$\boxed{\text{Exercice 3.9}}$ $\left((\mathbb{Z}/p\mathbb{Z})^\times, \times \right)$

$p = 7$ $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$

$(\mathbb{Z}/7\mathbb{Z}, +)$ 1 élément d'ordre 1 : $[0]_7$
6 éléments d'ordre 7 : les autres

$\text{card}(\mathbb{F}_p^\times) = p - 1 = 6$

ordres possibles $= 1, 2, 3, 6$

$m \in \mathbb{N}$
$m \geq 2$
$(\mathbb{Z}/m\mathbb{Z}, +)$ cyclique
$[1]_m$ est d'ordre m

élément	ordre dans $(\mathbb{Z}/7\mathbb{Z})^\times$
$[1]_7$	1 (élément neutre)
$[2]_7$	3
$[3]_7$	6
$[4]_7$	$\cancel{2}$ 3
$[5]_7$	6
$[6]_7$	2

$4^1 \equiv 4 \; [7]$
$4^2 \equiv 16 \; [7]$
$\equiv 2 \; [7]$
$4^3 \equiv 4 \times 4^2 \; [7]$
$\equiv 4 \times 2 \; [7]$
$\equiv 8 \; [7]$
$\equiv 1 \; [7]$

1 élément d'ordre 1
$\varphi(2) = 1$ élément d'ordre 2
$\varphi(3) = 2$ éléments d'ordre 3
$\varphi(6) = 2$ éléments d'ordre 6 (confirme que $(\mathbb{Z}/7\mathbb{Z})^\times$ est cyclique)

Exercice 3.11
(comment construire et manipuler des corps finis)

Rappel général : soit p un nombre premier et $n \in \mathbb{N}$, $n \geq 1$
On veut construire un corps fini de cardinal p^n et calculer explicitement dedans. Pour cela, il « suffit » d'exhiber un polynôme $P \in \mathbb{F}_p[X]$ irréductible de degré n. (on peut supposer P unitaire)
Alors $\mathbb{K} = \mathbb{F}_p[X]/\langle P \rangle$ est un corps fini de cardinal p^n
et la structure de quotient de $\mathbb{F}_p[X]$ permet des calculs explicite (il suffit de savoir calculer dans $\mathbb{F}_p[X]$ et de faire des divisions euclidiennes par P)

p quelconque
$n = 2$ liste des polynômes irréductibles unitaires de degré 2 de $\mathbb{F}_p[X]$?

liste des polynômes unitaires de degré 2 de $\mathbb{F}_p[X]$?

Ex : $p = 3$ $\quad X^2 + X + [1]_3 \qquad X^2 + [2]_3 X + [1]_3$

$X^2 + X + [2]_3 \qquad X^2 + [2]_3 X + [1]_3$

$P([0]_3) = [0]_3^2 + [1]_3 = [1]_3 \neq [0]_3$ $\quad X^2 + [1]_3 = P \qquad X^2 + [2]_3 \qquad X^2 + [1]_3 \in \mathcal{I}_{3,2}$

$P([1]_3) = [1]_3^2 + [1]_3 = [2]_3 \neq [0]_3$ $\quad X^2 + X \qquad X^2 + [2]_3 X$

X^2

$P([2]_3) = [2]_3^2 + [1]_3 = [5]_3 = [2]_3 \neq [0]_3$ $\quad \{ X^2 + [a]_3 \cdot X + [b]_3 \}_{a, b \in \mathbb{Z},\ 0 \leq a \leq 2,\ 0 \leq b \leq 2}$

$$\begin{aligned} \{0,1,2\} \times \{0,1,2\} &\longrightarrow \{\text{polynômes unitaires de degré 2 de } \mathbb{F}_3[X]\} \\ (a, b) &\longmapsto X^2 + [a]_3 \cdot X + [b]_3 \end{aligned}$$
est une bijection

(de manière générale, il y a p^n polynômes unitaires de degré n de $\mathbb{F}_p[X]$)

