Chapter 3

Finite fields

We have seen, in the previous chapters, some examples of finite fields. For example, the residue class ring $\mathbb{Z}/p\mathbb{Z}$ (when p is a prime) forms a field with p elements which may be identified with the Galois field $\mathbb{F}_p$ of order p.

The fields $\mathbb{F}_p$ are important in field theory. From the previous chapter, every field of characteristic p contains a copy of $\mathbb{F}_p$ (its prime subfield) and can therefore be thought of as an extension of $\mathbb{F}_p$. Since every finite field must have characteristic p, this helps us to classify finite fields.

6 Characterizing finite fields

Lemma 6.1
Let F be a finite field containing a subfield K with q elements. Then F has q^m elements, where $m = [F : K]$.

Proof. F is a vector space over K, finite-dimensional since F is finite. Denote this dimension by m; then F has a basis over K consisting of m elements, say $b_1, \ldots, b_m$. Every element of F can be uniquely represented in the form $k_1 b_1 + \cdots k_m b_m$ (where $k_1, \ldots, k_m \in K$). Since each $k_i \in K$ can take q values, F must have exactly q^m elements. ■

We are now ready to answer the question: "What are the possible cardinalities for finite fields?"

Theorem 6.2
Let F be a finite field. Then F has p^n elements, where the prime p is the characteristic of F and n is the degree of F over its prime subfield.

Proof. Since F is finite, it must have characteristic p for some prime p (by Corollary 2.19). Thus the prime subfield K of F is isomorphic to $\mathbb{F}_p$, by Theorem 4.5, and so contains p elements. Applying Lemma 6.1 yields the result. ■

So, all finite fields must have prime power order - there is no finite field with 6 elements, for example.

We next ask: does there exist a finite field of order p^n for every prime power p^n? How can such fields be constructed?

We saw, in the previous chapter, that we can take the prime fields $\mathbb{F}_p$ and construct other finite fields from them by adjoining roots of polynomials. If $f \in \mathbb{F}_p[x]$ is irreducible of degree n over $\mathbb{F}_p$, then adjoining a root of f to $\mathbb{F}_p$ yields a finite field of p^n elements. However, it is not clear whether we can find an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n, for *every* integer n.

The following two lemmas will help us to characterize fields using root adjunction.

Lemma 6.3
If F is a finite field with q elements, then every $a \in F$ satisfies $a^q = a$.

Proof. Clearly $a^q = a$ is satisfied for $a = 0$. The non-zero elements form a group of order $q - 1$ under multiplication. Using the fact that $a^{|G|} = 1_G$ for any element a of a finite group G, we have that all $0 \neq a \in F$ satisfy $a^{q-1} = 1$, i.e. $a^q = a$. ■

Lemma 6.4
If F is a finite field with q elements and K is a subfield of F, then the polynomial $x^q - x$ in $K[x]$ factors in $F[x]$ as

$$x^q - x = \prod_{a \in F} (x - a)$$

and F is a splitting field of $x^q - x$ over K.

Proof. Since the polynomial $x^q - x$ has degree q, it has at most q roots in F. By Lemma 6.3, all the elements of F are roots of the polynomial, and there are q of them. Thus the polynomial splits in F as claimed, and cannot split in any smaller field. ■

We are now ready to prove the main characterization theorem for finite fields.

Theorem 6.5 (Existence and Uniqueness of Finite Fields)
For every prime p and every positive integer n, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Proof. (Existence) For $q = p^n$, consider $x^q - x$ in $\mathbb{F}_p[x]$, and let F be its splitting field over $\mathbb{F}_p$. Since its derivative is $qx^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$, it can have no common root with $x^q - x$ and so, by Theorem 3.15, $x^q - x$ has q distinct roots in F. Let $S = \{a \in F : a^q - a = 0\}$. Then S is a subfield of F since

- S contains 0;
- $a, b \in S$ implies (by Freshmen's Exponentiation) that $(a-b)^q = a^q - b^q = a - b$, so $a - b \in S$;
- for $a, b \in S$ and $b \neq 0$ we have $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$,so $ab^{-1} \in S$.

