Internat. J. Math. & Math. Sci.
Vol. 8 No. 2 (1985) 373-388

ON FUNDAMENTAL SETS OVER A FINITE FIELD

YOUSEF ABBAS and JOSEPH J. LIANG

Department of Mathematics
University of South Florida
Tampa, Florida 33620 U.S.A.

(Received March 3, 1983)

ABSTRACT. A partition over finite field is defined and each equivalence class is constructed and represented by a set called the fundamental set. If a primitive element is used to construct the addition table over these fundamental sets then all additions over the field can be computed. The number of partitions is given for some finite fields.

KEY WORDS AND PHRASES. Finite field, primitive polynomial.
1980 MATHEMATICS SUBJECT CLASSIFICATION CODE. 12C99.

1. INTRODUCTION

Throughout, p,q will be fixed but arbitrary primes.

Let $\alpha \in GF(p^n)$; $n > 1$ and define $A = A_\alpha = \{\alpha, \alpha+1, \alpha+2, \ldots, \alpha+(p-1)\}$. If $\beta \in A_\alpha$, then $A_\beta = A_\alpha$. Define $2A_\alpha, 3A_\alpha, \ldots, (p-1)A_\alpha$ such that $\ell A_\alpha = \{\ell x / x \in A_\alpha\}$ $\ell = 1,2,\ldots,p-1$, thus $\ell A_\alpha = A_{\ell\alpha}$.

DEFINITION. $$^*A_\alpha \equiv \bigcup_{\ell=1}^{p-1} \ell A_\alpha = \bigcup_{\ell=1}^{p-1} A_{\ell\alpha}.$$

Note that if $\beta \in {}^*A_\alpha$, then ${}^*A_\alpha = {}^*A_\beta$.

DEFINITION. $A_\alpha^{p^\ell} = \{x^{p^\ell} / x \in A_\alpha\}$ for $\ell = 0,1,2,\ldots$, so, $A_\alpha^{p^\ell} = \alpha^{p^\ell}, \alpha^{p^\ell}+1, \ldots, \alpha^{p^\ell}+(p-1)\} = A_{\alpha^{p^\ell}}$. Since $\alpha^{p^n} = \alpha$ for every $\alpha \in GF(p^n)$, we have $A_\alpha^{p^n} = A_\alpha$. Therefore, the values of ℓ in the definition can be limited to $0,1,2,\ldots,n-1$.

DEFINITION. $$^*A_\alpha^{p^\ell} \equiv {}^*A_{\alpha^{p^\ell}} = {}^*(A_\alpha^{p^\ell}).$$

DEFINITION. $$\bar{A}_\alpha = \bigcup_{\ell=0}^{n-1} {}^*A_\alpha^{p^\ell}$$

thus, $\bar{A}_\alpha = \{a\alpha^{p^j}+b \mid a \in Z_p^*, b \in Z_p \text{ and } j \in Z_n\}$.

LEMMA 1.1. If $\beta \in \bar{A}_\alpha$, then $\bar{A}_\alpha = \bar{A}_\beta$.

PROOF. If $\beta \in \bar{A}_\alpha$, then there exist $a \in Z_p^*$, $b \in Z_p$ and $j \in Z_n$ such that $\beta = a\alpha^{p^j} + b$. This implies $\bar{A}_\beta \subset \bar{A}_\alpha$. Since $(Z_p,+,.)$ is a field and $a \neq 0$ both $a^{-1}, -b$ exist. Therefore, $\alpha = a^{-1}\beta^{p^{n-j}} + a^{-1}(-b)$ which says $\alpha \in \bar{A}_\beta$. Hence $\bar{A}_\alpha \subset \bar{A}_\beta$ or $\bar{A}_\alpha = \bar{A}_\beta$.

DEFINITION. A_α will be called a Fundamental Set.

Since $A_\alpha^{p^n} = A_\alpha$ for every $\alpha \in GF(p^n)$, there exists a least positive integer $m \leq n$ such that $A_\alpha^{p^m} = a A_\alpha$ for some $a \in Z_p^*$. It follows that $\bar{A}_\alpha = \bigcup_{\ell=0}^{m-1} {}^*A_\alpha^{p^\ell}$.

DEFINITION. Let $\alpha, \beta \in GF(p^n)$. We define the relation $\sim$ in $GF(p^n)$ as

$$\alpha \sim \beta \text{ iff } \bar{A}_\alpha = \bar{A}_\beta$$

THEOREM 1.1. From Lemma 1.1. the relation $\sim$ is an equivalence relation.

This equivalence relation $\sim$ will partition the field $GF(p^n)$ into equivalence classes $\bar{A}_\alpha$ and each class is represented by a fundamental set.

DEFINITION. $\bar{A}_\alpha$ will be called a Fundamental Class.

Let θ be a primitive element in $GF(p^n)$. Since, $\theta^{\frac{p^n-1}{p-1}}$ is primitive in Z_p, then for every $a \in Z_p^*$ there exists k_a, where $1 \leq k_a \leq p-1$. So, k_a can be determined easily. If the elements of the fundamental set A_α are expressed as powers of θ, then $\bar{A}_\alpha$ can be expressed from A_α as powers of θ. So to calculate the addition table of $\bar{A}_\alpha$, it is sufficient to have the addition table of A_α. Therefore, if $\bar{A}_{\alpha_1}, \bar{A}_{\alpha_2}, \ldots, \bar{A}_{\alpha_s}$, are all the fundamental classes in $GF(p^n)$, it will be enough to tabulate only the addition tables over $A_{\alpha_1}, \ldots, A_{\alpha_s}$ with respect to θ to do all the calculations over $GF(p^n)$.

If for some $\alpha \in GF(p^n)$, m is the least positive integer such that $\alpha^{p^m} = a\alpha + b$ for some $a \in Z_p^*$ and $b \in Z_p$, then it is true that m will be the smallest positive integer for every $\beta \in \bar{A}_\alpha$ such that $\beta^{p^m} = a\beta + b'$ where $b' \in Z_p$. This will be shown below.

DEFINITION. Let $\alpha \in GF(p^n)$, if m is the least positive integer such that $\alpha^{p^m} = a\alpha + b$ for some $a \in Z_p^*$, $b \in Z_p$ then m is called the index of α and a is the coefficient of α and we say α has an index m with coefficient a. If $\alpha \in Z_p$ we say α has index 0 with coefficient $a = 1$.

LEMMA 1.2. If α has index m with coefficient a, then every $\beta \in \bar{A}$ has the same index m and the same coefficient a.

PROOF. Let $\beta \in \bar{A}$ with index s and $\beta \notin Z_p$. There exist $\ell \in Z_p^*$, $\delta \in Z_p$ and $j \in Z_n$ such that $\beta = \ell\alpha^{p^j} + \delta$. This implies $\beta^{p^m} = (\ell\alpha^{p^j} + \delta)^{p^m} = \ell(a\alpha + b)^{p^j} + \delta = a\beta + c$ where $c \in Z_p$. Therefore $s \leq m$. But from Lemma 1.1. we have $\bar{A}_\alpha = \bar{A}_\beta$. Hence $\alpha \in \bar{A}$. Therefore $m \leq s$, which implies β has index m with coefficient a.

DEFINITION. The fundamental set A_α has index m with coefficient a if and only if m is the least positive integer such that $A^{p^m} = aA$.

THEOREM 1.2. If α has index m with coefficient a, then A_α has index m with coefficient a and each fundamental set $A_\beta \subset \bar{A}_\alpha$ has the same index m with the same coefficient a.

