Problem 1.1.

$$x + y = a$$

$\cancel{x = 0}$ $\quad$ $x = a$ $\quad$ $\cancel{x = 1}$ $\quad$ $\cancel{x = b}$

$\cancel{y = a}$ $\quad$ $y = 0$ $\quad$ $\cancel{y = b}$ $\quad$ $\cancel{y = 1}$

$by = 1$ $\quad$ $aa = b$ ✓ $\quad$ $a + a = 0$ $\quad$ $a\overset{1}{b} + b$

② $(\mathbb{Z}/8\mathbb{Z}, +, \cdot) \to 4$ can not be inversed

$(\mathbb{Z}/8\mathbb{Z}, +, \cdot)$ $\{1, 3, 5, 7\}$, $\boxed{\text{ok}}$

$((\mathbb{Z}/2\mathbb{Z})^3, +, \cdot)$

$(0,0,0), (0,0,1), (0,1,0)$, etc.

identity element for + $(0,0,0)$
inverse el lui-même

identity element for × $(1,1,1)$ $\boxed{\text{NO}}$
invers el

(3) 2^3 2, same characteristic

le characteristique : cb de fois to dois sommer un nb à lui-même pour obtenir l'inverse de la multiplicat°

(4)
$$\times 2 \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\to \begin{pmatrix} 0 & 2 & 2 \\ 1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 0 & 2 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$ pas lin indep.

5) $\boxed{p = 3}$

Problem 11.2

13
26
39
52
65

1.
$$\begin{array}{r} \\ +10 \\ +6 \end{array}\left(\begin{array}{cccc|c} 1 & 5 & 9 & 7 & 0 \\ 3 & 6 & 9 & 8 & 0 \\ 7 & 12 & 2 & 6 & 0 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{cc} 6 & 12 \\ 0 & \end{array}\right.$$

$$x_4 \begin{pmatrix} - \\ - \\ - \end{pmatrix}$$

13 possibilités

2. → vecteurs de tailles 4 mappés à des vecteurs de tailles 3

P

Problem 11.3

1

$$\begin{array}{c} \cdot 3 \\ \begin{pmatrix} 6 & 2 \\ 2 & 5 \\ 5 & 10 \end{pmatrix} \\ \cdot 3 \end{array}$$

$5 \cdot 3 = [15]_{13} = [2]_{2}$

$10 \cdot 3 = [30]_{13} = [4]_{13}$

non colinéaire

dimension : $n - 1 = 2$

n : dimension des vecteurs

1 : dimension ker

Cardinality : 13^2

deux vecteurs => forment un plan sauf qu'on ne va pas jusqu'à l'infini, on peut prendre 13 valeurs

(2)

3×2 $\qquad 6\alpha + 2\beta = 0$

$$\begin{pmatrix} 6 & 2 \\ 2 & 5 \\ 5 & 10 \end{pmatrix} \quad 2 \times 1$$

$$\to \begin{pmatrix} 1 & -8 \\ 2 & 5 \\ 5 & 10 \end{pmatrix}$$

$25 \% 13 =$

$$\to \begin{pmatrix} 1 & -8 \\ 10 & 12 \\ 10 & 7 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 5 \\ 0 & 5 \\ 10 & 7 \end{pmatrix} \to \begin{pmatrix} 1 & 5 \\ 0 & 5 \\ 0 & 9 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\gamma \begin{pmatrix} 6 \\ 2 \\ 5 \end{pmatrix} + \beta \begin{pmatrix} 2 \\ 5 \\ 10 \end{pmatrix}$$

$$\Rightarrow \begin{cases} v_1 = 6\alpha + 2\beta \quad] \cdot 5 \\ v_2 = 2\alpha + 5\beta \\ v_3 = 5\alpha + 10\beta \end{cases}$$

