NAP 2019 - MODULE V - CLASS #1
July 15,2019

Lea Terracini

- We discussed about the existence of finite fields and recall that $\mathbb{Z}_n$ is a field if and only if n is a prime number.
  For every prime p we denote by $\mathbb{F}_p$ the field of order p.

- We noticed that we can construct some other finite fields as quotients $K = \mathbb{F}_p[X]/(g(X))$ where $g(X)$ is an irreducible polynomial in $\mathbb{F}_p[X]$; such a field K has order p^n, where $n = \deg(g(X))$. It can be regarded as the extension $\mathbb{F}_p(\alpha)$ of $\mathbb{F}_p$, where α is a root of $g(X)$.
  Example: $K_1 = \mathbb{F}_7[X]/(X^2+1)$, $K_2 = \mathbb{F}_7[X]/(X^2+2)$ are both fields of order 49.

- Every finite field K has characteristic a prime number p, contains $\mathbb{F}_p$ as prime subfield and has order p^n for some $n \geq 1$.

- **Theorem**: a) For every prime number p and every natural number $n > 0$ there exists a field K of order p^n.
  b) K is the splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$.
  c) K is essentially unique, that is every field of order p^n is isomorphic to K.

- We deeply analysed point c) of the previous theorem, discussed the difference between *equality* and *isomorphism* and constructed explicitly an isomorphism
  $$\theta : \mathbb{F}_7(\alpha) \longrightarrow \mathbb{F}_7(\beta)$$
  where α is a root of $X^2 + 1$ and β is a root of $X^2 + 2$.

- The theorem above enables us to denote by $\mathbb{F}_p^n$ <u>the</u> field of order p^n (unique up to isomorphism). By construction $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a normal extension. It is obviously finite and it is separable, since it is algebraic over its prime subfield. It is a Galois extension.

- Next tasks: study the groups $\mathbb{F}_{p^n}^{\times}$, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.