PROOF. Follows from Lemma 1.2.

From the above theorem we can define the index $\bar{A}_\alpha$ to be the index of any element or any fundamental set included in $\bar{A}_\alpha$.

Now, we want to discuss some properties of the index and the coefficient of the fundamental set.

THEOREM 1.3. In $GF(p^n)$, if A has index m and coefficient a then m divides n and $a^{n/m} = 1$.

PROOF. Let $n = \ell m + r$, $0 \le r < m$. Since $\alpha^{p^m} = a\alpha + b$, for some $b \in Z_p$, we have $\alpha^{p^{\ell m}} = a^{\ell}(\alpha) + (a^{\ell-1} + a^{\ell-2} + \ldots + 1)b$ and $\alpha = \alpha^{p^n} = (\alpha^{p^{\ell m}})^{p^r} = a^{\ell}\cdot\alpha^{r} + (a^{\ell-1} + a^{\ell-2} + \ldots + 1)b$. So, $A^{p^r} = a^{\ell}A$ which implies $r = 0$ and $a = a^{n/m} = 1$.

THEOREM 1.4. Let A be a fundamental set with index m and coefficient a. If $A^{p^{\ell}} = bA$, $b \in Z_p^*$, then m divides ℓ and $a^{\ell/m} = b$.

PROOF. Since m is the index of A, we have $m \le \ell$. Let $\ell = km + r$, $0 \le r < m$. If $\alpha \in A$, then there exist δ, $\delta' \in Z_p$ such that $\alpha^{p^m} = a\alpha + \delta$ and $\alpha^{p^{\ell}} = b\alpha + \delta'$. But $b\alpha + \delta' = (\alpha^{p^{km}})^{p^r} = (a^k\alpha + \delta^*)^{p^r} + \delta' = a^k\alpha^{p^r} + \delta''$. This implies $r \ge m$. Therefore $r = 0$. Hence $m \mid \ell$ and $a^{\ell/m} = b$. Note: Since all finite fields of the same order are isomorphic, if $\alpha_1 \in GF_1(p^n)$ having index m with coefficient a, is the image of $\alpha_2 \in GF_2(p^n)$ under an isomorphism σ, then α_2 has index m with coefficient a. Therefore, $GF_1(p^n)$ and $GF_2(p^n)$ have the same partitions with respect to the equivalence relation $\sim$.

EXAMPLE: Let $F = GF(5^2)$ and θ be a primitive element in F such that θ satisfies the primitive polynomial [indexing polynomial], $P(x) = x^2 + 4x + 2$. The field F has two equivalence classes, Z_5 and $\bar{A}_\theta$. $A_\theta = \{\theta, \theta + 1 = \theta^{22}, \theta + 2 = \theta^{15}, \theta + 3 = \theta^2, \theta + 4 = \theta^{17}\}$. So, we have $\theta \to \theta^{22} \to \theta^{15} \to \theta^2 \to \theta^{17}$. Since $\theta^6 = 2$, then $4 = \theta^{12}$ and $3 = \theta^{18}$. Therefore,

$$2A_\theta = \{\theta^7, \theta^7 + 2 = \theta^4, \theta^7 + 4 = \theta^{21}, \theta^7 + 1 = \theta^8\},$$

$$3A_\theta = \{\theta^{19}, \theta^{19} + 3 = \theta^{16}, \theta^{19} + 1 = \theta^{10}, \theta^{19} + 4 = \theta^{21}, \theta^{19} + 2 = \theta^6\},$$

$$4A_\theta = \{\theta^{13}, \theta^{13} + 4 = \theta^{10}, \theta^{13} + 3 = \theta^3, \theta^{13} + 2 = \theta^{14}, \theta^{13} + 1 = \theta^5\}$$

and $A_\theta^5 = 4A_\theta$.

2. SOLUTIONS OF EQUATIONS OF THE FORM $A^{p^m} = aA$.

To study the fundamental sets in $GF(p^n)$ with index $m < n$, we have to study the solutions of: (a) $x^{p^m} = ax + \delta$; $a \in Z_p^*$, $a \ne 1$, $\delta \in Z_p$ and (b) $x^{p^m} = x + \delta$; $\delta \in Z_p^*$ in $GF(p^n)$. Note: If $\delta = 0$ in (b), then all the elements of the subfield $GF(p^m)$ will satisfy (b).

We will now consider the solutions of

$$x^{p^m} = ax + \delta \tag{2.1}$$

where $a \in Z_p^*$, $a \ne 1$ and $\delta \in Z_p$.

LEMMA 2.1. Equation (2.1) has a solution $\alpha \notin Z_p$ with index m only if m divides n and $a^{n/m} = 1$.

The proof is a direct application of Theorem 1.3 and Theorem 1.4.

LEMMA 2.2. In equation (2.1), for $y = x + \frac{\delta}{a-1}$, we have $y^{p^m} = ay$.

PROOF.

$$y^{p^m} = (x + \frac{\delta}{a-1})^{p^m} = x^{p^m} + \frac{\delta}{a-1}$$

$$= ax + \delta + \frac{\delta}{a-1} = a(y - \frac{\delta}{a-1}) + \frac{a\delta}{a-1}$$

$$= ay.$$

Therefore, to study the solutions of (2.1), it is sufficient to study the solutions of $y^{p^m} = ay$.

LEMMA 2.3. $x = \frac{\delta}{1-a}$ is a solution of equation (2.1).

If θ is a primitive element in $GF(p^n)$, then the following statements are true:

(a) $\theta^{\frac{p^n-1}{p-1}} \in Z_p^*$

(b) For every $a \in Z_p^*$ there exists an integer k_a such that $a = \theta^{\frac{p^n-1}{p-1}k_a}$, where $0 \leq k_a < p-1$. If $a \neq 1$, $k_a \neq 0$.

LEMMA 2.4. For every m such that m divides n and $\frac{n}{m} \mid p-1$, then $\frac{p^n-1}{p^m-1} \cdot \frac{1}{n/m}$ is an integer.

PROOF. Let $\frac{n}{m} = k$. So, $p \equiv 1 \pmod{k}$ and $\frac{p^n-1}{p^m-1} = \frac{(p^m)^k-1}{p^m-1} = (p^m)^{k-1} + (p^m)^{k-2} + \ldots + 1$. Since $p \equiv 1 \pmod{k}$, we have $p^j \equiv 1 \pmod{k}$ for $j = 1,2,\ldots$. Therefore, $\sum_{j=0}^{k-1} (p^m)^j \equiv 0 \pmod{k}$. Hence $\frac{n}{m} \left| \frac{p^n-1}{p^m-1} \right.$.

LEMMA 2.5. If $a^{n/m} = 1$, $a \neq 1$ and $\frac{n}{m} \mid p-1$, then $\frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1}$ is an integer.

PROOF. $\frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} = \frac{p^n-1}{p^m-1} \cdot \frac{1}{n/m} \cdot \frac{(n/m)k_a}{p-1}$.

But, from Lemma 2.4 $\frac{p^n-1}{p^m-1} \cdot \frac{1}{n/m}$ is an integer. Also, $a = \theta^{\frac{p^n-1}{p-1} \cdot k_a}$ implies $a^{n/m} = \theta^{\frac{p^n-1}{p-1} \cdot k_a \cdot \frac{n}{m}} = 1$. Therefore, $\frac{p^n-1}{p-1} k_a \cdot \frac{n}{m} \equiv 0 \bmod (p^n-1)$. So $p-1 \left| k_a \cdot \frac{n}{m} \right.$.