On the other hand, $x^q - x$ must split in S since S contains all its roots, i.e its splitting field F is a subfield of S. Thus $F = S$ and, since S has q elements, F is a finite field with $q = p^n$ elements. (Uniqueness) Let F be a finite field with $q = p^n$ elements. Then F has characteristic p by Theorem 6.2, and so contains $\mathbb{F}_p$ as a subfield. So, by Lemma 6.4, F is a splitting field of $x^q - x$. The result now follows from the uniqueness (up to isomorphism) of splitting fields, from Theorem 5.18. ■

As a result of the uniqueness part of Theorem 6.5, we may speak of *the* finite field (or *the* Galois field) of q elements. We shall denote this field by $\mathbb{F}_q$, where q denotes a power of the prime characteristic p of $\mathbb{F}_q$.

Example 6.6

- In Example 5.14, we constructed a field $L = \mathbb{F}_3(\theta)$ of 9 elements, where θ is a root of the polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$. By Theorem 6.5, L is *the* field of 9 elements, i.e. $\mathbb{F}_9$.
- In Example 5.15, we constructed a field $L = \mathbb{F}_2(\theta)$ of 4 elements, where θ is a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$. By Theorem 6.5, L is *the* field of 4 elements, i.e. $\mathbb{F}_4$.

We can also completely describe the subfields of a finite field $\mathbb{F}_q$.

Theorem 6.7 (Subfield Criterion)
Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.

Proof. Clearly, a subfield K of F must have order p^m for some positive integer $m \leq n$. By Lemma 6.1, $q = p^n$ must be a power of p^m, and so m must divide n.

Conversely, if m is a positive divisor of n, then $p^m - 1$ divides $p^n - 1$, and so $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$ in $\mathbb{F}_p[x]$. So, every root of $x^{p^m} - x$ is a root of $x^q - x$, and hence belongs to $\mathbb{F}_q$. It follows that $\mathbb{F}_q$ must contain a splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$ as a subfield, and (from proof of Theorem 6.5) such a splitting field has order p^m. If there were two distinct subfields of order p^m in $\mathbb{F}_q$, they would together contain more than p^m roots of $x^{p^m} - x$ in $\mathbb{F}_q$, a contradiction. ■

So, the unique subfield of $\mathbb{F}_{p^n}$ of order p^m, where m is a positive divisor of n, consists precisely of the roots of $x^{p^m} - x$ in $\mathbb{F}_{p^n}$.

Example 6.8
Determine the subfields of the finite field $\mathbb{F}_{2^{30}}$. To do this, list all positive divisors of 30. The containment relations between subfields are equivalent to divisibility relations among the positive divisors of 30. (For diagram, see lectures!)

We can also completely characterize the multiplicative group of a finite field. For the finite field $\mathbb{F}_q$, we denote the multiplicative group of non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$.

Theorem 6.9
For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.

Proof. We may assume $q \geq 3$. Set $h = q - 1$, the order of $\mathbb{F}_q^*$, and let $h = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ be its prime factor decomposition. For each i, $1 \leq i \leq m$, the polynomial $x^{h/p_i} - 1$ has at most h/p_i roots in $\mathbb{F}_q$. Since $h/p_i < h$, it follows that there are nonzero elements of $\mathbb{F}_q$ which are not roots of this polynomial. Let a_i be such an element, and set $b_i = a_i^{h/p_i^{r_i}}$. Now, $b_i^{p_i^{r_i}} = 1$, so the order of b_i divides $p_i^{r_i}$ and so has the form $p_i^{s_i}$ for some $0 \leq s_i \leq r_i$. On the other hand,

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1,$$

so the order of b_i is precisely $p_i^{r_i}$.

