A Brief Study of Extensions over Finite Fields

– a ‘generalisation’ of Fermat’s little theorem and a quick further exploration

I tried to understand an ‘algebraic’ generalisation of Fermat’s little theorem over all finite fields instead of just $\mathbb{F}_p$ where p is a prime number, and realised it is just “$\mathbb{F}_{p^n}$ is exactly the collection of all $(p^n - 1)$th roots of unity and 0”. Still, just for practice I noted down the process through which I had reached this answer, as well as some quick notes on the Frobenius map.

The Euler direction def worth noting and thinking about

Wilson’s Theorem. *In $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number, $-1 = (p-1)!$.*
Proof. Let a be an integer st. $0 < a < p$. Then $gcd(a, p) = 1$. By Bezout’s theorem, $\exists b, k \in \mathbb{Z}$ st. $ab + kp = 1$. $\therefore \mathbb{Z}_p$ is a field (the checking for other axioms in the definition of a field is omitted here). $\therefore$ All the non-zero elements in $\mathbb{Z}_p$ are units. $\because$ Except ± 1 other elements in $\mathbb{Z}_p$ come in pairs. $\therefore (p-1)! = -1$. □

Lemma 1 *Given $a \in \mathbb{Z}$ st. $0 < a < p$, in $\mathbb{Z}/p\mathbb{Z}$, $\{a, 2a, ..., (p-1)a\}$ is the same set as $\{1, 2, ..., p-1\}$.*
Proof. Suppose not. Then $\exists i, j \in \mathbb{Z}$ st. $i \neq j$ and $ia = ja$. $\therefore (j - i)a = 0$. $\because \mathbb{Z}_p$ is a field thus an *ID* and $a \neq 0$. $\therefore i = j$. Contradiction! □

Fermat’s Little Theorem. *In $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number, $\forall a \in \mathbb{Z}/p\mathbb{Z}$, $a^{p-1} = 1$.*
Proof. By Wilson’s theorem and lemma 1, $-a^{p-1} = (p-1)!a^{p-1} = a \cdot (2a) \cdot ... \cdot ((p-1)a) = -1$. $\therefore a^{p-1} = 1$. □

Definition. In F, a field of positive *char* p, the *Frobenius map of F* $\phi : F \to F$ is defined by $\phi(a) := a^p$.

Lemma 2 *ϕ is injective.*
Proof. If $\alpha, \beta \in F$ st. $\alpha^p = \beta^p$, then $(\alpha - \beta)^p = 0$ by Freshman’s dream. $\because F$ is a field thus *ID*. $\therefore \alpha - \beta = 0$. □
Remark.
If $|F| < \infty$, then ϕ is bijective. Thus all finite fields are perfect. Particularly, $F \cong F^p$ when F is finite.
If $|F| = \infty$, say $F := \mathbb{F}_p(t)$, there is no element $\frac{h(x)}{g(x)} \in \mathbb{F}_p(t)$ $(h(x), g(x) \in \mathbb{F}_p[x])$ st. $\left(\frac{h(x)}{g(x)}\right)^p = t$. Particularly, $\mathbb{F}_p(t) \ncong \mathbb{F}_p(t)$. Therefore, F may not be perfect when it is infinite.

Is none of infinite fields with positive *char* perfect?
One element field?

Lemma 3 *All finite fields have order p^n.*
Proof. A finite field F cannot have 0 *char*, or it would contain an element of infinite order (actually a copy of $\mathbb{Q}$). It cannot have positive *char* of a composite number either, or it would contain zero divisors. $\therefore \mathbb{F}_p \subset F$. $\because$ For any ring $S \subset R$, R is an $S-$module. $\therefore F$ is a vector space over $\mathbb{F}_p$. $\because F$ is finite. $\therefore \exists n < \infty$ st. $[F : \mathbb{F}_p] = n$. $\therefore |F| = p^n$. □

