Examples of Finite fields

① $\mathbb{Z}_p = GF(p) = F_p$ p is prime

eg. $\mathbb{Z}_5$

×	1	2	3	4
1	①	2	3	4
2	2	4	①	3
3	3	①	4	2
4	4	3	2	①

+	0	1	2	3	4
0					
1				①	0
2					
3					
4					

② $GF(2^2) = F_{2^2}$

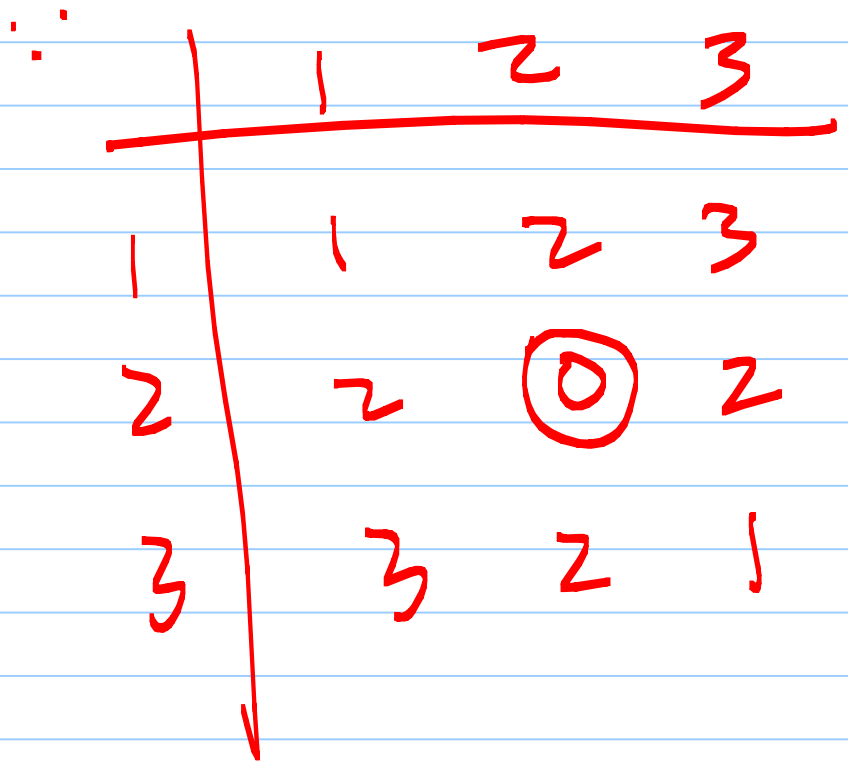
$$GF(2^2) \simeq \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, x, x+1\}$$

×	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

$$(x)^{-1} = x+1$$

$$(x+1)^{-1} = x$$

③ $\mathbb{Z}_4$ is not a field



not closed!

④ $F_{2^3} = GF(2^3)$

$F_{2^3} \simeq \mathbb{Z}_2[x]/(x^3+x+1)$ $\boxed{\simeq \mathbb{Z}_2[x]/(x^3+x^2+1)}$

$= \{ a_2x^2 + a_1x + a_0 \mid a_i \in \mathbb{Z}_2 \}$

$\therefore$ both x^3+x+1 and x^3+x^2+1

are irreducible!

Construct F_8 by using x^3+x+1

x	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	(1)						
x	x	x^2					
$x+1$	$x+1$	x^2+x	x^2+1				
x^2	x^2	$x+1$	x^2+x+1	x^2+x			
x^2+1	x^2+1	(1)	x^2	x	x^2+x+1		
x^2+x	x^2+x	x^2+x+1	(1)	x^2+1	$x+1$	x	
x^2+x+1	x^2+x+1	x^2+1	x	(1)	x^2+x	x^2	$x+1$

$h(x) = x^3 + x + 1$

x	001	010	011	100	101	110	111
001	001	010	011	100	101	110	111
010	010						
011	011						
100	100						
101	101						
110	110						
111	111						

⑤ $F_q = F_{3^2} = GF(3^2)$

as in Assignment 1.

⑥ $\mathbb{Z}_q$ is not a field (but a ring)

$\therefore$ 3 has no multiplicative inverse!

or $3 \times 3 = 0$ not closed!