Let $b = b_1 b_2 \dots b_m$. We claim: b has order $h(= q - 1)$, i.e. is a generator for the group. Suppose, on the contrary, that the order of b is a proper divisor of h. It is therefore a divisor of at least one of the m integers h/p_i, $1 \leq i \leq m$; wlog, say of h/p_1. Then

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Now, if $2 \leq i \leq m$, then $p_i^{r_i}$ divides h/p_1, and so $b_i^{h/p_1} = 1$. This forces $b_1^{h/p_1} = 1$. Thus the order of b_1 must divide h/p_1, which is impossible since the order of b_1 is $p_1^{r_1}$. Thus $\mathbb{F}_q^*$ is a cyclic group with generator b. ■

Definition 6.10
A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

By Theorem 1.13, $\mathbb{F}_q$ contains $\phi(q-1)$ primitive elements, where ϕ is Euler's function: the number of integers less than and relatively prime to $q - 1$. Recall that, if the integer n has the prime factorization $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}).$$

Example 6.11

- $\mathbb{F}_5$ has $\phi(4) = 2$ primitive elements, namely 2 and 3.
- $\mathbb{F}_4$ has $\phi(3) = 2$ primitive elements. Expressing $\mathbb{F}_4$ as $\mathbb{F}_2(\theta) = \{0, 1, \theta, \theta + 1\}$, where $\theta^2 + \theta + 1 = 0$, we find that both θ and $\theta + 1$ are primitive elements.

We are now ready to prove an important result.

Theorem 6.12
Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_r$ a finite extension field. Then

- *$\mathbb{F}_r$ is a simple extension of $\mathbb{F}_q$, i.e $\mathbb{F}_r = \mathbb{F}_q(\beta)$ for some $\beta \in \mathbb{F}_r$;*
- *every primitive element of $\mathbb{F}_r$ can serve as a defining element β of $\mathbb{F}_r$ over $\mathbb{F}_q$.*

Proof. Let α be a primitive element of $\mathbb{F}_r$. Clearly, $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. On the other hand, since $\mathbb{F}_q(\alpha)$ contains 0 and all powers of α, it contains all elements of $\mathbb{F}_r$. So $\mathbb{F}_r = \mathbb{F}_q(\alpha)$. ■

So, we can express *any* finite field K with subfield F, by adjoining to F a root β of an appropriate irreducible polynomial f, which of course must have degree $d = [K : F]$. Although the proof of Theorem 6.12 uses a β which is a primitive element of K, it is not in fact necessary for β to be a multiplicative generator of K^*, as the next example shows.

Example 6.13
Consider the finite field $\mathbb{F}_9$. We can express $\mathbb{F}_9$ in the form $\mathbb{F}_3(\beta)$, where β is a root of the polynomial $x^2 + 1$, irreducible over $\mathbb{F}_3$. However, since $\beta^4 = 1$, β does not generate the whole of $\mathbb{F}_9^*$, i.e. β is not a primitive element of $\mathbb{F}_9$.

Corollary 6.14
For every finite field $\mathbb{F}_q$ and every positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.

Proof. Let $\mathbb{F}_r$ be the extension field of $\mathbb{F}_q$ of order q^n, so that $[\mathbb{F}_r : \mathbb{F}_q] = n$. By Theorem 6.12, $\mathbb{F}_r = \mathbb{F}_q(\alpha)$ for some $\alpha \in \mathbb{F}_r$. Then, by properties of minimal polynomials, the minimal polynomial of α over $\mathbb{F}_q$ is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n. ■

7 Irreducible polynomials

In this section, we investigate irreducible polynomial over finite fields.

Lemma 7.1
Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over a finite field $\mathbb{F}_q$ and let α be a root of f in an extension field of $\mathbb{F}_q$. Then, for a polynomial $h \in \mathbb{F}_q[x]$, we have $h(\alpha) = 0$ if and only if f divides h.

Proof. The minimal polynomial of α over $\mathbb{F}_q$ is given by $a^{-1}f$, where a is the leading coefficient of f (since it is a monic irreducible polynomial in $\mathbb{F}_q[x]$ having α as a root). The proposition then follows from part (ii) of Theorem 4.10. ■

Lemma 7.2
Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m. Then f divides $x^{q^n} - x$ if and only if m divides n.

Proof. First, suppose f divides $x^{q^n} - x$. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $\alpha^{q^n} = \alpha$, so $\alpha \in \mathbb{F}_{q^n}$. Thus $\mathbb{F}_q(\alpha)$ is a subfield of $\mathbb{F}_{q^n}$. Since $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, we have $n = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)]m$, so m divides n.

