FINITE FIELDS

Sidhart Krishnan
Euler Circle
sidhartkrishnan@gmail.com

May 6, 2020

ABSTRACT

In this paper, I explore finite fields which are fields with a finite number of elements. There are many basic properties of these finite fields and perhaps one of the most important properties is that the order of each of them is of the form p^n where p is a prime and n is an integer. Ultimately, we prove that for each p and n there is exactly one finite field with order p^n up to isomorphism.
This theorem allows us prove that $(\mod p^n)$ there are generators of $\mathbb{F})p^{n\times}$ to look a little bit deeper at roots of unity $(\mod p)$. We are able to derive formulas to characterize how many roots of unity there are and what the roots of unity look like.
Then we introduce the Frobenius map and derive many applications of that map on the fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_p[x]/(f)$ where f is some degree n polynomial.
After establishing the Frobenius map then we determine a condition necessary for $\mathbb{F}_{p^m}$ to be contained in $\mathbb{F}_{p^n}$. The second theorem that we prove using Frobenius maps relates to the number of irreducible monic polynomials of degree n over a field $\mathbb{F}_{p^m}$.

***K*eywords** Finite Fields

1 Classification of Finite Fields

We can start off with a few defintions. We already know that a field is defined as basically an abelian group with an extra operation $\cdot$ where $F^\times$ is an abelian group under this multiplication. The final property they have to satisfy is the distributive property that $a(b+c) = ab + ac$.

Definition 1.1. The definition of a finite field is simply a field where the underlying set is finite.

Most fields that one thinks of are infinite $(\mathbb{Q}, \mathbb{Q}[x], \mathbb{R})$. However, one clear set of finite fields are $\mathbb{F}_p$ which is essentially $\mathbb{Z}/p\mathbb{Z}$ with the standard multiplication operation.

Definition 1.2. The characteristic of a field K is the minimal n such that $n := \underbrace{1+1+1+\cdots+1}_{n \text{ times}} = 0$. It is denoted as $\text{char}(K)$. Note that if no such n exists then $\text{char}(K) = 0$.

Proposition 1.3. *The characteristic of a finite field is nonzero.*

Proof. For any finite field K we see that if we consider $1, 1+1, 1+1+1, \ldots$ then since K is finite, there must be two terms of the sequence that are equal by Pigeonhole Principle. If $\underbrace{1+1+1+\cdots+1}_{a \text{ times}} = \underbrace{1+1+1+\cdots+1}_{b \text{ times}} = x$. Then consider $\underbrace{1+1+1+\cdots+1}_{(a-b) \text{ times}} = x - x = 0$. This means that $0 < \text{char}(K) \leq a - b$. ■

Proposition 1.4. *The characteristic of any field is* 0 *or a prime.*

Proof. First note that since $1 \neq 0$ then $\text{char}(K) \neq 1$. Thus, if $\text{char}(K) > 0$, then we will show that $\text{char}(K)$ is prime. Assume that $\text{char}(K) = ab$ where $a, b > 1$. Then notice that by the distributive property,

$$\underbrace{1+1+1+\cdots+1}_{ab \text{ times}} = \left(\underbrace{1+1+1+\cdots+1}_{a \text{ times}}\right)\left(\underbrace{1+1+1+\cdots+1}_{b \text{ times}}\right) = 0.$$

Then note that if $xy = 0$ for $x, y \in K$ then if $x \neq 0$ we can multiply by x^{-1} on both sides to get that $y = 0$. This means that one of $\underbrace{1+1+1+\cdots+1}_{a \text{ times}}, \underbrace{1+1+1+\cdots+1}_{b \text{ times}}$ is 0. However $a < \text{char}(K)$ which means that $\text{char}(K)$ is not minimal. Thus $\text{char}(K)$ is either 0 or a prime. ■

This means that the characteristic of a finite field is always a prime.

Proposition 1.5. *Any field with a prime characteristic p has $\mathbb{F}_p$ as a subfield.*

Proof. Consider the subfield $\{0, 1, 1+1, 1+1+1, \ldots, \underbrace{1+1+1+\cdots+1}_{(p-1) \text{ times}}\}$ The subfield has the same addition and multiplication rules as $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. ■

Lemma 1.6. *Any finite field has a prime power order.*

Proof. Let $\text{char}(K) = p$. Then we know that $\mathbb{F}_p$ is a subfield. Since K is a field extension of $\mathbb{F}_p$ then consider $[K : \mathbb{F}_p] = n$ and a basis for K: $\{e_1, e_2, \ldots, e_n\}$. This means that $K \cong \mathbb{F}_p^n$ since we can map $x = a_1e_1 + a_2e_2 + \cdots + a_ne_n \in K$ to $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_p^n$. Thus, $|K| = |\mathbb{F}_p^n| = p^n$. ■

To build up to a theorem which completely classifies all finite fields, we need to go a little bit more into algebraic closures.