Construction of $\mathbb{F}_{p^n}$
Let $f = x^{p^n} - x \in \mathbb{F}_p[x]$. $\because D(f) = -1 \neq 0$. $\therefore F$ is separable. $\therefore f$ has distinct p^n roots. By quick checking (done by hand), the collection of all the distinct roots of f consists of a field, denote as K. $\because f$ splits over K and is the smallest field we can get over which f splits. $\therefore K = \Sigma_{f/\mathbb{F}_p}$.
Particularly, all units in $\mathbb{F}_{p^n}$ are the $(p^n - 1)$th roots of unity. $(\ast)$

my thoughts on separability, Bezout’s lemma, EA, gcd and ideals

Proposition 4 *All finite fields are isomorphic to $\mathbb{F}_{p^n}$.*
Proof. Let K be a field with order p^n. Every element in K has to be order no greater than $p^n - 1$ due to the order of $K^\times$, the multiplicative group of K. By Lagrange’s theorem, the order of the subgroup generated by an element in $K^\times$ has to divide $p^n - 1$. $\therefore$ for $\forall \alpha \in K^\times$, $\alpha^{p^n - 1} = 1$ and thus α is a root of $x^{p^n - 1} - 1 \in \mathbb{F}_p[x]$. $\therefore K$ is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. By the uniqueness of splitting fields up to isomorphism, hence $K \cong \mathbb{F}_{p^n}$. □

Lemma 1 can be self-evidently generalised to $\mathbb{F}_{p^n}$ following the same proof: let α be a unit in $\mathbb{F}_{p^n}$; then $\alpha\mathbb{F}_{p^n} = \mathbb{F}_{p^n}$ because $\mathbb{F}_{p^n}$ is a field thus *ID*. Lemma 1 is the $n = 1$ specific case for $\ast$ and its proof is spreading out the separability of $x^p - 1$ over $\mathbb{F}_p[x]$. Specifically, $x^p - x = x(x-1)(x-2)...(x-(p-1))$.

$\ast$ itself or equivalently the identity $\phi^n - id_{\mathbb{F}_{p^n}} = 0$ in $\mathbb{F}_{p^n}$ can be viewed as a ‘generalisation’ of Fermat’s little theorem to $\mathbb{F}_{p^n}$ for $n > 1$, while the one in elementary number theory characterises $\mathbb{F}_p$, the prime field of positive *char* fields, among all positive *char* fields.

In $\mathbb{F}_{p^n}, n > 1$, it is easy to see that '$\alpha^p = \alpha$' no longer works for $\forall \alpha \in \mathbb{F}_{p^n}, n > 1$, since $\mathbb{F}_{p^n}[x]$ is an *ED* hence *UFD* and thus $x^p - x$ can only have at most p distinct roots. It is natural to ask "then what happens to $\phi^i - id_{\mathbb{F}_{p^n}}, 1 \le i < n$ in $\mathbb{F}_{p^n}$?" $\phi^i - id_{\mathbb{F}_{p^n}}$ is clearly not a field homomorphism but module one, or in this case equivalently linear map, so at first, I was thinking about viewing $\phi^i - id_{\mathbb{F}_{p^n}}, 1 \le i < n$ as a 'linear operation' that 'neatly peels off the $\mathbb{F}_{p^i}$ part from $\mathbb{F}_{p^n}$' for every $i \le n$ one by one looking at the null space $N(\phi^i - id_{\mathbb{F}_{p^n}}) \coloneqq \{\alpha \in \mathbb{F}_{p^n} | (\phi^i - id_{\mathbb{F}_{p^n}})(\alpha) = 0\}$ (the image is not necessarily a field). Yet my 'intuition' was shown to be wrong during my attempt to prove "$rank(\phi^i - id_{\mathbb{F}_{p^n}}) = n - i, 1 \le i \le n$" in $\mathbb{F}_{p^n}$:

Lemma 5 *Given $n > i$ and $i \nmid n$, $\mathbb{F}_{p^i} \notin \mathbb{F}_{p^n}$.*
Proof. Suppose $\exists$ such n, i and prime number p. Then $[\mathbb{F}_{p^n} : \mathbb{F}_{p^i}] = k$ for some positive integer $k > 1$. $\therefore$ The size of a basis of $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_{p^i}$ is k. $\therefore p^n = |\mathbb{F}_{p^n}| = (p^i)^k = p^{ik}$. Contradiction! □

Lemma 6 *For $1 \le i \le n$, if $i|n$, then $\mathbb{F}_{p^i} \subset \mathbb{F}_{p^n}$.*
Proof. By $\circledast$, $\mathbb{F}_{p^i}$ is the collection of roots of $x^{p^i} - x$. When $i|n$, $x^{p^n} = x^{p^i p^i \cdots p^i}$ for $\frac{n}{i}$ times. Pick an arbitrary $a \in \mathbb{F}_{p^n}$. $\because a = a^{p^i} = a^{p^i p^i} = \cdots = a^{p^i p^i \cdots p^i}$. $\therefore a \in \mathbb{F}_{p^n}$. $\therefore \mathbb{F}_{p^i} \subset \mathbb{F}_{p^n}$. □

Lemma 5 and 6 together characterise all the subfields of $\mathbb{F}_{p^n}$.