THEOREM 2.1. Given $x^{p^m} = ax$ (2.2)

where $m \mid n$, $a \neq 1$ and $O(a) = \frac{n}{m}$, then

(a) Equation (2.2) has solution α in $GF(p^n)$ and $\alpha \in Z_p$.

(b) If α is a solution of (2.2) where $\alpha = \theta^r$, θ is primitive in $GF(p^n)$, then

$$r \equiv \frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} \pmod{\frac{p^n-1}{p^m-1}}.$$

(c) $x = 0$ is the only solution of (2.2) in Z_p.

PROOF.

(a) If $x \in Z_p$, then $x^{p^m} = x = ax$. Therefore $x = 0$.

(b) Since $x^{p^m} = ax$ and $a \neq 1$, then $x \notin GF(p^m)$.

(c) If θ^r is a solution of (2.2) then $(\theta^r)^{p^m-1} = a = \theta^{\frac{p^n-1}{p-1} k_a}$. Thus,

$$r(p^m-1) \equiv \frac{p^n-1}{p-1} k_a \pmod{p^n-1}$$

which implies $r \equiv \frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} \pmod{\frac{p^n-1}{p^m-1}}$.

It follows from Lemma 2.5 that the above congruence is meaningful.

THEOREM 2.2. For every $r \equiv \frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} \pmod{\frac{p^n-1}{p^m-1}}$, θ^r is a solution of (2.2).

PROOF. Let $r = \frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} + j\frac{p^n-1}{p^m-1}$; $j = 0,1,2,\ldots$ then

$(\theta^r)^{p^m-1} = \theta^{\frac{p^n-1}{p-1}\cdot k_a} \cdot (\theta^{p^n-1})^j = a \cdot 1 = a$. So, $(\theta^r)^{p^m} = a\theta$.

Now consider the solutions of

$$x^{p^m} = ax + \delta \tag{2.3}$$

where $a \neq 1$, $a \in Z_p^*$, $\delta \in Z_p$, $m|n$ and $O(a) = \frac{n}{m}$. From Lemma 2.2, Theorem 2.1 and Theorem 2.2, we have $\theta^r + \frac{\delta}{1-a}$ is a solution of (2.3), where $r \equiv \frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} \pmod{\frac{p^n-1}{p^m-1}}$ and $\frac{\delta}{1-a}$ is the only solution in Z_p.

THEOREM 2.3. Let A be a fundamental set in $GF(p^n)$ with index m and coefficient $a \neq 1$. If A is not included in any proper subfield of $GF(p^n)$, then $O(a) = \frac{n}{m}$ and $\frac{n}{m} | (p-1)$.

PROOF. Let $O(a) = d$ and $\alpha \in A$. It follows $d|\frac{n}{m}$ and α has an index m with coefficient a. Thus, $\alpha^{p^m} = a\alpha + \delta$ for some $\delta \in Z_p$. Hence $\alpha^{p^{dm}} = a^d\alpha + (\alpha^{d-1} + \alpha^{d-2} + \ldots + 1)\delta = \alpha$. Therefore $\alpha \in GF(p^{dm})$, which implies $GF(p^{dm}) = GF(p^n)$ and $d = \frac{n}{m}$.

COROLLARY 2.1. Let $X^{p^m} = aX + \delta$ (2.4)

such that $a \neq 1$, $\delta \in Z_p$, $m|n$, $a^{\frac{n}{m}} = 1$ and $O(a) = \ell$, then equation (2.4) has solutions in $GF(p^n)$ and all the solutions are included in $GF(p^{\ell m})$.

PROOF. $GF(p^{\ell m})$ is a subfield of $GF(p^n)$. Equation (2.4) satisfies the conditions of Theorem 2.1 over $GF(p^{\ell m})$ and if α is a solution, then $\alpha^{p^{\ell m}} = a^\ell\alpha + (a^{\ell-1} + a^{\ell-2} + \ldots + 1)\delta = \alpha + 0 = \alpha$. Therefore $\alpha \in GF(p^{\ell m})$.

Note: If θ is a primitive element in $GF(p^n)$, then $\gamma = \theta^{\frac{p^n-1}{p^{\ell m}-1}}$ is a primitive element in $GF(p^{\ell m})$. Therefore, the solutions of equation (2.4) are of the form: $\gamma^{r'} + \frac{\delta}{1-a}$ where $r' \equiv \frac{p^{\ell m}-1}{p^m-1} \cdot \frac{k'_a}{p-1} \pmod{\frac{p^{\ell m}-1}{p^m-1}}$ and $a = \gamma^{\frac{p^{\ell m}-1}{p-1}k'_a}$. Since $a = \theta^{\frac{p^n-1}{p-1}k_a}$, we have $\theta^{\frac{p^n-1}{p-1}k_a} = (\theta^{\frac{p^n-1}{p^{\ell m}-1}\cdot\frac{p^{\ell m}-1}{p-1}k'_a}) = \theta^{\frac{p^n-1}{p-1}k'_a}$.

So, $k_a = k'_a$. Therefore, the solutions of (2.4) over $GF(p^n)$ are of the form $\theta^r + \frac{\delta}{1-a}$, where

$$r = \frac{p^n-1}{p^{\ell m}-1} \cdot r' \equiv \frac{p^n-1}{p^m-1} \cdot \frac{k_a}{p-1} \pmod{\frac{p^n-1}{p^m-1}}.$$

LEMMA 2.6. Equation (2.4) has p^m solutions in $GF(p^n)$.

PROOF. Corollary 2.1 insures that equation (2.4) has solution in $GF(p^{\ell m})$. From the previous note, Theorem 2.1 and Theorem 2.2 we have $\alpha_0 = \theta^{\frac{p^n-1}{p^m-1}\cdot\frac{k_a}{p-1}}$ and $\alpha_0 + \frac{\delta}{1-a}$ is a solution and if $\alpha \in H = \{\alpha_0 \cdot \beta + \frac{\delta}{1-a} \mid \beta \in GF(p^m)\}$, then α is a solution of (2.4). It is clear that H has p^m elements.

THEOREM 2.4. For every m divides n and every $a \in Z_p^*$, $a \neq 1$ such that $O(a) \mid \frac{n}{m}$, there exists a fundamental set in $GF(p^n)$ with index m and coefficient a.

PROOF. By Lemma 2.6, $x^{p^m} = ax$ has solutions in $GF(p^n)$. If θ is a primitive element in $GF(p^n)$ then $\alpha = \theta^{\frac{p^n-1}{p^m-1}\cdot k_a}$ is a solution. We claim that α has an index m with coefficient a. To prove this, we assume α has an index $\ell < m$ with coefficient b, therefore by Theorem 1.4 and Theorem 2.2 we conclude that α is a solution of $x^{p^\ell} = bx$ and it is of the form θ^s where $s \equiv \frac{p^n-1}{p^\ell-1}\cdot\frac{k_b}{p-1} \bmod (\frac{p^n-1}{p^\ell-1})$.

So, there exists j where $j \geq 0$ such that:

$$\frac{p^n-1}{p^\ell-1}\cdot\frac{k_b}{p-1} + j\,\frac{p^n-1}{p^\ell-1} = \frac{p^n-1}{p^m-1}\cdot\frac{k_a}{p-1}$$

then $0 \leq j = \frac{1}{p-1}\left[\frac{k_a}{p^m-1/p^\ell-1} - k_b\right]$.

Since $\frac{p^m-1}{p^\ell-1} > p$, $k_a < p-1$ and $1 \leq k_b$ we will have

$$0 \leq j < \frac{1}{p-1}\left[\frac{p-1}{p} - 1\right] < 0$$

and this is a contradiction.

