \in L$, and $L$ has a primitive cube root of unity, and we have nothing to prove. So we can assume $\Delta(t) \neq 0$ for all $t \in L$. So either

(a) for all $T \in L$ the equation $X^3 - TX^2 + (T-3)X + 1 = 0$ has three distinct roots in $L$,

or

(b) $L$ has a normal extension with Galois group $\mathbf{Z}_3$.

We show that (a) conflicts with the weak pigeon hole principle, hence there is a polynomial $X^3 - TX^2 + (T-3)X + 1 = 0$, for some $T \in L$ whose splitting field over $L$ has $\mathbf{Z}_3$ as Galois group.

Let $\lambda \in L$, $\lambda \neq 0, 1$ and consider the three elements

$$\lambda, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda - 1}{\lambda}.$$

They are roots of the polynomial of degree 3

$$X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3,$$

where $\sigma_1 = \lambda + \frac{1}{1-\lambda} + \frac{\lambda-1}{\lambda}$, $\sigma_2 = \frac{\lambda}{1-\lambda} - \frac{1}{\lambda} + (\lambda - 1)$, and $\sigma_3 = 1$. Consider the map $f\colon L \longrightarrow L$ defined as follows

$$f(\lambda) = \frac{\lambda^3 - 3\lambda + 1}{\lambda^2 - \lambda}.$$

The function $f$ is defined for $\lambda \neq 0, 1$, so if $L$ has $q$ elements the domain of definition of $f$ has cardinality $q - 2$. Our aim is to prove that $f$ is not surjective establishing (b). If $T$ is not in the image of $f$ consider the polynomial $X^3 - TX^2 + (T-3)X + 1 = 0$, its roots are not in $L$ (if one is in the field also the other two are).

Assume that $f$ is surjective. We will define an injective map $h$ from $3q$ into $q$ contradicting the weak pigeon hole principle. Let $a < 3q$, so $a = 3b + r$ for some $b < q$ and $0 \leq r < 3$. In order to define $h(a)$ consider $f^{-1}(b)$, this is not empty because of the surjectivity of $f$. Define now $h(a)$ as the first, second or third root of $X^3 - bX^2 + (b-3)X + 1 = 0$ according to $r = 0, 1, 2$, respectively. $h$ is clearly injective, a contradiction.

*Note:* We have some hopes of elaborating this to give another proof of Theorem 7.2, using [D] .

## 9. Application

It is a standard result of the elementary theory of finite fields that if $L$ is a finite extension of $K$ then the norm map is surjective. This can be proved by counting (see for example [Sm]).

We could give an elementary proof also in our setting using quasicyclicity of $\mathbf{F}_p$, but we choose rather to give a cohomological proof, using the general result (proved e.g. in [S1], see also [LvdD]) that for a field $K$ the following are equivalent:

(a) For all finite normal extensions $L$ of $K$ the norm map $N_{L/K}$ is surjective.

(b) The absolute Galois group $G_K$ of $K$ has cohomological dimension 1.

(c) $G_K$ is a projective group.

(d) Each Sylow $r$-subgroup of $G_K$ is free pro-$r$.

We may now check for $K$ non standard finite that each Sylow $r$-subgroup of $G_K$ is free pro-$r$. Since each finite normal extension $L$ of $K$ has the Sylow $r$-subgroups of $G(L/K)$ cyclic, a standard projective limit argument shows that for any $r$ either

(i) the Sylow $r$-subgroups are free pro-$r$ on one generator,

or

(ii) the Sylow $r$-subgroups are finite cyclic.

In our situation (ii) cannot occur. For, suppose $G_r$ is a Sylow $r$-subgroup of $G_K$, with $G_r$ finite non trivial. If $F = Fix(G_r)$ then by Galois theory $G(F^{alg}/K) = G_r$. But, by Artin–Schreier characterization if $G(F^{alg}/K)$ is finite then $G(F^{alg}/K) = \mathbf{Z}_2$. Suppose $G(F^{alg}/K) = \mathbf{Z}_2$, so $r = 2$. But we have shown in Corollary 6.11 that $K$ has a normal extension of dimension 4, so $G_2$ cannot be $\mathbf{Z}_2$. This proves

THEOREM 9.1: *The norm map $N$: $L \longrightarrow K$ is surjective for all finite normal extensions $L$ of $K$.*

ACKNOWLEDGEMENT: We are grateful for advice and information from Professors Koenigsmann, Krajicek, Matzat and Pop.

