NAP 2019 - MODULE V - CLASS #2
July 17, 2019

Lea Terracini

- **Example**: we showed the irreducibility of the polynomial $X^p - X - 1$ over $\mathbb{F}_p$, and its variants $X^p - X - j$, $j \in \mathbb{F}_p^\times$. Adding to $\mathbb{F}_p$ a root α of each of these polynomials gives rise to a field $\mathbb{F}_p(\alpha)$ of order p^p.

- $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n|m$

- **Corollary**:
$$X^{p^n} - X = \prod g(X)$$
where $g(X)$ varies in the set of irreducible polynomials in $\mathbb{F}_p[X]$ of degree dividing n.

- **Example**: Factorization
$$X^{16}-X = X(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1).$$

- **Question**: Let p, q be prime numbers; how many irrducible polynomials of degree q are there in $\mathbb{F}_p[X]$?

- Preliminary considerations on Galois groups: if L/K is a finite extension of finite fields and $G = \mathrm{Gal}(L/K)$ then
  - every subgroup of G is normal: G is a *Dedekind* group.

  - for every d dividing $|G|$ there exists exactly one subgroup of G of order d.

  We observed that *cyclic* groups satisfy both this conditions.

- **Theorem** : $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group generated by the Frobenius automorphism Φ.