Hence $A = A_\alpha$ is a fundamental set with index m and coefficient a.

COROLLARY 2.2. The minimum subfield which contains all the solutions of equation (2.4) is $GF(p^{\ell m})$.

PROOF. The proof is a direct application of Theorem 1.3 and Theorem 2.4.

We will now review some known facts about the solutions of $x^{p^m} = x + b$ in the field $GF(p^n)$.

Let $x^{p^m} = x + b$, where $b \in GF(p^n)$ (2.5)

and $d = g.c.d.\ (m, n)$ and $r = \frac{n}{d}$. The following theorems were given in [1].

LEMMA 2.7. If x_0 is a solution of (2.5) in $GF(p^n)$, then for every $j = 1, 2, \ldots, p^d-1$, $\left(x_0 + \theta^{\frac{p^n-1}{p^d-1}j}\right)$ is a solution of (2.5) where θ is a primitive element in $GF(p^n)$.

PROOF.

$$\left(x_0 + \theta^{\frac{p^n-1}{p^d-1}}\right)^{p^m} = x_0^{p^m} + (\theta^{p^m})^{\frac{p^n-1}{p^d-1}j}$$

$$= (x_0 + b) + \theta^{\frac{p^n-1}{p^d-1}j} = \left(x_0 + \theta^{\frac{p^n-1}{p^d-1}j}\right) + b$$

THEOREM 2.5. The number of solutions of (2.5) in $GF(p^n)$ is either 0 or p^d.

THEOREM 2.6. Equation (2.5) has solutions in $GF(p^n)$ if and only if

$$\sum_{\ell=0}^{r-1} b^{p^{\ell d}} = 0.$$

If we assume m divides n and $b \in Z_p^*$ in the equation

$$x^{p^m} = x + b \tag{2.6}$$

then we can conclude the following:

(a) $d = m = g \cdot c \cdot d(m.n)$,

(b) for every $b \in Z_p^*$, we have

$$\sum_{\ell=0}^{\frac{n}{m}-1} p^{\ell m} = \sum_{\ell=0}^{\frac{n}{m}-1} b = \frac{n}{m} b = 0$$

if and only if p divides $\frac{n}{m}$.

Now, we can restate the following theorems:

(a) Theorem 2.7. Equation (2.6) has solution in $GF(p^n)$ if and only if p divides $\frac{n}{m}$.

(b) Theorem 2.8. If equation (2.6) has a solution in $GF(p^n)$, it has p^m solutions, also if x_0 is a solution then $x_0 + \theta^{\frac{p^n-1}{p^m-1}j}$, $j = 0,1,\ldots,p^m - 1$ is a solution where θ is primitive in $GF(p^n)$.

THEOREM 2.9. If (2.6) has a solution in $GF(p^n)$, then the minimum subfield that contain all the solutions is $GF(p^{pm})$.

PROOF. Since equation (2.6) has a solution and m divides n then by Theorem 2.7 p divides $\frac{n}{m}$, therefore $GF(p^{pm})$ is a subfield of $GF(p^n)$. If α is a solution of (2.6), then we have $\alpha^{p^m} = \alpha + b$, which implies $\alpha^{p^{pm}} = \alpha + pb = \alpha$ so $\alpha \in GF(p^{pm})$ and $\alpha \notin GF(p^m)$ [$b \neq 0$].

Let $GF(p^\ell)$ be the minimum subfield which contains all the solutions of (2.6) therefore

$$GF(p^\ell) \subset GF(p^{pm})$$

and $\ell \neq m$. This implies $\ell \mid pm$. But since equation (2.6) has p^m solutions in $GF(p^\ell)$ and by Theorem 2.5 and Theorem 2.6, $g \cdot c \cdot d(m,\ell) = m$. Hence, $m \mid \ell \mid pm$. Therefore, $pm = \ell$.

LEMMA 2.8. If α is a solution of (2.6) in $GF(p^n)$ where α has an index s with coefficient a then s divides m and $a = 1$.

PROOF. Theorem 1.4 implies $s|m$. Let $\frac{m}{s} = r$. Assumes $a \neq 1$ and $\alpha^{p^s} = a\alpha + \delta$ for some $\delta \in Z_p$, therefore $\alpha^{p^m} = \alpha^{p^{rs}} = a^r\alpha + (a^{r-1} + a^{r-2} + \ldots + 1)\delta = \alpha + b$. Hence $a^r = 1$ and $a^{r-1} + a^{r-2} + \ldots + 1 = 0$ which implies $b = 0$, but this contradicts the condition $b \neq 0$ of equation (2.6).

COROLLARY 2.3. In $GF(p^n)$, for every m divides n and p divides $\frac{n}{m}$, there exist $(p-1)p^m$ elements α, where $\alpha \in A_\alpha$, such that $A_\alpha^{p^m} = A_\alpha$ and $A_\alpha \notin GF(p^m)$.

PROOF. Equation (2.6) has p^m solutions over $GF(p^n)$ for fixed $b \in Z_p^*$ and there are $p-1$ different values for b.

COROLLARY 2.4. In $GF(p^n)$, if m is a prime, then all solutions of (2.6) have index m with coefficient $a = 1$.

PROOF. This is a direct consequence of Lemma 2.8.

THEOREM 2.10. In equation (2.6) if p divides $\frac{n}{m}$, then there exists an α where α is a solution of (2.6) and α has an index m with coefficient 1.

PROOF. Since $p|\frac{n}{m}$, then (2.6) has p^m solutions. Also by Lemma 2.8, if α has an index s with coefficient $a = 1$ where $s|m$, then α satisfies $x^{p^s} = x + \delta$ (2.7) where $\delta = \frac{m}{s}(b)$, hence $s|m$ and $p|\frac{n}{m}$. By Theorem 2.7 and Theorem 2.8, equation (2.7) has p^s solutions. Let $\{s_1, s_2, \ldots, s_\ell\}$ be the set of all the indices of the solutions of (2.6) such that $1 \leq s_i < s_j < m$ for every $1 < j \leq \ell$. Since $s_\ell \leq \left[\frac{m}{2}\right]$ where $\left[\frac{m}{2}\right]$ is the greatest integer less than or equal to $\frac{m}{2}$, we have

$$p^m \leq p^{s_1} + p^{s_2} + \ldots + p^{s_\ell} \leq p + p^2 + \ldots p^{\left[\frac{m}{2}\right]} = \frac{p^{\left[\frac{m}{2}\right]+1} - p}{p-1}$$

But since $\frac{p^{k+1} - p}{p-1} < p^{2k}$ for $k \geq 1$ and $\frac{p^{k+1} - p}{p-1} < p^{2k+1}$, we have

$$p^m \leq \frac{p^{\left[\frac{m}{2}\right]+1} - p}{p-1} < p^m$$

and this is a contradiction.

COROLLARY 2.5. In $GF(p^n)$, for every m divides n, and p divides $\frac{n}{m}$, there exists a fundamental set with index m and coefficient $a = 1$.

3. THE TOTAL NUMBER OF FUNDAMENTAL CLASSES IN SOME FINITE FIELDS.

In this section we will investigate the total number of fundamental classes for some special finite fields. From the previous study we conclude that if $p|\frac{n}{m}$, there exists a fundamental set with index m and coefficient 1 in $GF(p^n)$.