Definition 1.7. A field extension L/F is algebraic if for each $a \in L$, there exists a subfield of L, L_a which contains a so that $[L_a : F]$ is finite.

Proposition 1.8. *Given an algebraic extension K/F then for every $\alpha \in K$, α is algebraic over F meaning that α is the root of a monic polynomial in $F[x]$.*

Proof. Define K_α to be a subfield of K which contains α and is finite over F. Let the $[K_\alpha : F] = n$. Then if we consider $1, \alpha, \alpha^2, \ldots, \alpha^n$ then this set must be linearly dependent. Thus there exists $c_0, c_1, \ldots, c_n$, so that $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$ and then dividing by c_n gives us the monic polynomial that we need. Thus α is algebraic. ■

Definition 1.9. A field F is algebraically closed if the only finite field extension of F is an isomorphism.

Proposition 1.10. *F is algebraically closed if and only if every monic irreducible polynomial over F has degree* 1.

Proof. We will prove the only if first. Assume F is algebraically closed. Then we consider the field $F[x]/(f)$ where f is a monic irreducible polynomial. Define this field $F[x]/(f)$ as $F[x]$ mod the equivalence relation $\sim$ where $g \sim h$ if and only if $f \mid g - h$. This field clearly satisfies the addition and multiplication properties and to find the inverse we see that for any $g \in F[x]$ then we can use the Euclidean Algorithm to find the inverse of g. Note that $F \subseteq F[x]/(f)$ because $F[x]/(f)$ constant all of the constant polynomials. However, since F is algebraically closed then any extension of F, $F \cong F[x]/(f) \longrightarrow \dim_F(F[x]/(f)) = 1$. But also note that if $n = \deg(f)$, then $x^n \equiv g(x) \pmod{f}$ for some polynomial $g(x)$ which degree less than n. Thus, $(1, x, \ldots, x^{n-1})$ is a basis of $F[x]/(f)$ over F. Thus $\deg(f) = \dim_F(F[x]/(f)) = 1$.
Note that because this relation holds then it means that we can factor any polynomial in $F[x]$ into linear factors.

To prove the second part we assume that F is not algebraically closed. Then we can take some finite extension K which is not isomorphic to F. Now we want to show that there exists an irreducible polynomial with degree higher than 1. Take some $y \in K - F$. We are going to find a monic irreducible polynomial in F such that $f(y) = 0$. Because K is a finite extension of F then we know that it is algebraic. This is important because then by Proposition 1.8 then we can construct a minimal polynomial with y as a root. However, because yF, then this polynomial has a to have a degree of more than 1. Thus if F is algebraically closed then every monic irreducible polynomial over F has degree 1. ■

Definition 1.11. A field $\overline{K}$ is the algebraic closure of a field K if $[\overline{K} : K]$ is finite and $\overline{K}$ is algebraically closed.

Note that if L/K is an algebraic extension of K then an algebraic closure $\overline{L}$ of L is also an algebraic closure of K since $[\overline{L} : K] = [\overline{L} : L][L : K]$ is finite.

Theorem 1.12. *Every finite field has order p^n for some prime p and a nonnegative integer n. For each p and n there is a field $\mathbb{F}_{p^n}$ which has order p^n and is unique up to isomorphism.*

Proof. The first part of this theorem is true because of Lemma 1.6.

