5.2. Campo de Galois

$E = (\mathbb{Z}, \{+, \cdot\})$

→ $\exists\, e \quad +, \cdot$

→ $a * (b * c) = (a * b) * c$

→ $a + b = b + a$

$a \cdot b = b \cdot a$

→ $a * (b + c) = a * b + a * c$

$GF(n), \quad n = p^m$

$GF(2)$

$\{0, 1\}$

A	B	A + B	A
0	0	0	
0	1	1	
1	0	1	

$A \cdot B$

0

0

0

.

1 2 0

$GF(2)^5$

[0, 0, 0, 0, 0]

[0, 0, 0, 0, 1]