Explaining why $x^{p^n} - x$ is the product of all irreducibles of degree dividing n in $\mathbb{F}_p[x]$?

by Some Undergrad

The main point of this short essay is to outline exactly why $x^{p^n} - x$ is the product of all the irreducible polynomials in $\mathbb{F}_p[x]$ of degree dividing n, because whenever I attempt to find a proof of this statement online I only find either incomplete answers or appeals to a Wikipedia page which is missing the relevant reference for this result. Once we have proven the statement we can then easily obtain a function that gives us the exact number of irreducible polynomials of any degree in $\mathbb{F}_p[x]$ for any prime p.

In order to establish that $x^{p^n} - x$ is the product of all the irreducible polynomials in $\mathbb{F}_p[x]$ of degree dividing n, I first need to prove a couple of Lemmas.

Lemma 1. *d divides n if and only if $x^d - 1$ divides $x^n - 1$.*

Proof. $(\Rightarrow)$

Let $n = dq$, then clearly

$$\begin{aligned}\left(x^d - 1\right)\left(\sum_{i=0}^{q-1} x^{di}\right) &= \sum_{i=1}^{q} x^{di} - \sum_{i=0}^{q-1} x^{di} \\ &= x^{dq} - 1 \\ &= x^n - 1.\end{aligned}$$

Which shows that $x^d - 1$ divides $x^n - 1$

$(\Leftarrow)$

Let $n = dq + r$, where $0 \leq r < d$ then we can write

$$x^n - 1 = x^{dq+r} - 1 = x^{dq+r} - x^r + x^r - 1 = x^r\left(x^{dq} - 1\right) + (x^r - 1)$$

Since we know $x^d - 1$ divides $x^n - 1$ and $x^{dq} - 1$ this means that it must divide $x^r - 1$, but since $0 \leq r < d$ this means that $x^r - 1 = 0$ which implies $r = 0$, hence it follows that d divides n $\square$

Lemma 2. *$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n,*

Proof. $(\Rightarrow)$

Since the prime subfield of both $\mathbb{F}_{p^d}$ and $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{F}_p$ we have the following field inclusion

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}.$$

since field extensions are multiplicative it follows that

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{F}_p]$$

Since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$ this shows that d divides n.

($\Leftarrow$)

Since d divides n then by Lemma 1 we have that

$$\begin{aligned} x^d - 1 | x^n - 1 &\Rightarrow p^d - 1 | p^n - 1 && \text{(Substitute } p \text{ for } x\text{)} \\ &\Rightarrow x^{p^d - 1} - 1 | x^{p^n - 1} - 1 && \text{(Apply Lemma 1 again)} \\ &\Rightarrow x^{p^d} - x | x^{p^n} - x && \text{(Multiply by } x \text{ on both sides)} \end{aligned}$$

This then implies that the splitting field of $x^{p^d} - x$ is a subfield of the splitting field of $x^{p^n} - x$, in other words $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.

□

Lemma 3. *Let $f(x)$ be an irreducible monic polynomial of degree d, then $f(x)$ divides $x^{p^n} - x$ if and only if d divides n.*

Proof. Let α be a root of $f(x)$ in some field extension, it then follows that $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$, by uniqueness of finite fields it follows that $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d}$.

($\Rightarrow$)

If $f(x)$ divides $x^{p^n} - x$ this means that the splitting field of $f(x)$ (denote it by $\mathbb{F}$) is a subfield of the splitting field of $x^{p^n} - x$ which is $\mathbb{F}_{p^n}$. This gives us the field inclusion $\mathbb{F}_{p^d} \subseteq \mathbb{F} \subseteq \mathbb{F}_{p^n}$, in particular this means $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, which by Lemma 2 implies that d divides n

($\Leftarrow$)

If d divides n then by Lemma 2 we have that

$$\alpha \in \mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$$

Since α can be any root of $f(x)$, this shows that every root of $f(x)$ has an isomorphic image in $\mathbb{F}_{p_n}$ and since any isomorphism between fields fixes the prime subfield (In this case $\mathbb{F}_p$) it follows that $\alpha \in \mathbb{F}_{p^n}$, and hence is a root of $x^{p^n} - x$ (because its splitting field is $\mathbb{F}_{p^n}$), which implies that every linear factor of $f(x)$ is also a linear factor of $x^{p^n} - x$, this shows that $f(x)$ divides $x^{p^n} - x$.

□

Theorem 1. *Let $\mathcal{F}_{p,n} := \{f(x) \in \mathbb{F}_p[x] : f(x)$ is an irreducible monic polynomial of degree $n\}$, then we have that*

$$x^{p^n} - x = \prod_{d|n} \left(\prod_{f(x) \in \mathcal{F}_{p,d}} f(x) \right)$$

Proof. By Lemma 3 we know that the only irreducible factors of $x^{p^n} - x$ are precisely the polynomials in $\mathcal{F}_{p,d}$ where d divides n, hence $\prod_{d|n} \left(\prod_{f(x) \in \mathcal{F}_{p,d}} f(x) \right)$ is the unique factorization of $x^{p^n} - x$ into irreducibles.

□

It is now easy to see that we might be able to establish the cardinality of the set $\mathcal{F}_{p,n}$ that is defined in Theorem 1, and in the end we can use the equation in Theorem 1 to derive $|\mathcal{F}_{p,n}|$ explicitly. The following corollary is the result of that calculation.

Corollary 1.1. *Let p be a prime and $n > 1$, and let $\phi_p(n)$ denote the number of irreducible monic polynomials of degree n in $\mathbb{F}_p[x]$. Then the value of $\phi_p(n)$ is given by*

$$\phi_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}},$$

where $\mu(d)$ is the Möbius function.

Proof. By comparing powers of the equation given in Theorem 1 we get the equation

$$p^n = \sum_{d|n} d|\mathcal{F}_{p,d}|$$

Since $\phi_p(d) = |\mathcal{F}_{p,d}|$ we have a relation between arithmetic functions given by

$$p^n = \sum_{d|n} d\phi_p(d).$$

This allows us to use the Möbius inversion formula to get

$$n\phi_p(n) = \sum_{d|n} \mu(d) p^{\frac{n}{d}},$$

which after division by n yields the result to be proved

$$\phi_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

□