Lecture 13 : More on the polynomial construction of finite fields

Recall the field $(\mathbb{F}[x]/f(x), +, \mathbb{F}, \cdot)$, where $f(x) \in \mathbb{F}^d[x]$ is an irreducible polynomial of degree d, constructed in the last lecture.

If $\mathbb{F} = \mathbb{F}_p$, we simply call $\mathbb{F}[x]/f(x)$ as $\mathbb{F}_{p^d}$.

↳ "extension field of $\mathbb{F}$".

Qn: How many elements does $\mathbb{F}_{p^d}$ have?

Example : Consider the case when $\mathbb{F} = \mathbb{F}_2$ and let $f(x) = x^3+x^2+x+1$ be an irreducible poly. in $\mathbb{F}_2^3[x]$.

We now illustrate a convenient representation of $\mathbb{F}_8 = \mathbb{F}[x]/f(x)$.

Polynomial form	d-tuple representation ($d=3$)
0	000
1	100
x	010
x^2	001
$x^3 = x+1$	110
$x^4 = x^2+x$	011
$x^5 = x^2+x+1$	111

$x^7 = 1$

Def 1: Let $\mathbb{F}$ be a field and $\mathbb{K}$ be an extension field of $\mathbb{F}$. An element $\beta \in \mathbb{K}$ is called a root of $f(x) \in \mathbb{F}[x]$ if $f(\beta) = 0$, when evaluated in $\mathbb{K}$, or equivalently, when $(x-\beta) \mid f(x)$ in $\mathbb{K}[x]$.
↳ "divides"

Def 2: The multiplicity of a root β of $f(x)$ is the largest integer $m \geq 0$ s.t. $(x-\beta)^m \mid f(x)$.

The following theorem is important and will be of use to us soon.

Theorem 1: A polynomial $f(x) \in \mathbb{F}[x]$ of degree m has at most m roots (counting multiplicities) over any extension field $\mathbb{K}$ of $\mathbb{F}$.

Proof: Observe that in $\mathbb{K}[x]$, we must have

$$\prod_{i=1}^{n} (x-\beta_i)^{m_i} \mid f(x),$$

where $\beta_1, \dots, \beta_n$ are given roots and $m_1, \dots, m_n$ are their multiplicities. We must then have that $\sum_{i=1}^{n} m_i \leq m$. ▨

Example: Recall that x^2+1 has no roots over $\mathbb{R}$, but 2 roots in $\mathbb{C}$.