Conversely, suppose m divides n. Then by Theorem 6.7, $\mathbb{F}_{q^n}$ contains $\mathbb{F}_{q^m}$ as a subfield. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, and so $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Thus $\alpha \in \mathbb{F}_{q^n}$, hence $\alpha^{q^n} = \alpha$, and so α is a root of $x^{q^n} - x \in \mathbb{F}_q[x]$. Therefore, by Lemma 7.1, f divides $x^{q^n} - x$. ■

We are now ready to describe the set of roots of an irreducible polynomial.

Theorem 7.3
If f is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m, then f has a root α in $\mathbb{F}_{q^m}$. Moreover, all the roots of f are simple and are given by the m distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.

Proof. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, hence $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, and so $\alpha \in \mathbb{F}_{q^m}$.

We now show that, if $\beta \in \mathbb{F}_{q^m}$ is a root of f, then β^q is also a root of f. Write $f = a_m x^m + \cdots + a_1 x + a_0$ ($a_i \in \mathbb{F}_q$). Then

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \cdots + a_1 \beta^q + a_0 \\ &= a_m^q \beta^{qm} + \cdots + a_1^q \beta^q + a_0^q \\ &= (a_m \beta^m + \cdots + a_1 \beta + a_0)^q \\ &= f(\beta)^q = 0, \end{aligned}$$

using Lemma 6.3 and Freshmen's Exponentiation.

Thus, the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ are roots of f. We must check that they are all distinct. Suppose not, i.e. $\alpha^{q^j} = \alpha^{q^k}$ for some $0 \leq j < k \leq m-1$. Raising this to the power q^{m-k} , we get

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

It then follows from Lemma 7.1 that f divides $x^{q^{m-k+j}} - x$. By Lemma 7.2, this is possible only if m divides $m - k + j$, a contradiction since $0 < m - k + j < m$. ■

This result gives us two useful corollaries.

Corollary 7.4
Let f be an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m. Then the splitting field of f over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$.

Proof. Theorem 7.3 shows that f splits in $\mathbb{F}_{q^m}$. To see that this is the splitting field, note that $\mathbb{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. ■

Corollary 7.5
Any two irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree have isomorphic splitting fields.

As we shall see later, sets of elements such as those in Theorem 7.3 appear often in the theory of fields.

Theorem 7.6
For every finite field $\mathbb{F}_q$ and every $n \in \mathbb{N}$, the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$.

Proof. By Lemma 7.2, the monic irreducible polynomials over $\mathbb{F}_q$ which occur in the canonical factorization of $g = x^{q^n} - x$ in $\mathbb{F}_q[x]$ are precisely those whose degrees divide n. Since $g' = -1$, by Theorem 3.15 g has no multiple roots in its splitting field over $\mathbb{F}_q$. Thus each monic irreducible polynomial over $\mathbb{F}_q$ whose degree divides n occurs exactly once in the canonical factorization of g in $\mathbb{F}_q[x]$. ■

Example 7.7
Take $q = n = 2$; the monic irreducible polynomials over $\mathbb{F}_2[x]$ whose degrees divide 2 are x, $x+1$ and x^2+x+1. It is easily seen that $x(x+1)(x^2+x+1) = x^4+x = x^4-x$.

Corollary 7.8
If $N_q(d)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d, then

$$q^n = \sum_{d|n} dN_q(d) \text{ for all } n \in \mathbb{N},$$

where the sum is extended over all positive divisors d of n.

Proof. This follows immediately from Theorem 7.6, upon comparing the degree of $g = x^{q^n} - x$ with the total degree of the canonical factorization of g. ■

This corollary allows us to obtain an explicit formula for the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of a given degree. To do so, we need the following arithmetic function, which will also prove useful in the next chapter.

Definition 7.9
The *Moebius function* μ is the function on $\mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } n \text{ is divisible by the square of a prime.} \end{cases}$$

Example 7.10
(i)$\mu(5) = -1$; (ii)$\mu(35) = 1$; (iii)$\mu(50) = 0$.

