The Construction of Finite Fields

**Notation:** If $F$ is a field, and $n \leq 1$, then $F[X]_n$ denotes the set of all polynomials of degree $< n$:

$$F[X]_n := \{ a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} : a_i \in F \}.$$  

**Note:** The addition of polynomials and multiplication by constants give $F[X]_n$ the structure of an $F$-vector space. Moreover, the rule

$$a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \mapsto (a_0, \ldots, a_{n-1})$$

defines an isomorphism of $F$-vector spaces:

$$F[X]_n \cong F^n.$$  

**Notation:** Fix a polynomial $g \in F[X]$ with $\deg(g) = n$ and define a multiplication on $F[X]_n$ by:

$$f_1 \ast g f_2 = \text{rem}(f_1 f_2, g), \quad \text{for } f_1, f_2 \in F[X]_n.$$ 

This makes $F[X]_n$ into a *ring* which is denoted by:

$$A_g = F[X]/(g).$$  

**Remark:** Thus, the remainder function $f \mapsto \text{rem}(f, g)$ defines a surjective ring homomorphism

$$r_g : F[X] \rightarrow F[X]/(g).$$
Remark: Similar to the case of integers, we write
\[ f_1 \equiv f_2 \pmod{g} \iff \text{rem}(f_1, g) = \text{rem}(f_2, g). \]

Proposition 1': \( F[X]/(g) \) is a field \iff \( g \) is irreducible over \( F \).

Remark: The proof of \((\Leftarrow)\) uses the following special case of the Extended Euclidean Algorithm (for polynomials): If \( f, g \in F[X] \), \( g \) irreducible and \( g \nmid f \), then there exist polynomials \( h_1, h_2 \in F[X] \) s. th.

\[ h_1(X)f(X) + h_2(X)g(X) = 1. \]

Application: Let \( F = \mathbb{F}_p \) be the prime field with \( p \) elements, where \( p \) is a prime.

(a) For any \( g \in \mathbb{F}_p[X] \) of degree \( n := \deg(g) \geq 1 \),

\[ A_g = \mathbb{F}_p[X]/(g) \]

is a finite ring consisting of \( p^n \) elements.

(b) If \( g \in \mathbb{F}_p[X] \) is irreducible of degree \( n \), then

\[ A_g = \mathbb{F}_p[X]/(g) \]

is a finite field of order \( p^n \).

Remark: Later we will see that every finite field can be constructed in this way.