Now for the second part of the theorem, we first need to consider the algebraic closure of $\mathbb{F}_p$, $\overline{\mathbb{F}}_p$. Then we can define $\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}}_p \mid x^{p^n} - x = 0\}$. Then note that this satisfies all of the properties of a field.
It satisfies the addition property since $x^{p^n} + y^{p^n} \equiv \left(x^{p^{n-1}} + y^{p^{n-1}}\right)^p \equiv \cdots \equiv (x+y)^{p^n} \in \mathbb{F}_{p^n}$.
It satisfies the multiplication property since $x^{p^n} y^{p^n} = (xy)^{p^n} \in \mathbb{F}_{p^n}$.
It satisfies the inverse property since for any nonzero x, $(x^{-1})^{p^n} = \left(x^{p^n}\right)^{-1} = x^{-1} \in \mathbb{F}_{p^n}$.
Finally we inherent the distributive and commutative property from $\overline{\mathbb{F}}_p$. Now we need to prove that $|\mathbb{F}_{p^n}| = p^n$. Consider $f(x) = x^{p^n} - x$. Then since $f(x) \in \overline{\mathbb{F}}_p$ which is algebraically closed then it means that $f(x)$ factors into p^n linear factors. Now we just need to know that none of these linear factors repeat. To show this we take the derivative of $f(x)$ and we get that $f'(x) = p^n x^{p^n-1} - 1$ so for every value of x, $f'(x) = -1 \neq 0$. Thus there are no repeated roots meaning that $|\mathbb{F}_{p^n}| = p^n$.

Now we need to prove that $\mathbb{F}_{p^n}$ is unique up to isomorphism. For this assume that there is another field K which has order p^n. Since K is finite it is thus algebraic over $\mathbb{F}_p$. Thus if we done an algebraic closure of K as $\overline{\mathbb{F}}_p$ then that is also an algebraic closure of $\mathbb{F}_p$. Consider a field homomorphism $\phi : K \to \overline{\mathbb{F}}_p$. It suffices to show that $\operatorname{im}\phi \subseteq F_{p^n} \subseteq \overline{\mathbb{F}}_p$ since ϕ is injective meaning that $|K| \geq p^n$ but also $|K| \leq |F_{p^n}| = p^n$.
Now to show that $\operatorname{im}\phi \subseteq F_{p^n}$. We need to show that for all $x \in K$, $\phi(x)^{p^n} = \phi(x)$ which is essentially showing that $x^{p^n} = x$. This clearly holds for $x = 0$ so we only need to consider $x \in K^\times$. But since $x \neq 0$ then we just need to show that $x^{p^n-1} = 1$. Since $|K^\times| = p^n - 1$, we can use Lagrange's Theorem on $K^\times$ as a group to see that the order of every element in $K^\times$ divides $p^n - 1$. This means that $x^{p^n-1} = 1$ so we are done. ■

2 Roots of Unity $\pmod p$

First we can prove a proposition about $\mathbb{F}_p^\times$.

Proposition 2.1. $\mathbb{F}_{p^n}^\times \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$

Proof. To show that $\mathbb{F}_{p^n}^\times$ is cyclic we need to find an element with order $p^n - 1$.
We know by the Fundamental Theorem of Finite Abelian Groups that $\mathbb{F}_{p^n}^\times \cong \prod_i \mathbb{Z}/p_i^{a_i}\mathbb{Z}$. Note that if each of the p_i's are distinct then we can see that $(1, 1, \ldots, 1)$ would be an element of order $\prod_i p_i^{a_i}$.
Now assume that for $r \neq s, p_r = p_s$ and $a_r \geq a_s$. Then we can essentially say that $\mathbb{F}_{p^n}^\times \cong \prod_{i \neq s} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ since for any $x \in \mathbb{F}_{p^n}^\times$, $x \pmod{p_s^{a_s}}$ is determined by $x \pmod{p_r^{a_r}}$. This means that we can continue to eliminate primes which are equal until we have a set of distinct primes such that $\mathbb{F}_{p^n}^\times \cong \prod_j \mathbb{Z}/p_j^{a_j}\mathbb{Z}$ where the set of j's is a subset of the set of i's. Then we see that $(1, 1, \ldots, 1)$ is an element of maximal order $m = \prod_j p_j^{a_j} < |\mathbb{F}_{p^n}^\times|$. However if such an m existed where $x^m = 1$ for all $x \in \mathbb{F}_{p^n}^\times$, then the polynomial $x^m - 1$ has a maximum of m roots in $\overline{\mathbb{F}}_p$. Thus there is some element of $\mathbb{F}_{p^n}^\times$ which has order $p^n - 1$. Thus $\mathbb{F}_{p^n}^\times$ is cyclic so $\mathbb{F}_{p^n}^\times \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$. ■

From this proposition we can draw the conclusion that there are generators of $\mathbb{F}_{p^n}$. This has a a couple implications.

