14.3 Finite fields.

For any prime p and $n \in \mathbb{N}$, the extension F_{p^n}/F_p is Galois.

Hence

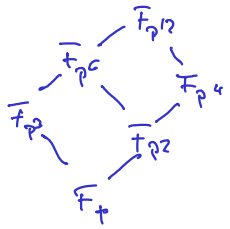
(1) $n = [F_{p^n} : F_p] = |\mathrm{Gal}(F_{p^n})|$
(2) Since $F_{p^n}^* = \langle \alpha \rangle$ is cyclic, also $F_{p^n} = F_p(\alpha)$ and there exists an irreducible $m_{\alpha, F_p}(x) \in F_p[x]$ of degree n.

Proposition. $\mathrm{Gal}(F_{p^n}/F_p) = \langle \sigma_p \rangle$ for the Frobenius automorphism $\sigma_p \colon F_{p^n} \to F_{p^n}, x \mapsto x^p$.

Proof. $|\langle G_p \rangle| = n$ by HW □

Example. $n = 12$

$\langle G \rangle \cong \mathbb{Z}_{12}$



Corollary. $F_{p^d} \leq F_{p^n}$ *iff* $d|n$.

Corollary. $x^{p^d} - x | x^{p^n} - x$ *iff* $d|n$.

? cf HW

Corollary. $x^{p^n} - x$ *is the product of all monic irreducible polynomials* $f(x) \in F_p[x]$ *with* $\deg f | n$.

Proof. Let $f(x) \in \mathbb{F}_p[x]$ irreducible, monic, $\deg f(x) = d$,
Let α such that $f(\alpha) = 0$.

1) Assume $d|n$. Then $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d}$, the splitting field of $x^{p^d} - x$.
So $f(x)$ divides $x^{p^d} - x$ and also $x^{p^n} - x$ by previous Cor.

2) Conversely assume $f(x) \mid x^{p^n} - x$.
Then $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$ yields $d|n$ by above Cor.
Hence the irred factors of $x^{p^n} - x$ are exactly all the monic irred polynomials whose degree divides n (with multiplicity 1 since $x^{p^n} - x$ is separable). □

Example. For F_8/F_2 consider
$x^8 - x = x(x+1)(x^6 + x^5 + \dots + x + 1)$
$(x^3 + x + 1)(x^3 + x^2 + 1)$

Corollary. *The algebraic closure of F_p is*

$$\bar{F}_p = \bigcup_{n\in\mathbb{N}} F_{p^n}.$$

Proof. For $F_{p^n}, F_{p^m} \subseteq F_{p^{\mathrm{lcm}(n,m)}}$ □

The number of irreducible polynomials of degree n over F_p.

Number Theory: For $n \in \mathbb{N}$, the *Möbius function* is

$$\mu(n) := \begin{cases} (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes,} \\ 0 & \text{if } n \text{ has a squared factor.} \end{cases}$$

For $f\colon \mathbb{N} \to \mathbb{R}$ and

$$g(n) := \sum_{d|n} f(d) \text{ for all } n \in \mathbb{N},$$

the *Möbius inversion formula* states:

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) \text{ for all } n \in \mathbb{N}.$$

Let $\psi(n) := |\{q(x) \in F_p[x] : \ q(x) \text{ monic, irreducible, } \deg q(x) = n\}|$.
By the Corollary above

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

By the Möbius inversion formula

$$n\psi(n) = \sum_{d|n} \mu(d) p^{n/d}$$

Example. For $p = 2, n = 4$

$$\psi(4) = \frac{1}{4}\left[\underbrace{\mu(1)}_{=1} 2^{4/1} + \underbrace{\mu(2)}_{=-1} \cdot 2^{4/2} + \underbrace{\mu(4)}_{=0} \cdot 2^{4/4}\right]$$

$$= \frac{1}{4}\left[16 - 4\right] = 3$$