<u>Notation</u> Soit p premier, $n \in \mathbb{N}$, $n \geq 1$. On note $\mathcal{S}_{p,n}$ l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_p[X]$
$\mathrm{Card}(\mathcal{S}_{p,n}) = p^n$

Soit p premier, $n \in \mathbb{N}$, $n \geq 1$. On note $\mathcal{I}_{p,n}$ l'ensemble des polynômes unitaires IRRÉDUCTIBLES de degré n de $\mathbb{F}_p[X]$

<u>Notation</u> Soit p premier, $n \in \mathbb{N}$, $n \geq 1$. On note $\mathcal{S}_{p,n}$ l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_p[X]$

$\text{card}(\mathcal{S}_{p,n}) = p^n$

Soit p premier, $n \in \mathbb{N}$, $n \geq 1$. On note $\mathcal{I}_{p,n}$ l'ensemble des polynômes unitaires IRRÉDUCTIBLES de degré n de $\mathbb{F}_p[X]$

$\mathcal{I}_{3,2}$? $P \in \mathcal{S}_{3,2}$ Si X divise P, alors $P \notin \mathcal{I}_{3,2}$

Si $P \notin \mathcal{I}_{3,2}$ P s'écrit $(X-\alpha)(X-\beta)$ $\alpha, \beta \in \mathbb{F}_3$

Comme $\deg(P) = 2$, on a $P \in \mathcal{I}_{3,2}$

$\iff P([0]_3) \neq 0$ et $P([1]_3) \neq 0$ et $P([2]_3) \neq 0$

<u>Méthode générale (élémentaire) pour décrire $\mathcal{I}_{p,n}$</u> $\left(\begin{array}{l} p \text{ FIXÉ,} \\ n \text{ quelconque} \end{array}\right)$

- On détermine $\mathcal{I}_{p,2}$ et $\mathcal{I}_{p,3}$ en regardant quels éléments de $\mathcal{S}_{p,2}$ et $\mathcal{S}_{p,3}$ n'ont pas de racine dans $\mathbb{F}_p$
- Soit $n \geq 4$ quelconque. On suppose avoir déterminé $\mathcal{I}_{p,2}, \mathcal{I}_{p,3}, \dots, \mathcal{I}_{p,n-1}$

Pour déterminer $\mathcal{I}_{p,n}$, on regarde pour chaque élément P de $\mathcal{S}_{p,n}$ s'il est divisible par un élément de $\mathcal{I}_{p,r}$ pour tout $r \in \{1,2,3,\dots,n-1\}$

↳ en calculant les divisions euclidiennes

$P \in \mathcal{I}_{p,n} \iff \forall r \in \{1,2,3,\dots,n-1\}, \forall Q \in \mathcal{I}_{p,r}$, Q ne divise pas P

$n=4$ $P \in \mathcal{S}_{p,4}$ $\forall Q \in \mathcal{I}_{p,3}$, Q ne divise pas P

$P \in \mathcal{I}_{p,4} \iff \forall Q \in \mathcal{I}_{p,2}$, Q ne divise pas P

$\forall Q \in \mathcal{I}_{p,1}$, Q ne divise pas P

$P \in \mathcal{S}_{p,4}$

$P = \underset{\mathcal{I}_{p,3}}{Q} R$ alors $\deg(R) = 1$

↳ c'est-à-dire : $\forall \alpha \in \mathbb{F}_p$, $P(\alpha) \neq 0$

$\mathcal{I}_{p,1} = \{X - \alpha\}_{\alpha \in \mathbb{F}_p}$ $X - \alpha$ divise P $\iff P(\alpha) = 0$

<u>Exercice</u> : déterminer $\mathcal{I}_{2,2}$, $\mathcal{I}_{3,3}$, $\mathcal{I}_{2,4}$

$P = X^2 + [1]_3 \in \mathbb{F}_3[X]$

P est irréductible (dans $\mathbb{F}_3[X]$)

$\mathbb{K} = \mathbb{F}_3[X] / \langle P \rangle$ est un corps de cardinal $3^2 = 9$