Corollary 2.2. *The number of n-th roots of unity $\pmod p$ is $\gcd(n, p-1)$. The roots of unity are the solutions to $x^n \equiv 1 \pmod p$.*

Proof. We can see this as if we let g be the generator of $\mathbb{F}_p^\times$. Then we can represent any element of $\mathbb{F}_p^\times$ as $x = g^y$ where y is between 0 and $p - 1$. Then we get that $x^n = g^{ny}$. Thus we know that for $x^n = 1$, $p - 1 \mid ny$. If $d = \gcd(n, p-1)$ then we just need $\frac{p-1}{d} \mid (\frac{n}{d})y$. Since $\gcd(\frac{p-1}{d}, \frac{n}{d}) = 1$, then we see that $\frac{p-1}{d} \mid y$. Thus $y = \frac{(p-1)a}{d}$ where $a \in \mathbb{Z}$. Since $0 \leq y < p - 1$, then we get that $0 \leq a < d$ meaning there are d solutions. ■

This also means that for the polynomial $x^n - 1$ to have n solutions in $\mathbb{F}_p$, $\gcd(n, p-1) = n \implies n \mid p-1$.

The proposition can also be used to prove Wilson's theorem if you let consider $(p-1)! \equiv \prod_{i=0}^{p-2} g^i \pmod{p}$ where g is a generator of $\mathbb{F}_p^\times$. Thus

$$(p-1)! \equiv g^{1+2+\cdots+(p-2)} \equiv g^{(p-2)(p-1)/2} \equiv \left(g^{\frac{p-1}{2}}\right)^{p-2} \equiv (-1)^{p-2} \equiv -1 \pmod{p}$$

3 Frobenius Maps

Before we go into Frobenius Maps we should first establish that $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$. This is because $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ and thus it is normal. It is also separable which means that $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$.
With this we can explore the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Definition 3.1. The Frobenius map is defined as a function $\mathrm{Frob}_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$$\mathrm{Frob}_p(x) = x^p$$

. We can verifty that this map is an isomorphism because

$$\mathrm{Frob}_p(x+y) \equiv (x+y)^p \equiv x^p + y^p \equiv \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y) \pmod{p}$$

$$\mathrm{Frob}_p(xy) \equiv (xy)^p \equiv x^p y^p \equiv \mathrm{Frob}_p(x)\mathrm{Frob}_p(y) \pmod{p}$$

Now we are going to prove the following theorem through various smaller lemmas that explore the Frobenius map.

Theorem 3.2. *First we will define Frob_p^0 as the identity map. We will also define $\mathrm{Frob}_p^a(x) = x^{pa}$.*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{(\mathit{Frob}_p^a \mid a \in \mathbb{Z}, 0 \le a \le n-1\}$$

Proof. Let's explore this theorem. There are some important lemmas that we need to use.

Lemma 3.3. *Any one of these Frobenius maps: Frob_p^a fixes $\mathbb{F}_p$.*

Proof. We first have to consider $\mathrm{Frob}_p(x) = x^p$. By Fermat's Little Theorem, we know that $x^p \equiv x \pmod{p}$. Thus, the Frobenius map fixes $\mathbb{F}_p$.
We can also extend this to say that $x^{pa} \equiv x \pmod{p}$. Thus Frob_p^a fixes $\mathbb{F}_p$. This means that $\mathrm{Frob}_p^a \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. ■

Lemma 3.4. *These Frob_p^a's are distinct as maps $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.*

Proof. We wish to show that $\mathrm{Frob}_p^r \neq \mathrm{Frob}_p^s$ for $0 \le r < s \le n-1$. We can compose Frob_p^s with Frob_p^{-r} to get that Frob_p^{s-r} is not the identity. The restriction on $s-r$ is $0 \le s-r \le n-1$. Thus, if we define $t = s-r$, then it suffices to show that $\mathrm{Frob}_p^t \neq \mathrm{Frob}_p^0$ for $0 \le t \le n-1$.
Thus to show that Frob_p^t is not the identity, then we have to show that there is a $x \in \mathbb{F}_{p^n}$ so that $x^{p^t} \neq x$. This is not hard to show since $x^{p^t} - x$ is a polynomial with degree $p^t \le |\mathbb{F}_{p^n}| = p^n$. Thus, $x^{p^t} - x$ cannot be 0 over all $x \in \mathbb{F}_{p^n}$ so each Frob_p^a is a distinct automorphism that fixes $\mathbb{F}_p$. ■