Lemma 7.11
For $n \in \mathbb{N}$, the Moebius function satisfies

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. The $n = 1$ case is immediate. For $n > 1$ we need only consider the positive divisors d of n for which $\mu(d)$ is non-zero, namely those d for which $d = 1$ or d is a product of distinct primes. If $p_1, \ldots, p_k$ are the distinct prime divisors of n then

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \le i_1 < i_2 \le k} \mu(p_{i_1} p_{i_2}) + \cdots + \mu(p_1 p_2 \ldots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1 + (-1))^k = 0. \end{aligned}$$

■

Theorem 7.12 (Moebius Inversion Formula)

- *Additive version: let h and H be two functions from $\mathbb{N}$ into an additively written abelian group G. Then*

$$H(n) = \sum_{d|n} h(d) \text{ for all } n \in \mathbb{N} \tag{3.1}$$

if and only if

$$h(n) = \sum_{d|n} \mu(\frac{n}{d}) H(d) = \sum_{d|n} \mu(d) H(\frac{n}{d}) \text{ for all } n \in \mathbb{N}. \tag{3.2}$$

- *Multiplicative version: let h and H be two functions from $\mathbb{N}$ into a multiplicatively written abelian group G. Then*

$$H(n) = \prod_{d|n} h(d) \text{ for all } n \in \mathbb{N} \tag{3.3}$$

if and only if

$$h(n) = \prod_{d|n} H(d)^{\mu(\frac{n}{d})} = \prod_{d|n} H(\frac{n}{d})^{\mu(d)} \text{ for all } n \in \mathbb{N}. \tag{3.4}$$

Proof. Additive version: we prove the forward implication; the converse is similar and is left as an exercise. Assume the first identity holds. Using Lemma 7.11, we get

$$\begin{aligned} \sum_{d|n} \mu(\frac{n}{d}) H(d) &= \sum_{d|n} \mu(d) H(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} h(c) \\ &= \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) h(c) = \sum_{c|n} h(c) \sum_{d|\frac{n}{c}} \mu(d) = h(n) \end{aligned}$$

for all $n \in \mathbb{N}$.

Multiplicative version: immediate upon replacing sums by products and multiples by powers. ■

We can now apply this result as follows.

Theorem 7.13

The number $N_q(n)$ of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by

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

Proof. Apply the additive case of the Moebius Inversion Formula to the group $G = (\mathbb{Z}, +)$. Take $h(n) = nN_q(n)$ and $H(n) = q^n$ for all $n \in \mathbb{N}$. By Corollary 7.8, the identity (3.1) is satisfied, and so the result follows. ■

Remark 7.14

Since it is clear from this formula that $N_q(n)$ is greater than zero for all n, this gives an alternative proof of Theorem 6.14.

Example 7.15

The number of monic irreducibles in $\mathbb{F}_q[x]$ of degree 12 is given by

$$\begin{aligned} N_q(12) &= \frac{1}{12}(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q) \\ &= \frac{1}{12}(1.q^{12} + (-1)q^6 + (-1)q^4 + 0.q^3 + 1.q^2 + 0.q) \\ &= \frac{1}{12}(q^{12} - q^6 - q^4 + q^2). \end{aligned}$$

We can also obtain a formula for the *product* of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of fixed degree.

Theorem 7.16
The product $I(q,n;x)$ of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by:

$$I(q,n;x) = \prod_{d|n}(x^{q^d} - x)^{\mu(\frac{n}{d})} = \prod_{d|n}(x^{q^{\frac{n}{d}}} - x)^{\mu(d)}.$$

Proof. From Theorem 7.6 we know that

$$x^{q^n} - x = \prod_{d|n} I(q,d;x).$$

Now apply Moebius Inversion in the multiplicative form to the multiplicative group G of non-zero rational functions over $\mathbb{F}_q$. Take $h(n) = I(q,n;x)$ and $H(n) = x^{q^n} - x$ to get the desired formula. ■

Example 7.17
Take $q = 2$ and $n = 4$. Then the product of all monic irreducible quartics in $\mathbb{F}_2[x]$ is:

$$\begin{aligned} I(2,4;x) &= (x^{16} - x)^{\mu(1)}(x^4 - x)^{\mu(2)}(x^2 - x)^{\mu(4)} \\ &= \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} \\ &= x^{12} + x^9 + x^6 + x^3 + 1 \end{aligned}$$