In $GF(p^n)$, for every m divides n, and every $a \in Z_p^*$, $a \neq 1$ where $a^{\frac{n}{m}} = 1$ there exists a fundamental set with index m and coefficient a. Since $a^{\frac{n}{m}} = 1$ then the $g \cdot c \cdot d(\frac{n}{m}, p-1) \neq 1$.

If A is a fundamental set with index m then $\bar{A}$ has $p(p-1)m$ elements.

In this section we will use the following notations:

(a) $0(p^n)$ = Number of fundamental classes in $GF(p^n)$.

(b) $\Delta(p^n)$ = Number of fundamental classes in $GF(p^n)$ but not in any proper subfield of $GF(p^n)$.

(c) $\lambda(p^n,m,a)$ = Number of elements in $GF(p^n)$ with index m and coefficient a and none of these elements belonging to any proper subfield of $GF(p^n)$.

(d) $E(m,a) = \{x^{p^m} = ax + \delta;\ \delta \in Z_p,\ a \in Z_p^*$ and $\delta \neq 0$ if $a = 1\}$.

(e) $SE(m,a,n)$ is the set of all solutions of the equations of $E(m,a)$ in $GF(p^n)$ but not in Z_p.

We shall investigate in the following the number of fundamental classes in $GF(p^{q^\ell})$, where $q \mid p-1$, and $q \neq p$.

LEMMA 3.1. If $q \mid p-1$, then q^{t+1} divides $p^{q^t[q-1]} - 1$ for every $t = 0,1,2, \ldots$.

PROOF. We will prove this lemma by induction. By Fermat Theorem the lemma is true for $t = 0$. Assume it is true for $t = s$ then

$$\left[p^{q^{s+1}[q-1]} - 1\right] = \left[\left(p^{q^s[q-1]}\right)^{q^s} - 1\right]$$

$$= \left(p^{q^s[q-1]} - 1\right)\left[\left(p^{q^s[q-1]}\right)^{q^s-1} + \left(p^{q^s[q-1]}\right)^{q^s-2} + \ldots + 1\right]$$

$$\left[p^{q^s[q-1]} - 1\right]\left[\sum_{j=1}^{q^s}\left(p^{q^s[q-1]}\right)^{q^s-j}\right].$$

Since $p^{q^s[q-1]} \equiv 1 \bmod q$, then $\left(p^{q^s[q-1]}\right)^{q^s-j} \equiv 1 \pmod q$ for every $j = 0,1,\ldots,q^s$.

So, $\sum_{j=1}^{q^s}\left(p^{q^s[q-1]}\right)^{q^s-j} \equiv q^s \pmod q \equiv 0 \pmod q$ which implies q^{s+2} divides $[p^{q^{s+1}[q-1]} - 1]$.

LEMMA 3.2. In $GF(p^{q^{t+1}})$ where $q \mid p-1$ and $q \neq p$, we have

$$\Delta(p^{t+1}) = \frac{p^{q^t[p^{q^t[q-1]}-1]}}{p(p-1)q^{t+1}}.$$

PROOF. Since $g \cdot c \cdot d(q,p-1) = 1$, then for every $a \in Z_p^*$, where $a \neq 1$, $a^{q^s} \neq 1$ for every $s \geq 0$, therefore equation (2.6) and equation (2.7) have no solutions in $GF(p^{q^{t+1}})$ for every $m = q^h$; $h \geq 0$. Hence every element in $GF(p^{q^{t+1}})$ but not in $GF(p^{q^t})$ has index q^{t+1} which implies that every fundamental set in $GF(p^{q^{t+1}})$ but not in $GF(p^{q^t})$ also has index q^{t+1}. So:

$$\Delta(p^{t+1}) = \frac{p^{q^{t+1}} - p^{q^t}}{p(p-1)q^{t+1}} = \frac{p^{q^t[p^{q^t[q-1]}-1]}}{p(p-1)q^{t+1}}$$

From Lemma 3.1 and $g \cdot c \cdot d(p-1,q) = 1$ we have $\Delta(p^{t+1})$ is an integer.

COROLLARY 3.1 In $GF(p^q)$ where $g \mid p-1$, $q \neq p$ we have:

$$0(p^q) = 1 + \frac{p^q - p}{p(p-1)q} = 1 + \frac{p(p^{q-1}-1)}{p(p-1)q} \quad . \tag{3.1}$$

Since $O(p^{q^{t+1}}) = O(p^{q^t}) + \Delta(p^{q^{t+1}})$ we conclude that:

$$O(p^{q^\ell}) = 1 + \sum_{t=0}^{\ell-1} \Delta(p^{q^{t+1}})$$

$$= 1 + \sum_{t=0}^{\ell-1} \frac{p^{q^t}[p^{q^t}[q-1] - 1]}{p(p-1)q^{t+1}}$$

where $q \nmid p-1$, $q \neq p$.

We shall now study the number of fundamental classes in $GF(p^{p^s})$.

By Theorem 2.7, Theorem 2.8 and Theorem 2.9, the equation

$$x^{p^{p^t}} = x + b \tag{3.2}$$

where $b \in Z_p^*$ and $t < s$ has p^{p^t} solutions and all solutions are included in $GF(p^{p^{t+1}})$.

LEMMA 3.3. All the solutions of (3.2) have an index p^t.

PROOF. Let α be a solution of (3.2) and has index m. We have $m = p^k$ for some $k < t$ and $\alpha^{p^{p^k}} = \alpha + c$ for some $c \in Z_p$ which implies $\alpha^{p^{p^t}} = \alpha + 0 = \alpha$. Therefore α is not a solution of (3.2).

COROLLARY 3.2. In $GF(p^{p^{t+1}})$ but not in $GF(p^{p^t})$, there are $(p-1)p^{p^t}$ elements with index p^{p^t}. So $\lambda(p^{p^{t+1}}, p^t, 1) = (p-1)p^{p^t}$.

PROOF. For a fixed $b \in Z_p^*$ equation (3.2) has p^{p^t} solutions and we have $(p-1)$ elements in Z_p^*.

COROLLARY 3.3. If $\alpha \in GF(p^{p^{t+1}})$ but $\alpha \notin GF(p^t)$ then α has index p^{t+1} or p^t, where $t \geq 1$.

COROLLARY 3.4. For $t \geq 1$;

$$\Delta(p^{p^{t+1}}) = \frac{(p-1)p^{p^t}}{p(p-1)p^t} + \frac{p^{p^{t+1}} - p^{p^t} - (p-1)p^{p^t}}{p(p-1)p^{t+1}}$$

$$= \frac{p^{p^t}}{p^{t+1}} + p^{p^t - t - 1}\left[\frac{p^{p^t}(p-1) - 1 - 1}{(p-1)}\right]$$

$$= p^{p^t - t - 1}\left[\frac{p^{p^t}(p-1) - 1 - 1}{(p-1)} + 1\right]. \tag{3.3}$$

In $GF(p^p)$, the equation $x^p = x + b$ (3.4)

where $b \in Z_p^*$ has p solutions and each solution has index p. Therefore there are $p(p-1)$ elements in $GF(p^p) - Z_p$ with index p. This implies:

LEMMA 3.4.
$$O(p^p) = 1 + \frac{p(p-1)}{p(p-1)} + \frac{p^p - p(p-1) - p}{p(p-1)p}$$

$$= 2 + \frac{p^{p-2} - 1}{p-1} \tag{3.5}$$

COROLLARY 3.5.
$$O(p^{p^s}) = 2 + \frac{p^{p-2}-1}{p-1} + \sum_{t=1}^{s-1} \Delta(p^{p^{t+1}}) \tag{3.6}$$

In what follows we will study the number of fundamental classes in $GF(p^{p^s \cdot q^\ell})$ where $q \nmid p-1$, $q \neq p$ and $s, \ell \geq 1$.