Lemma 3.5. *We need is that we can express $\mathbb{F}_{p^n}$ in the form $\mathbb{F}_p[x]/(f)$ for $f \in \mathbb{F}_p[x]$ of degree n.*

Proof. We already established through Proposition 2.1 that there is a generator g of $\mathbb{F}_{p^n}^\times$. We also know that by Proposition 1.8, since $\mathbb{F}_{p^n}$ is an algebraic extension of $\mathbb{F}_p$, then g satisfies some irreducible monic polynomial f over $\mathbb{F}_p$. Then we can consider a a map $\phi : \mathbb{F}_p[x]/(f) \to \mathbb{F}_{p^n}$

$$x \mapsto g$$

This map is necessarily injective because it is a field homomorphism. Since g is a generator of $\mathbb{F}_{p^n}^\times$ and $\phi(0) = 0$, then ϕ is also surjective.
Thus ϕ is an isomorphism. It follows that $\deg(f) = n$ because since $[\mathbb{F}_p[x]/(f) : \mathbb{F}_p] = \deg(f)$. Insofar as $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}$ and $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ then we can see that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_p[x]/(f) : \mathbb{F}_p] = n \implies \deg(f) = n$. ■

Finally we can piece all of these lemmas together to prove the theorem. By Lemma 3.3, then all Frob_p^a are in $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Then by Lemma 3.4 we know that each of these $\text{Frob}_p^a, 0 \leq a \leq n-1$ are distinct so we have at least n distinct elements of $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.
Then finally by Lemma 3.5 we have that $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}$. Thus any map $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ will be the same as a map $\mathbb{F}_p[x]/(f) \to \mathbb{F}_{p^n}$. However a map from $\mathbb{F}_p[x]/(f)$ to $\mathbb{F}_{p^n}$ will have to send x to a root of f. Thus, there are at maximum $\deg(f) = n$ possible maps $\mathbb{F}_p[x]/(f) \to \mathbb{F}_{p^n}$. It follows that $\text{Aut}(\mathbb{F}_{p^n}) \leq n$. Since we already have n elements of $\text{Aut}(\mathbb{F}_{p^n}) \leq n$: $\{(\text{Frob}_p^a \mid a \in \mathbb{Z}, 0 \leq a \leq n-1\}$ Thus we are done,

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{(\text{Frob}_p^a \mid a \in \mathbb{Z}, 0 \leq a \leq n-1\}$$

■

4 Two Important Theorems

There are two important conclusions which we can draw from the Frobenius map: Theorem 4.1 and Theorem 4.2.

Theorem 4.1. *For a prime p and $m, n > 0$, we have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$.*

Proof. First we should consider what happens if $m \mid n$. We know that $\mathbb{F}_{p^m}$ is the set of elements of $\overline{\mathbb{F}}_p$ for which $x^{p^m} = x$ and $\mathbb{F}_{p^n}$ is the set of elements of $\overline{\mathbb{F}}_p$ for which $x^{p^n} = x$. If $n = md$, then

$$x^{p^n} = x^{p^{md}} = \left(x^{p^{m(d-1)}}\right)^p = x^{p^{m(d-1)}} = \cdots = x^{p^m} = x$$

Thus if $x \in \mathbb{F}_{p^m}$ then $x \in \mathbb{F}_{p^n}$.

Now if $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^m}$. Let us say that $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = d$. Then

$$|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d \iff p^n = (p^m)^d \implies m \mid d$$

. ■

The proof of the following theorem uses Frobenius Maps ot count the number of irreducible monic polynomials in a finite field $\mathbb{F}_{p^m}$ of a specific degree.

Theorem 4.2. *The number of irreducible monic polynomials of degree n over a field $\mathbb{F}_{p^m}$ represented by N_n is given by the equation*

$$n \cdot N_n = \sum_{d|n} \mu(d) q^{n/d}$$

Where $q = p^m$ and $\mu(n) = \begin{cases} 1 & \text{if } n \text{ is squarefree and has an even number of prime divisors} \\ -1 & \text{if } n \text{ is squarefree and has an odd number of prime divsors} \\ 0 & \text{if } n \text{ has a squared prime factor} \end{cases}$.

Proof. To prove this we should first establish what the Frobenius map looks like over the field $F = \mathbb{F}_q = \mathbb{F}_{p^m}$. Given some finite field extension $K = \mathbb{F}_{q^n}$ then the Frobenius operator can be defined as $\Phi = \text{Frob}_q : K \to K$ where $\Phi(x) = x^q$. It is fairly clear that Φ is a valid isomorphism similar to what we did for the Frob_p operator. It can also be shown that the Φ operator follows all of the lemmas that we established in section 3. Now we will prove the following lemma.