$\pi : \mathbb{F}_3[X] \longrightarrow \mathbb{F}_3[X] / \langle P \rangle \qquad \alpha := \pi(X)$

On sait (cf chapitre 3) que $\{1, \alpha^{1 = \deg(P) - 1}\}$ est une base du $\mathbb{F}_3$-espace vectoriel $\mathbb{K}$

$$\varphi : \begin{array}{ccc} \mathbb{F}_3^2 & \longrightarrow & \mathbb{K} \\ (\beta_1, \beta_2) & \longmapsto & \beta_1 + \beta_2 \cdot \alpha \end{array} \qquad \text{bijection}$$

$$\mathbb{K} = \{ [0]_3, [1]_3, [2]_3, \\ [0]_3 + \alpha, [1]_3 + \alpha, [2]_3 + \alpha, \\ [0]_3 + [2]_3 \alpha, [1]_3 + [2]_3 \cdot \alpha, [2]_3 + [2]_3 \cdot \alpha \}$$

L'addition sur $\mathbb{K}$ (comme corps) c'est l'addition sur $\mathbb{K}$ vu comme $\mathbb{F}_3$-espace vectoriel

$$\forall \beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{F}_3, \quad (\beta_1 + \beta_2 \cdot \alpha) + (\beta_3 + \beta_4 \cdot \alpha) = (\beta_1 + \beta_3) + (\beta_2 + \beta_4)\alpha$$

<u>Exemple</u> : $([1]_3 + \alpha) + ([1]_3 + [2]_3 \cdot \alpha) = [2]_3 + [3]_3 \cdot \alpha$
$= [2]_3$

$\forall \beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{F}_3$
$\beta_1 + \beta_2 \alpha = \beta_3 + \beta_4 \alpha$
$\Leftrightarrow \begin{cases} \beta_1 = \beta_3 \\ \beta_2 = \beta_4 \end{cases}$

<u>Multiplication</u> $([1]_3 + \alpha) \times ([1]_3 + [2]_3 \cdot \alpha)$

$= [1]_3 \times [1]_3 + [1]_3 \times [2]_3 \times \alpha + \alpha \times [1]_3 + \alpha \times [2]_3 \times \alpha$

$= [1]_3 + ([2]_3 + [1]_3) \times \alpha + [2]_3 \times \alpha^2$

$= [1]_3 + [2]_3 \times \alpha^2$ → sous cette forme, le résultat n'est pas écrit sous la forme unique donnée par la bijection φ

$= \beta_1 + \beta_2 \times \alpha$

$\beta_1, \beta_2 \in \mathbb{F}_3 \quad \beta_1, \beta_2$?

Multiplication $([1]_3 + \alpha) \times ([1]_3 + [2]_3 \cdot \alpha)$

$$= [1]_3 \times [1]_3 + [1]_3 \times [2]_3 \times \alpha + \alpha \times [1]_3 + \alpha \times [2]_3 \times \alpha$$

$$= [1]_3 + ([2]_3 + [1]_3) \times \alpha + [2]_3 \times \alpha^2$$

$$= [1]_3 + [2]_3 \times \alpha^2)$$

→ sans cette forme, le résultat n'est pas écrit sous la forme unique donnée par la bijection φ

$$= \beta_1 + \beta_2 \times \alpha$$

$\beta_1, \beta_2 \in \mathbb{F}_3$ $\quad \beta_1, \beta_2$?

$\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[X] / \langle P \rangle$ $\qquad P = X^2 + [1]_3$

$\alpha = \pi(X)$

$P \in \mathrm{Ker}(\pi)$ $\qquad \pi(X^2 + [1]_3) = [0]_3$

fait crucial

donc $\pi(X)^2 + [1]_3 = [0]_3$

donc $\alpha^2 + [1]_3 = [0]_3$

donc $\alpha^2 = [2]_3$

$$[1]_3 + [2]_3 \times \alpha^2 = [1]_3 + [2]_3 \times [2]_3 = [2]_3$$

<u>Exercice</u> Dresser la table de multiplication de $\mathbb{K}$

Exhiber un générateur de $\mathbb{K}^\times$