Since $q \nmid p-1$ then for every m divides $p^s \cdot q^\ell$ and every $a \in Z_p^*$ with $a \neq 1$, we have $a^{\frac{p^s \cdot q^\ell}{m}} \neq 1$. So, Theorem 1.3 implies that $SE(m, a, p^s q^\ell) = \phi$ for every $a \neq 1$ and every $m \mid p^s \cdot q^\ell$.

By Theorem 2.7, Theorem 2.8 and Theorem 2.9, we conclude the following:

LEMMA 3.5. For every t and h; $0 \leq t \leq s-1$, $0 \leq h \leq \ell$, $SE(p^t q^h, 1, p^s q^\ell)$ has $(p-1)p^{p^t \cdot q^h}$ elements, all of them are contained in the minimum subfield $GF(p^{p^{t+1} q^h})$ and $SE(p^t q^h, 1, p^s q^\ell) \cap GF(p^{p^t \cdot q^h}) = \phi$.

LEMMA 3.6. For every t, h such that $0 \leq t \leq s-1$, $0 \leq h \leq \ell - 1$, $SE(p^t q^h, 1, p^s q^\ell)$ is included in $SE(p^t q^{h+1}, 1, p^s q^\ell)$.

PROOF. Let $\alpha \in SE(p^t q^h, 1, p^s q^\ell)$. Then $\alpha^{p^{p^t q^h}} = \alpha + \delta$ for some $\delta \in Z_p^*$, which implies $\alpha^{p^{p^t \cdot q^h + 1}} = \alpha + [q \cdot \delta]$, where $[x]$ is the least nonnegative residue of x mod p. Since $[q \cdot \delta] \neq 0$ then $\alpha \in SE(p^t \cdot q^{h+1}, 1, p^s q^\ell)$.

It is clear that if $\alpha \in SE(p^t q^h, 1, p^s q^\ell)$, then α has an index $p^t \cdot q^r$ for some $0 \leq r \leq h$. Since, $SE(p^t, 1, p^s q^\ell) \subset SE(p^t q, 1, p^s q^\ell) \subset \ldots \subset SE(p^t q^{h+1}, 1, p^s q^\ell)$ we conclude that

$$\lambda(p^{p^{t+1} \cdot q^{h+1}}, p^t q^{h+1}, 1) = (p-1)p^{p^t \cdot q^{h+1}} - (p-1)p^{p^t \cdot q^h}$$
$$= (p-1)p^{p^t \cdot q^h}\left[p^{p^t \cdot q^h [q-1]} - 1\right]. \tag{3.7}$$

Therefore, in $GF(p^{p^{t+1} q^{h+1}})$ there are

$$\frac{(p-1)p^{p^t \cdot q^h}[p^{p^t \cdot q^h [q-1]} - 1]}{p(p-1)p^{t \cdot q^{h+1}}} = \frac{p^{p^t \cdot q^h}[p^{p^t \cdot q^h [q-1]} - 1]}{p^{t+1} \cdot q^{h+1}} \tag{3.8}$$

fundamental classes with index $p^t \cdot q^{h+1}$. From Lemma 3.1 and the fact that $p^t \geq t+1$, the number given in (3.8) is an integer.

Since any proper subfield of $GF(p^{p^{t+1} \cdot q^{h+1}})$ is a subfield of $GF(p^{p^t \cdot q^{h+1}})$ or $GF(p^{p^{t+1} \cdot q^h})$. So, in $GF(p^{p^{t+1} \cdot q^{h+1}})$, the number of fundamental classes with index $p^{t+1} \cdot q^{h+1}$ is equal to

$$\frac{p^{p^{t+1} \cdot q^{h+1}} - p^{p^t \cdot q^{h+1}} - p^{p^{t+1} \cdot q^h} + p^{p^t \cdot q^h} - (p-1)p^{p^t \cdot q^h}[p^{p^t \cdot q^h [q-1]} - 1]}{p(p-1)p^{t+1} \cdot q^{h+1}}$$
$$= \frac{p^{p^{t+1} \cdot q^h}[p^{p^{t+1} \cdot q^h [q-1]} - 1] - p^{p^t \cdot q^h}[p^{p^t \cdot q^h [q-1]} - 1] \cdot p}{p(p-1)p^{t+1} \cdot q^{h+1}} \tag{3.9}$$

Therefore, we have the following

THEOREM 3.11. In $GF(p^{p^s \cdot q^\ell})$,

$$\Delta(p^{p^{t+1} \cdot q^{n+1}}) = (3.8) + (3.9).$$

From it follows that

$$O(p^{p^{t+1} \cdot q^{h+1}}) = \Delta(p^{p^{t+1} \cdot q^{h+1}}) + O(p^{p^{t+1} \cdot q^{h}}) + O(p^{p^{t} \cdot q^{h+1}}) - O(p^{p^{t} \cdot q^{h}}) . \tag{3.10}$$

We now study the general case, i.e. the number of fundamental classes in $GF(p^n)$. First, let $n = q_1^{\ell_1} \cdot q_2^{\ell_2} \dots q_r^{\ell_r}$ such that $\ell_i \neq 0$ $g_i \nmid p-1$ and $q_i \neq p$ for every $i = 1,2,\dots,r$.

Let $N(s,p)$ be the number of elements in $GF(p^s)$ but not in any proper subfield of $GF(p^s)$.

THEOREM 3.12. The number $N(s,p) = \sum_{i \cdot j = s} \mu(i) q^j$ where μ is the Möbius functions. (See [2]).

Since for every m divides n and every $a \in Z_p^*$, the set $SE(m,a,n) = \phi$. It implies that if $\alpha \in GF(p^k)$ where $GF(p^k)$ is a subfield of $GF(p^n)$ and α doesn't belong to any proper subfield of $GF(p^k)$, then α has an index p^k. So, we have the following

THEOREM 3.13. If $GF(p^k) \subseteq GF(p^n)$ then $\Delta(p^k) = \dfrac{N(k,p)}{p(p-1)p^k}$.

Now let $n = p^k q_1^{\ell_1} \cdot q_2^{\ell_2} \cdot \dots q_s^{\ell_s}$ such that $k \neq 0$, $q_i \neq p$, $\ell_i \neq 0$ and $q_i \nmid p-1$ for every $i = 1,2,\dots,s$.

LEMMA 3.7. For every $m = p^t \cdot q_1^{t_1} \cdot q_2^{t_2} \cdot \dots \cdot q_s^{t_s}$ where $0 \leq t \leq k-1$, $0 \leq t_i \leq \ell_i$, $i = 1,2,\dots,s$ then $SE(m,1,n)$ has $(p-1)p^m$ elements, all of them are contained in the minimum subfield $GF(p^{pm})$ and $SE(m,1,n) \cap GF(p^m) = \phi$.

Since $SE(m,1,n) \subset GF(p^{pm})$, we have $SE(m,1,n) = SE(m,1,pm)$.

LEMMA 3.8. For every $m = p^t \cdot q_1^{t_1} \cdot \dots \cdot q_s^{t_s}$ where $0 \leq t \leq k-1$, $0 \leq t_i \leq \ell_i$ for $i = 1,2,\dots,s$ and for some t_r; $t_r \leq \ell_r - 1$, $SE(m,1,n)$ is a proper subset of $SE(mq_r,1,n)$.

LEMMA 3.9. If p^k divides m, and m divides n then $SE(m,1,n) = \phi$.