## References

[Al] A. A. Albert, *Fundamental Concepts of Higher Algebra*, University of Chicago Press, 1956.

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

[B] J. H. Bennett, *On spectra*, Doctoral Dissertation, Princeton University, 1962.

[BD'A] A. Berarducci and P. D'Aquino, *$\Delta_0$-complexity of the relation $y = \Pi_{i \leq n} F(i)$*, Annals of Pure and Applied Logic **75** (1995), 49–56.

[BI] A. Berarducci and B. Intrigila, *Combinatorial principles in elementary number theory*, Annals of Pure and Applied Logic **55** (1991), 35–50.

[BCSS] L. Blum, F. Cucker, M. Shub and S. Smale, *Complexity and Real Computation*, Springer-Verlag, Berlin, 1998.

[Bu] S. Buss, *Bounded Arithmetic*, Bibliopolis, Naples, 1986.

[D'A] P. D'Aquino, *Local behaviour of Chebyshev theorem in models of* $I\Delta_0$, Journal of Symbolic Logic **57** (1992), 12–27.

[D] R. Dentzer, *Polynomials with cyclic Galois group*, Communications in Algebra **23** (1995), 1593–1603.

[GD] H. Gaifman and C. Dimitracopoulos, *Fragments of Peano Arithmetic and the MRDP-Theorem*, in *Logic and Algorithmic*, Monographie de L'Eiseignement Mathematique, Geneve, 1982, pp. 187–206.

[G] K. Godel, *Uber formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik **38** (1931), 173–198.

[HP] P. Hajek and P. Pudlak, *Metamathematics of First-Order Arithmetic*, Springer-Verlag, Berlin, 1991.

[H] M. Hall, *The Theory of Groups*, The Macmillan Company, New York, 1959.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers (3rd ed.)*, Oxford University Press, 1954.

[KP] J. Krajicek and P. Pudlak, *Some consequences of cryptographical conjectures for* $S_2^1$ *and* $EF$, manuscript, 1997.

[L] S. Lang, *Algebra*, Addison Wesley, Reading, 1993.

[LvdD] A. Lubotzky and L. van den Dries, *Subgroups of free profinite groups and large subfields of* $\tilde{\mathbf{Q}}$, Israel Journal of Mathematics **39** (1981), 25–45.

[M1] A. Macintyre, *Residue fields of models of* $P$, in *Logic, Methodology and Philosophy of Science VI* (L. E. Cohen et al., eds.), North-Holland, Amsterdam, 1982, pp. 193–206.

[M2] A. Macintyre, *The strength of weak systems*, in *Logic, Philosophy of Science and Epistemology*, Proceeding of the 11th International Wittgenstein Symposium, Holder-Pichler-Tempsky, Wien, 1986.

[MM] A. Macintyre and D. Marker, *Primes and their residue rings in models of open induction*, Annals of Pure and Applied Logic **43** (1989), 57–77.

[Ma] Yu. Manin, *A Course in Mathematical Logic*, Springer-Verlag, Berlin, 1977.

[Mi] G. L. Miller, *Riemann's Hypothesis and tests for primality*, Journal of Computer and Systems Sciences **13** (1976), 300–317.

[Pa] R. Parikh, *Existence and feasibility in Arithmetic*, Journal of Symbolic Logic **36** (1971), 494–508.

[PWW] J. Paris, A. Wilkie and A. Woods, *Provability of the pigeon hole principle and the existence of infinitely many primes*, Journal of Symbolic Logic **53** (1988), 1235–1244.

[P] D. S. Passman, *Permutation Groups*, Benjamin, New York, 1968.

[Pr] V. Pratt, *Every prime has a succinct certificate*, SIAM Journal on Computing **4** (1975), 214–220.

[R] J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, Berlin, 1995.

[S1] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[S2] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[Sh] I. Shparlinski, *Computational and Algorithmic Problems in Finite Fields*, Kluwer, Dordrecht, 1992.

[Sm] C. Small, *Arithmetic of Finite Fields*, Dekker, New York, 1991.

[WP] A. Wilkie and J. B. Paris, *On the scheme of induction for bounded arithmetic formulas*, Annals of Pure and Applied Logic **35** (1987), 261–302.

[W] A. Woods, *Some problems in logic and number theory and their connections*, Ph.D. thesis, Manchester University, 1981.