⊙ **Galois field** (finite fields)

A finite field can be constructed with p^m elements

p — prime number

$m \in (+ Z)$

$GF(p^m)$

for $m = 1$

$GF(p)$ is called prime field

for $m > 1$, $GF(p^m)$ is called extension field

$GF(2^8)$ used for AES encryption

$$GF(p) = (Z_n, +_n, \cdot_n) = \{0, \ldots, p-1\}$$

$a \cdot a^{-1} = 1$ (Identity element). a^{-1} can be computed using Extended Euclidean Algorithm.

→ Extension field $GF(2^m)$

Elements of $GF(2^m)$ are of the form

$$\boxed{a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} = A(X)} \in GF(2^m)$$

where $a_i \in GF(2)$ prime field.

Eg Let $m = 3$. Then $A(X) = a_0 + a_1 x + a_2 x^2$

$\Rightarrow A(x) = (a_0, a_1, a_2)\, x$

vector of 3 bits since $a_0, a_1, a_2 \in GF(3) = \{0, 1\}$

$GF(2^3) = \{0, 1, x, (x+1), x^2, (x^2+1), (x^2+x), (x^2+x+1)\}$ —— 8 elements.