COROLLARY 3.6. If $SE(mq_{r_1},1,n) \neq \phi$ and $SE(mq_{r_2},1;n) \neq \phi$ for some $r_1 \neq r_2$ then $SE(mq_{r_1},1,n) \neq SE(mq_{r_2},1,n)$.

The proof is an immediate application of Lemma 3.7.

COROLLARY 3.7. If p^t divides m but not r, then $SE(m,1,n) \cap SE(r,1,n) = \phi$.

The proof is a direct application of Lemma 3.7.

COROLLARY 3.8. If for some $0 \leq t \leq k-1$ $p^t \mid m$ and $p^t \mid r$ but $p^{t+1} \nmid m$ and $p^{t+1} \nmid r$ then

$$SE(m,1,n) \cap SE(r,1,n) = SE((m,r),1,n)$$

where $(m,r) = g \cdot c \cdot d(m,r)$.

The proof is a direct application of Lemma 3.7, Corollary 3.6 and

Corollary 3.8.

We know from Theorem 2.10 if m divides n and $SE(m,1,n) \neq \phi$ then there is an $\alpha \in SE(m,1,n)$ such that α has an index m. We want to find the number of elements in $SE(m,1,n)$ with index m. Let $m = p^t \cdot q_{l_1}^{t_{l_1}} \cdot q_{l_2}^{t_{l_2}} \cdot \ldots \cdot q_{l_h}^{t_{l_h}}$ and m divides n where $0 \leq t \leq k-1$, $t_{l_r} \neq 0$ for $r = 1,\ldots,h$ and $h < s$. If we rearrange the q's in the factorization of n such that $q_{l_r} = q_r$ for $r = 1,2,\ldots,h$, then $SE(\frac{m}{q_i},1,n) \subset SE(m,1,n)$ for every $i = 1,2,\ldots,h$, and $\bigcap_{i=1}^{h} SE(\frac{m}{q_i},1,n) = SE(\frac{m}{q_1 q_2 \cdots q_h}, 1, n)$.

We shall use the following notations for the remaining of this section:

$$m = p^t \cdot q_1^{t_1} \cdot q_2^{t_2} \cdot \ldots \cdot q_h^{t_h} \; ; \quad 1 \leq t_i$$

and

$$m_1 = \sum_{i=1}^{h} \frac{m}{q_i} \qquad m_2 = \sum_{\substack{i,j=1 \\ i<j}}^{h} \frac{m}{q_i q_j}$$

$$m_r = \sum_{i_j=1}^{h} \frac{m}{q_{i_1} \cdot q_{i_2} \cdot \ldots \cdot q_{i_r}} \qquad 1 \leq i_1 < i_2 < \ldots < i_r \leq h \; , \quad \text{and}$$

$$\prod_{j=1}^{r} q_{i_j} \neq \prod_{j=1}^{r} q_{\ell_i} \quad \text{for} \quad i \neq \ell \; .$$

If $r > h$ then we define $m_r = 0$. Therefore $m_h = p^t \cdot q_1^{t_1-1} \cdot q_2^{t_2-1} \cdot \ldots \cdot q_h^{t_h-1}$. From previous Lemmas, we conclude the following.

If $R[SE(m,1,n)]$ is the number of elements in $SE(m,1,n)$ with index m then

$$R[SE(m,1,n)] = m - m_1 + m_2 - m_3 + \ldots + (-1)^r m_r + \ldots + (-1)^h m_h \; . \tag{3.11}$$

Also, if $\beta \in GF(p^{pm})$ and not in any proper subfield of $GF(p^{pm})$, then β has index m or pm. Hence we have the following.

THEOREM 3.14.

$$\Delta(p^{pm}) = \frac{R[SE(m,1,pm)]}{p(p-1)m} - \frac{N(pm,p)-R[SE(m,1,pm)]}{p(p-1)pm} \; . \tag{3.12}$$

To determine the number of equivalence classes in $GF(p^{q^s})$ where $q|p-1$, we need to study $SE(m,a,q^s)$ for all m dividing q^s and $a \in Z_p^*$. From Theorem 2.7 we have $SE(M,1,q^s) = \phi$ for every $m|q^s$. Also we know that for every $m|q^s$ and every $a \neq 1$, $a \in Z_p^*$ if $a^{q^s/m} = 1$ then $SE(m,a,q^s)$ has $P(p^m-1)$ elements. One question we will try to answer first is that for given m, is there an $a \in Z_p^*$, $a \neq 1$ such that $a^{q^s/m} = 1$ and then how many such a's in Z_p^* can one find? Another question is for fixed m and a, how many m''s, a''s are there such that $SE(m',a',q^s) \subset E(m,a,q^s)$.

LEMMA 3.10. In Z_p, if q^v divides $(p-1)$ then there are $q^{v-1}(q-1)$ elements of order q^v.

PROOF. Let b be primitive element in Z_p. Assume for some k; $1 \leq k \leq p-1$, b^k is a solution $x^q = 1$. This implies $k \cdot q \equiv 0 \bmod(p-1)$. So, $k = t \cdot \frac{p-1}{q}$ for some

$t = 1,2,\ldots,q-1$. But also if $r = \ell\frac{p-1}{q}$ for every $\ell = 1,2,\ldots,q-1$ we have $(b^r)^q = b^{\ell(p-1)} = 1$ and $b^r \neq 1$ which implies that in Z_p we have $(q-1)$ elements of order q. Let $p - 1 = q^{\ell} \cdot h$ where the $g \cdot c \cdot d(p-1,h) = 1$, then for every r such that $r \equiv 0 \bmod(q^{\ell-v}\cdot h)$ and $0 \leq r < q^v$ we have b^r is a solution of $x^{q^v} = 1$, which implies that in Z_p, there are q^v-1 elements such that $x^{q^v} = 1$ and $x \neq 1$. For $v = 1$, $v = 2$ we will have $q^2 - 1 - (q-1) = q(q-1)$ elements of order q^2. The same for $v = t - 1$, $v = t$ we will have $q^t - 1 - (q^{t-1}-1) = q^{t-1}(q-1)$ elements of order q^t.

LEMMA 3.11. In Z_p, if for a fixed b where $O(b) = q^{\mu}$ and $1 \leq \mu < \ell$ there exists an a of order q^v where $\ell \geq v > \mu$ and a satisfies

$$x^{q^{v-\mu}} = b \tag{3.13}$$

then there are $q^{v-\mu}$ distinct elements in Z_p^* of order q^v satisfying (3.13)

PROOF. Note that equation (3.13) has no repeated roots. If a is a solution, we claim that $a, a^{q^{\mu}+1}, a^{2q^{\mu}+1}, \ldots, a^{(q^{v-\mu}-1)\cdot q^{\mu}-1}$ are distinct solutions of (3.13). To prove our claim, first since $O(a) = q^v$ then $a^{r_i q^{\mu}+1}$ for $r_i = 1,2,\ldots,q^{v-\mu}-1$ are distinct elements in Z_p. Also $(a^{r^{q^{\mu}}+1})^{q^{v-\mu}} = a^{r\cdot q^v} \cdot a^{q^{v-\mu}} = 1 \cdot b = b$. Since $g \cdot c \cdot d(rq^{\mu}+1,q) = 1$ and $O(a) = q^v$, we have $O(a^{rq^{\mu}+1}) = q^v$.

THEOREM 3.15. If $b \in Z_p$ such that $O(b) = q^{\mu}$; $0 < \mu < \ell$, then for every v, $\ell \geq v > \mu$, there are $q^{v-\mu}$ elements of order q^v and satisfying (3.13).

