Theorem. We fix a prime p. For every $q = p^n$, the extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois, and

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \phi \rangle,$$

where ϕ is the Frobenius automorphism , $\phi(x) = x^p$, all $x \in \mathbb{F}_q$.

The Galois correspondence in the case of finite fields.

We fix a prime p and we consider the finite field F_{p^n}, with $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$ cyclic or order n.

- For every divisor d of n there is a unique subfield of $\mathbb{F}_{p^n}$ of cardinality p^d.
- For every divisor d of n there is a unique subgroup of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of order $\frac{n}{d}$, namely $G_d = \langle \phi^d \rangle$.
- There is a one-to-one correspondence

$$\{\text{subgroups of } \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)\} \leftrightarrow \{\text{ subfields of } \mathbb{F}_{p^n}\}$$

$$G_d \leftrightarrow \mathbb{F}_{p^d},$$

since $x \in \mathbb{F}_{p^n} \Leftrightarrow x^{p^d} = x \Leftrightarrow \phi^d(x) = x$.

Example: $K = \mathbb{F}_{3^6}$, the field with 729 elements.

(i) We find all the subfields of K. Since $K \simeq \mathbb{F}_{3^6}$, any subfield of K is of the form $\mathbb{F}_{3^n}$ with $n|6$. Thus, the subfields of K are $\mathbb{F}_3, \mathbb{F}_9, \mathbb{F}_{27}$ and K itself.

(ii) The Galois group of $F/\mathbb{F}_3$ is $G_6 = \langle \phi \rangle$, with $\phi(X) = x^3$ for all $x \in \mathbb{F}_{3^6}$, with subgroupsG_2 of order 3 and G_3 of order 2. The Galois correspondence between the subgroups of G_6, with $\phi(X) = x^3$ and the subfields of K is $G_6 \leftrightarrow \mathbb{F}_3$,$G_2 \leftrightarrow \mathbb{F}_{p^2}$,$G_3 \leftrightarrow \mathbb{F}_{p^3}$,Id. $\leftrightarrow \mathbb{F}_{p^6}$.

(iii) We compute how many elements $\alpha \in K$ satisfy $K = \mathbb{F}_3[\alpha]$. We know that $\alpha \in K$ satisfies $K = \mathbb{F}_3[\alpha]$ if and only if α is en K and α is in no proper subfield of K. Since $\mathbb{F}_9 \cap \mathbb{F}_{27} = \mathbb{F}_3$, there are $729 - 27 - 9 + 3 = 696$ such α. □

(iv) We also know many irreducible polynomials of degree 6 there are in $\mathbb{F}_3[X]$. Since the set of zeros of these polynomials has cardinal 696, there are $\frac{696}{6} = 116$ irreducible polynomials of degree 6 in en $\mathbb{F}_3[X]$. For each such polynomial f, it is $\mathbb{F}_{3^6} = \mathbb{F}_3[X]/(f)$.