⊙ Polynomials over fields

t degree polynomial over field $(F, +, \circ)$

$$\boxed{f(X) = a_0 + (a_1 \circ X) + \cdots + a_t X^t}$$

where $a_i \in F$

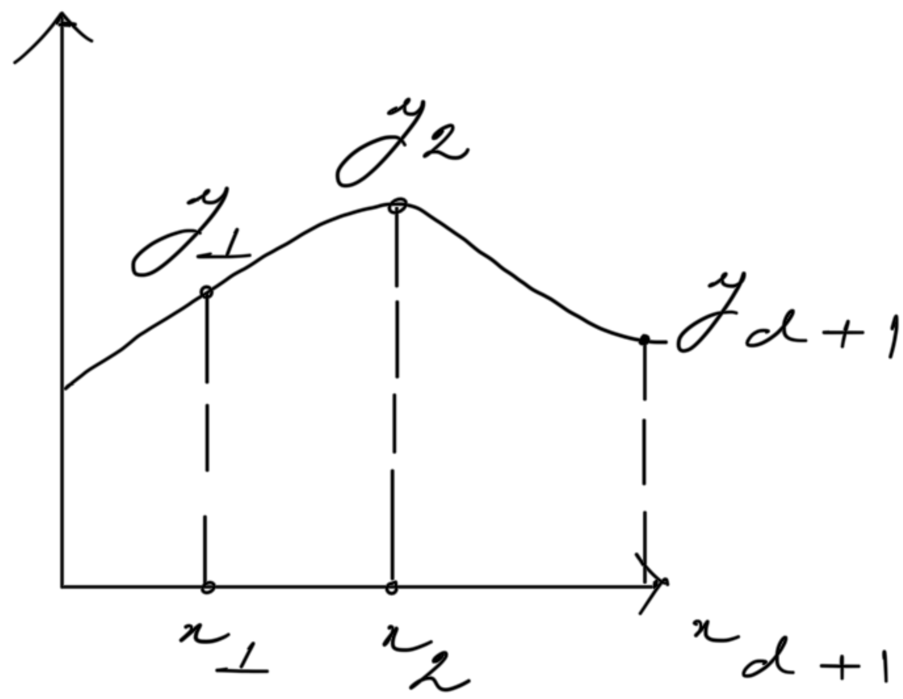
Root of the polynomial $v \in F$ if

$\boxed{f(v) = 0}$ th element of F

⊙ A t degree polynomial over field F can have at most t roots.

⊙ 2 distinct t degree polynomials over F can have atmost t common values.

⊙ Let $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ be $d+1$ points from F, where the x are distinct, then there exists a unique d degree polynomial $f(X)$ over F, such that $f(x_i) = y_i$ for $1 \leq i \leq (d+1)$



Lagrange Polynomial

Proof

$f(X)$ be a linear combination of $(d+1)$ d degree polynomials. Then

$$\boxed{f(X) = y_1\,\delta_1(X) + \cdots + y_{d+1}\,\delta_{d+1}(X)}$$

The δ polynomials should be such that

$\delta_i(x_i) = 1$ and $\delta_i(x_{\neq i}) = 0$ at $x = x_i$.

Then $f(X) = y_i$ at $x = x_i$

$$\boxed{\delta_i(X) = \frac{(X-x_1)\cdots(X-x_{i-1})(X-x_{i+1})\cdots}{(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots}}$$

$$\Rightarrow \delta_i(X) = c_i\left\{(X-x_1)\cdots(X-x_{i-1})(X-x_{i+1})\cdots\right\}$$

where c_i is the multiplicative inverse of $(x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots$

So $c_i \neq$ 0th element of F.