Lemma 4.3. *For $k \in K$, there is exactly one monic irreducible polynomial $p \in F[x]$ which has k as a root and this polynomial is given by*

$$p(x) = (x-k)(x-\Phi(k))(x-\Phi^2(k))\dots(x-\Phi^{d-1}(k))$$

Where $\Phi^c(k) = \underbrace{\Phi \circ \Phi \cdots \circ \Phi}_{c \text{ times}}(k)$ and d is the smallest positive integer such that $\Phi^d(k) = k$.

Proof. First we have to note that by Pigeonhole principle since K is finite, there are some $0 \leq i < j$ so that $\Phi^i(k) = \Phi^j(k)$. Thus we get that $\Phi^{j-i}(k) = k$ meaning that such a d exists which is less than or equal to $j - i$. Now consider $p(x) = (x-k)(x-\Phi(k))(x-\Phi^2(k))\dots(x-\Phi^{d-1}(k))$. We know that $p(x)$ is at least in $K[x]$. But if we take $\Phi(p(x))$ then we see that

$$\Phi(p(x)) = \Phi(x-k)\Phi(x-\Phi(k))\dots\Phi(x-\Phi^{d-1}(k)) = (\Phi(x)-k)(\Phi(x)-\Phi(k)\dots(\Phi(x)-\Phi^{d-1}(k)) = p(\Phi(x))$$

Thus for $x \in F$, $\Phi(p(x)) = p(x)$. However $\Phi(p(x))$ can also be seen as Φ acting on each of the coefficients of p. However, if $\Phi(p(x)) = p(x)$ then that means that each of the coefficients must be in F so $p(x) \in F[x]$. ■

Lemma 4.4. *Let p be an irreducible monic polynomial of degree d with d dividing the degree n of an irreducible polynomial q. Then $p(x)$ has d distinct roots in $F[x]/(q)$.*

Proof. Consider $L = F[x]/(p) \cong \mathbb{F}_{p^{md}}$. Let k be a generator of $\mathbb{F}^{\times}_{p^{md}}$ which is what x maps to in the isomorphism from $F[x]/(p)$ to $\mathbb{F}_{p^{md}}$. We know that $p(k) = 0$ and $p(x) = (x-k)(x-\Phi(k))(x-\Phi^2(k))\dots(x-\Phi^{d-1}(k))$ by Lemma 4.3 where Φ is defined as the Frobenius automorphism of $K = F[x]/(q)$ over F.
By Lagrange's Theorem $k^{q^d-1} = 1 \implies p(x) \mid x^{q^d-1} - 1$. But now we can also consider g to be the generator of $K^{\times} = \mathbb{F}^{\times}_{q^{mn}}$ where $g^{q^n-1} = 1$. Then $\{1, g, g^2, \dots g^{q^n-2}\}$ are all the roots of the polynomial $x^{q^n-1} - 1$. Then we can see that

$$q^d - 1 \mid q^n - 1 \implies x^{q^d-1} - 1 \mid x^{q^n-1} - 1 \implies p(x) \mid x^{q^n-1} - 1$$

Thus, $p(x)$ has d roots in K since $x^{q^n-1} - 1$ factors into linear factors over $K[x]$. ■

Now to finally complete this proof we are going to count $|K| = q^n$. We can group them in d-tuples of roots of elements of irreducible monic polynomials in $F[x]$ where d goes over all positive divisors of n. Then this grouping gives us another way to count $|K|$ as

$$|K| = q^n = \sum_{d|n} d \cdot N_d$$

Then we can use Mobius inversion which is essentially inclusion and exclusion which says that $g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$. Thus applying Mobius inversion where $g(n) = q^n$ and $f(n) = n \cdot N_n$, we get

$$n \cdot N_n = \sum_{d|n} \mu(d) q^{n/d}$$

■

References

[1] Landesman, Aaron. Notes on Finite Fields. Retrieved from https://web.stanford.edu/ aaronlan/assets/finite-fields.pdf.

[2] Conrad, Keith. Finite Fields. Retrieved from https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf.

[3] Proofs about Frobenius. Retrieved from http://www-users.math.umn.edu/ garrett/coding/Overheads/23proofs.pdf.