Oct 6, 2021.

$$\mathbb{F}_{2^k} = \mathbb{F}_2[x] \pmod{P(x)}$$

$P(x)$ = irreducible poly in $\mathbb{F}_2[x]$

$\deg(P(x)) = k$.

Let $P(\alpha) = 0$, α = root of $P(x)$

$\alpha \in \mathbb{F}_{2^k}$ $\quad \alpha \notin \mathbb{F}_2$

Operations in $\mathbb{F}_{2^k}$.

1. Reduce coefficients $\pmod 2$

2. Reduce all computations $\pmod{P(\alpha)}$

Any element A in F_{2^k}

$$A = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$$

$$a_i \in \{0,1\} = F_2$$

$$F_{2^2} = F_2[x] \pmod{x^2+x+1}$$

$$\alpha^2+\alpha+1 = 0.$$

$00 \quad = a_0 = 0 = a_1$

$= 0 + 0\cdot\alpha$

$01 \quad a_0 = 1,\ a_1 = 0 = 1$

$10 \quad a_0 = 0 \quad a_1 = 1\ \alpha$

$11 \quad \alpha + 1$

$\mathbb{F}_{16}$. $\qquad x^4+x^3+1$

$$\alpha^5 = \overset{a_3}{\alpha^3} + \overset{a_1}{\alpha} + \overset{a_0}{1} = A \checkmark$$

$$\alpha^{11} = \alpha^3 + \underset{b_2}{\alpha^2} + \underset{b_0}{1} = B$$

A

a_3	a_2	a_1	a_0
1	0	1	1

B

1	1	0	1

$+$

0	1	1	0

$$\alpha^2+\alpha = \alpha^{13}$$

Compute inverses.

$$a \in \mathbb{Z}_p = \mathbb{F}_p \quad a \cdot \underset{?}{\underline{\underline{a^{-1}}}} = 1$$

$$GCD(a, p) = 1$$

$$s \cdot a + t \cdot p = 1 \pmod{p}$$

$$\Rightarrow \underline{\underline{s \cdot a}} = 1 \pmod{p}$$

---

this works in $\mathbb{F}_p = \mathbb{Z}_p$

How would you use this in $\mathbb{F}_{2^k}$?

[Think – HW!!]

Generally denote $\mathbb{F}_q$ or $GF(q)$.

$$q = p^K \quad \left(2^K \text{ in our case}\right).$$

If $P(x) =$ Primitive poly.

$P(\alpha) = 0$, $\alpha =$ Primitive root.

Then $\mathbb{F}_q = \{0, 1 = \alpha^{q-1}, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$

If $P(x) =$ irreducible, but <u>not</u> primitive,

the we cannot generate all elements of the field.

Algebraically Closed Field
(ACF)

$\mathbb{F} = \text{ACF}$ iff

$\forall\, p(x) \in \mathbb{F}[x]$,

$p(\alpha) = 0 \Rightarrow \alpha \in \mathbb{F}$.

R : x^2+1, $x^2 = -1$

$x = \pm i$

$i \notin R$

$R \neq \text{ACF}$. $C = \text{ACF}$.

ACF = infinite field

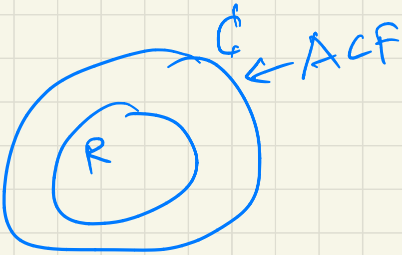
$\mathbb{F}_q$ = <u>NOT</u> ACF

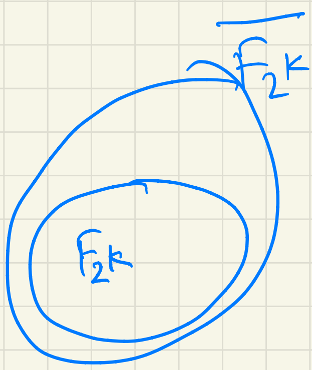
Every field $\mathbb{F} \subset \overline{\mathbb{F}}$

$\overline{\mathbb{F}}$ = ACF.

$$\mathbb{F}_q \subset \overline{\mathbb{F}_q} \leftarrow \text{ACF.}$$

$$\overline{\mathbb{F}_{2^k}} = \bigcup_{n \mid k} \mathbb{F}_{2^n}$$





$\mathbb{F}_{2^k}[x]$ $\quad p(\alpha)=0$

$\mathbb{R}[x]$ $\quad \mathbb{Z}[x]$ $\quad \mathbb{Q}[x]$

$$f = \alpha^2 \cdot x^2 + \alpha^{99} \cdot x + \alpha^{203}$$

$p(\alpha)=0$

$\mathbb{F}_9[x]$.

$$f(x) = x^9 - x$$

$\forall \alpha \quad \alpha^9 = \alpha$

$\alpha^9 - \alpha = 0$

Vanishing poly of $\mathbb{F}_9$.

$f_1(x),\ f_2(x) \in \mathbb{F}_q[x].$

$c_1 \qquad c_2 \qquad \Rightarrow p^x$

Prove,

$$f_1(x) = f_2(x) \quad \forall x. \qquad x^2 = x$$

$$x^2 - x = 0$$

$$f_1(x) - f_2(x) = g(x)$$

$f_1 = f_2 \iff g(x) = 0$. in $\mathbb{F}_q$.

$g(x) = 0$

$x^q - x \mid g(x)$ $\mod(x^q - x)$

$\leftarrow 0 \Leftarrow$

$$\alpha^5 = \alpha^3 + \alpha + 1$$

$$\alpha^{10} = \alpha^3 + \alpha$$