- Now if I am given $(x_1, y_1) \cdots (x_{d+1}, y_{d+1})$, we can find $f(X)$ using Lagrange Interpolation and then compute $f(X)$ at $x = x_{new}$.

$$f(x_{new}) = y_1 \cdot \delta_1(x_{new}) + \cdots + y_{d+1} \cdot \delta_{d+1}(x_{new})$$

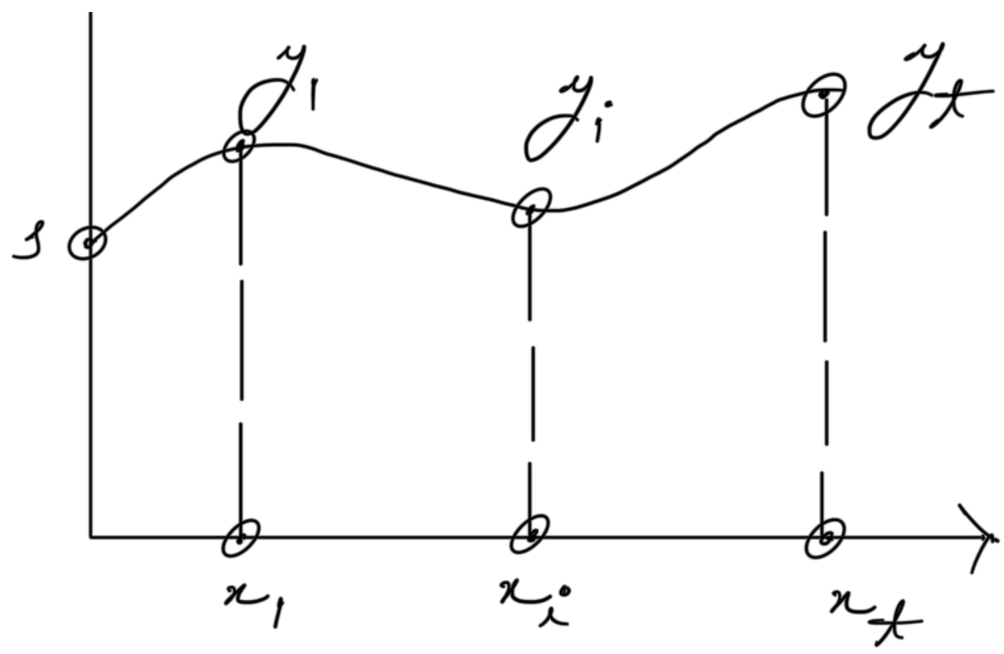
- Let $P^{s,t}$ be the set of all t degree polynomial F with $a_0 = s$.

$f(X) \in P^{s,t}$ where $f(X) = s + a_1 X + \cdots$

$$\boxed{|P^{s,t}| = |F|^t}$$

For any given $s \in F$, there is a unique polynomial from $P^{s,t}$ passing through $\{(0, s), (x_1, y_1), \ldots, (x_t, y_t)\}$

$\uparrow$



⊙ Shamir's Experiment

$$\xrightarrow{s \in F} \begin{array}{l}\text{Randomly pick}\\ f(X) \text{ from } P^{s,t}\end{array} \longrightarrow \{(x_1, y_1), \ldots, (x_n, y_n)\}$$

If someone knows t (x, y) pairs, then the probability that he/she can find s,

$$\boxed{\Pr_{f(X) \in P^{s,t}} \left[(f(x_1) = y_1) \wedge \cdots \wedge (f(x_t) = y_t) \right] = \frac{1}{|P^{s,t}|}}$$

So probability of the first term of $f(X)$ being s is the same as the probability of the first term being s' (any other

$\in \rho^{s,t})$

But if someone knows $(t+1)$ pairs, then $f(X)$ can be traced back. Then s can be known using $\boxed{f(0) = s}$

Shamir's Secret Sharing Protocol

✓ Correctness

✓ Privacy

① Why field is required

→ Use $(F, +_n, \circ_n)$ since $+_n$ and $\circ_n$ operations can be done more effectively compared to arithmetic $+$ and $\circ$

→ Privacy will break if Z or R is used instead of F.