Porism 6.1 *For $1 \le i \le n$, if $i|n$, then $N(\phi^i - id_{\mathbb{F}_{p^n}}) = \mathbb{F}_{p^i} \subset \mathbb{F}_{p^n}$.*
By the definition of the null space $N(\phi^i - id_{\mathbb{F}_{p^n}})$ and the proof of lemma 6.

Lemma 7 *If $gcd(i, n) = 1$, then $N(\phi^i - id_{\mathbb{F}_{p^n}}) = N(\phi - id_{\mathbb{F}_{p^n}}) = \mathbb{F}_p$.*
Proof. It is quick to check that $\mathbb{F}_p \subset N(\phi^i - id_{\mathbb{F}_{p^n}})$, so we only need to prove the other direction of of inclusion. For $\forall \alpha \in N(\phi^i - id_{\mathbb{F}_{p^n}})$, by the definition of the null space, $\phi^i(\alpha) = \alpha$. Meanwhile, since $\alpha \in \mathbb{F}_{p^n}$, $\phi^n(\alpha) = \alpha$. By Bezout's lemma, $\exists k, l \in \mathbb{Z}$ st. $ki + ln = 1$. By the remark of lemma 2, ϕ^{-1} is well-defined.
$\therefore \phi(\alpha) = \phi^{ki+ln}(\alpha) = \phi^{ki} \circ \phi^{ln}(\alpha) = id_{\mathbb{F}_{p^n}}(\alpha)$. Thus, $\alpha \in N(\phi - id_{\mathbb{F}_{p^n}})$. □

Lemma 8 *If $gcd(i, n) = d, 1 < d < i$, then $N(\phi^i - id_{\mathbb{F}_{p^n}}) = N(\phi^d - id_{\mathbb{F}_{p^n}})$.*
Proof. The proof is the same as that of lemma 6 and 7.
$\because \forall \alpha \in N(\phi^d - id_{\mathbb{F}_{p^n}}), \phi^i(\alpha) = \phi^d \circ \cdots \circ \phi^d = \alpha$. $\therefore N(\phi^d - id_{\mathbb{F}_{p^n}}) \subset N(\phi^i - id_{\mathbb{F}_{p^n}})$.
For $\forall \alpha \in N(\phi^i - id_{\mathbb{F}_{p^n}})$, by the definition of the null space, $\phi^i(\alpha) = \alpha$. Meanwhile, since $\alpha \in \mathbb{F}_{p^n}$, $\phi^n(\alpha) = \alpha$. By Bezout's lemma, $\exists k, l \in \mathbb{Z}$ st. $k(\frac{i}{d}) + ln = 1$. $\therefore ki + (ld)n = d$. By the remark of lemma 2, ϕ^{-1} is well-defined.
$\therefore \phi^d(\alpha) = \phi^{ki+(ld)n}(\alpha) = \phi^{ki} \circ \phi^{(ld)n}(\alpha) = id_{\mathbb{F}_{p^n}}(\alpha)$. Thus, $N(\phi^i - id_{\mathbb{F}_{p^n}}) \in N(\phi^d - id_{\mathbb{F}_{p^n}})$. □

Proposition 8 *In $\mathbb{F}_{p^n}$, $rank(\phi^i - id_{\mathbb{F}_{p^n}}) = n - d, 1 \le i \le n$ where $gcd(i, n) = d$.*
As a result of porism 6.1, lemma 7 and 8.

In fact, proposition 8 is a specific case of the Galois theory: over $\mathbb{F}_p$, any i-degree finite extension is a splitting field for $x^{p^i} - x$ thus normal and consequently Galois over $\mathbb{F}_p$, so $\mathbb{F}_{p^n}$ can only contain $\mathbb{F}_{p^d}, d = gcd(i, n)$. From the group perspective to explain the 'gaps of layers' that occurs in the chains of field extensions of finite fields, it goes back to using Lagrange theorem to find out all the subgroups of the n–cyclic Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ and thus reduced to study the divisors of n, and the writing is satisfactory. However, if it is possible to use results arising from studying the chains of field extension over finite fields to 'understand' cyclic groups? One of the initial reasons why I studied this small topic of finite fields is to know better "what *symmetry* exactly groups are studying or can study".