$$3v_2 = 6\alpha + 2\beta$$

$$3v_2 = v_1$$

$$v_1 - 3v_2 = 0 \quad \Leftrightarrow \quad v_1 = 10v_2$$

$$\alpha = \cancel{v_3 - 2v_2 = 5\alpha + 10\beta - 4\alpha - 10\beta}$$

$$\cdot 11 \begin{pmatrix} 6 & 2 & 5 \\ 2 & 5 & 10 \end{pmatrix} \rightarrow \begin{array}{ccc} \cdot 2 & \cdot 2 & \\ \end{array} \begin{pmatrix} 1 & 9 & 3 \\ 2 & 5 & 10 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 9 & 3 \\ 0 & 0 & 4 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 9 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\boxed{x_3 = 0}$$

et $\boxed{v_1 = 10 v_2}$

Problem 11.4

① 2 $\quad 2^2 = 4$

pas un choix arbitraire

②

+	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

$x+1$ ne peut pas être 1 sinon $x=0$!

therefore $y = x+1$!

③ characteristic is 2

$\Rightarrow 1+1=0$

$$3\times 6 \quad \boxed{6\times 1} \quad 3\times 1$$

$$\left(\begin{array}{cccccc|c} 1 & 0 & 0 & 1 & 1 & x+1 & 0 \\ 0 & 1 & 0 & 1 & x & x & 0 \\ 0 & 0 & 1 & 1 & x+1 & 1 & 0 \end{array}\right)$$

6   3

nb column avec pivots = Dim image + Dim ker

$\Rightarrow$ dim image $= 3$

Problem 11.5

① $\sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^{k}$

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$$\overset{0}{=} x^3 + (x+x+x)xy + (x+x+x)y^2 + y^2 = 0$$

$$= x^3 + y^2$$

$\dfrac{p!}{(p-k)!\,k!}$) on veut montrer que c'est un multiple de p

d

$$c = p \cdot \frac{(p-1)!}{(p-k)!\,k!}$$

$\longrightarrow$ comment savoir si c'est un entrer ?

on scait que p est premer, donc il ne se hove pao dans $(p-1)!$ ni $(p-k)!$ ni $k!$ donc comme c est enter alors d cussi.

$$(x+y)^p = x^p + y^p$$

$$+ \underbrace{p \sum_i u\, x^\alpha y^\beta}_{=0}$$

(2) $(F, +)$ has to be a commutative group.

also $(F \setminus \{0\}, \cdot)$ is a commutative group

therefore the cardinality of F_q is $q-1$

$\Rightarrow x^{q-1} \cdot x = 1 \cdot x = x$

3. Il faut vérifier si l'ordre de x dans le groupe est $p-1$

mais on est pas sûrs!

Ordre = $\forall x, \exists$ ordre t.q $x^{\text{ordre}} = 1$, et ordre divise q (la cardinalité de l'ensemble)

$q = p^m$ mais rien ne dit que

p est l'ordre de x dans q

4

$\underbrace{q=4}_{=2^2},\quad p=2$

$(x+y)^2 = x^2 + \overbrace{2xy}^{=0} + y^2 = x^2+y^2$

$(x-y)^2 = x^2 - \overbrace{2xy}^{=0} + y^2 = x^2+y^2$

$(x+y)^n = x^n + y^n$

$(x-y)^n = x^n - y^n$

mais ⊕ dredenent

$y \xrightarrow{+y} 0 \xrightarrow{+y} y \xrightarrow{+y} 0$, $0 \xrightarrow{-y} y$

$-y = y$

$\Rightarrow y = -y$

5 m linear eq

$$\begin{array}{c} \begin{pmatrix} \cdot & - & \cdot & \cdot & n \\ \cdot & - & \cdot & \cdot & \\ \cdot & - & \cdot & - & \\ \cdot & - & \cdot & \cdot & \end{pmatrix} = W \\ m \end{array}$$

$q = p^k$ $m \times n$ matrix

$=$

Par chaque equation on réduit l'espace d'unité. Penser à ça, on est dans $\mathbb{R}^3$ et :

- on ajoute $z = 0$ (on perd une dim)
- on ajoute $y = 0$ (on perd une dim)

Chaque équat° lin ajoute une contrainte

A cardinality of a set with dim $n-m$ is q^{n-m}

(think about the nb of possibilite).