PROOF. In Z_p we have $q^{v-1}(q-1)$ elements of order q^v. Let $c \in Z_p$ and $O(c) = q^v$ and let $c^{q^{v-\mu}} = d$ so $d \neq 1$ and $d^{q^{\mu}} = 1$. Furthermore, the order of d is q^{μ}. By Lemma 3.11, we have $q^{v-\mu}$ elements satisfying $x^{q^{v-\mu}} = d$ for each d. But there are $\frac{q^{v-1}(q-1)}{q^{n-\mu}} = q^{\mu-1}(q-1)$ distinct d's of order q^{μ} for which the above equation is solvable and that is exactly the total number of elements in Z_p having order q^{μ}.

LEMMA 3.12. If q divides $p-1$, then q^t divides $p^{q^t}-1$ for every $t > 0$.

PROOF. By induction.

In $GF(p^q)$ where q divides $p-1$, the set $SE(1,a,q) \neq \phi$ if and only if $O(a) = q$. Since there are $(q-1)$ elements of order q and for a fixed b with $O(b) = q$, the set $SE(1,b,q)$ has $p(p-1)$ elements, therefore $GF(p^q)$ has $\frac{p(p-1)(q-1)}{p(p-1)} = (q-1)$ fundamental classes with index 1. So we conclude:

$$\begin{aligned} O(p^q) &= (q-1) + \frac{p^q-p-p(p-1)(q-1)}{p(p-1)\cdot q} + 1 \\ &= (q-1) + \frac{(p^{q-1}-1) + (p-1)}{(p-1)q} \\ &= (q-1) + \frac{p^{q-2}+p^{q-3}+\ldots+1+1}{q} \end{aligned} \tag{3.14}$$

Since $P \equiv 1 \bmod q$.

$$1 + \sum_{r=2}^{q} p^{q-r} \equiv 1 + (q-1) \bmod q \equiv 0 \bmod q.$$

So, (3.14) is an integer.

THEOREM 3.16. In $GF(p^{q^s})$ where q divides $(p-1)$, if $O(a) = q^v$, then for every t, where $0 \leq t \leq s - v$ we have $SE(q^t,a,q^s) = SE(q^t,a,q^{t+v}) \neq \phi$ and $SE(q^t,a,q^{v+t}) \cap SE(q^t,a,q^{v+t=1}) = \phi$.

PROOF. By Corollary 2.1 we have

$$SE\left(q^t,a,q^s\right) = SE\left(q^t,a,q^{v+t}\right)^{q^t} \neq \phi .$$

Theorem 2.4 and Corollary 2.2 will imply that $X^{p^{q^t}} = aX + b$; $b \in Z_p$ has a solution α_0 with index $m = q^t$ and $\alpha_0 \notin GF(p^{q^{t+v-1}})$. By Theorem 2.1 the solution set of this equation is $H = \{\alpha_0 \cdot \beta + \frac{b}{1-a} \; / \; \beta \in GF(p^{q^t})\}$ and it is clear that $H \cap GF(p^{q^{t+v-1}}) = \left\{\frac{b}{1-a}\right\}$.

NOTE: This theorem is not true in general. It is possible that in some cases the minimum subfield that contains all the solutions of $x^{p^m} = ax + \delta$ has a proper subfield which contains some of these solutions.

From Theorem 3.16 we conclude that in $GF(p^{q^s})$, where $q \nmid p-1$, $SE(q^{t'},b,q^s)$ is a subset of $SE(q^t,a,q^s)$ if and only if $t' + v' = t + v$ and $b^{q^{t-t'}} = a$, where $O(b) = q^{v'}$, $O(a) = q^v$, $t' \leq t \leq s-v$. Also for a fixed $a \in Z_p^*$ with order q^v where $v > 0$, Theorem 3.15 insures the existence of exactly q elements "b" in Z_p such that $O(b) = q^{v+1}$ and $b^q = a$. Hence, for a fixed a with order q^v and fixed t; $t \leq s-v$ there are q elements b in Z_p such that:

$$SE(q^{t-1},b,q^s) \subset SE(q^t,a,q^s).$$

Therefore, if we start with $a_0 \in Z_p^*$ such that $O(a_0) = q^v$, then there are $a_1, \ldots, a_n \in Z_p^*$ where $O(a_i) = q^{v+i}$ and $(a_{i+1})^q = a_i$. So, we have $SE(q^{t-(i+1)}, a_{i+1}, q^s) \subset SE(q^{t-i},a_i,q^s)$ for every $i = 0,1,2,\ldots,n-1$ where $t - n \geq 0$ and $q^{v+n} \mid (p-1)$.

Let $p - 1 = q^{\ell} \cdot h$ where $g \cdot c \cdot d(h,q) = 1$. Then for every $a \in Z_p^*$, $a \neq 1$ and every $t \geq 1$ such that $O(a) = q^v$, $1 \leq v < \ell$ and $t + v \leq s$ we have the following Lemma.

LEMMA 3.13. In $SE(q^t,a,q^s)$, there are exactly $(p^{q^t}-1)p-(p^{q^{t-1}}-1)p \cdot g$ elements with index q^t and coefficient a.

From this lemma, we conclude that in $GF(p^{q^{t+v}})$ there are

$$\frac{(p^{q^t}-1)-(p^{q^{t-1}}-1) \cdot q}{(p-1) \cdot q^t} \cdot q^{v-1}(q-1) \tag{3.15}$$

fundamental classes and each class has an index q^t and a coefficient with order q^v. Lemma 3.12 insures that (3.15) has an integer value. We will use the notation:

$$\Gamma(m,t,v) = (3.15), \text{ where } m = t + v,\ 1 \leq v < \ell \text{ and } t \geq 1 .$$

It is clear now that in $GF(p^{q^s})$ where $s \geq 1$, we have

$$\frac{(p^{q^s}-p^{q^{s-1}})-p(p^{q^{s-1}}-1)(q-1)}{p(p-1)q^s} \tag{3.16}$$

fundamental classes and each class has index q^s with coefficient 1.

Therefore, for $s \geq 2$, $\ell \geq 2$ we conclude that:

$$O(q^s) = O(q^{s-1}) + (3.16) + \sum_{v=1}^{s-\delta-1} \Gamma(s,s-v,v) + \frac{p(p^{q^\delta}-1)q^{s-\delta-1}(q-1)}{p(p-1)q^\delta} \tag{3.17}$$

where $s - \delta - 1 = \min\{\ell-1, s-1\}$ and $\delta = \max\{0, s-\ell\}$.

If $\ell = 1$ then we have:

$$O(q^s) = O(q^{s-1}) + (3.16) + \frac{p(p^{q^{s-1}}-1)(q-1)}{p(p-1)q^{s-1}} \quad . \tag{3.18}$$

REFERENCES

1. LIANG, Joseph J., On the solutions of trinomial equations over a Finite Field. Bull. Calcutta Math. Soc. 70(1978), no. 6, pp. 379-382.
2. LONG, Andrew F., Factorization of irreducible Polynomials over a Finite Field with the substitution X^q-X for X. Acta Arith. XXV 1973, pp. 65-80.
3. ALBERT, A.A., Fundamental Concepts of Higher Algebra. Phoenix Science Series, The University of Chicago Press, 1956.
4. ALAHEN, J.D. and KNUTH, Donald E., Tables of Finite Fields. Sankhya, The Indian Journal of Statistics, Series A, Vol. 26, Dec. 1964, Part 4, pp. 305-328.