

Corrigé :

Partie I :

1. On a : $\forall i \in \llbracket 1, p-1 \rrbracket, p \times \binom{p-1}{i-1} = i \times \binom{p}{i}$. Donc p divise $i \times \binom{p}{i}$. Or, p étant premier, il ne peut diviser i .

Donc p divise $\binom{p}{i}$, c'est-à-dire que $\boxed{\binom{p}{i} \equiv 0 \pmod{p}}$.

2. On note respectivement 0_K et 1_K les éléments neutres pour l'addition et la multiplication dans K .

On pose : $\phi : \mathbb{Z} \longrightarrow K$ définie par : $\forall k \in \mathbb{Z}, \phi(k) = k.1_K$.

Dire que $\mathbb{F}_p \subset K$ signifie qu'il existe $\delta : \mathbb{F}_p \longrightarrow K$ morphisme injectif de corps.

Donc : $\delta(\bar{0}) = 0_K, \delta(\bar{1}) = 1_K$ et $\forall k \in \mathbb{Z}, \delta(\bar{k}) = \delta(k \cdot \bar{1}) = k \delta(\bar{1}) = k.1_K$.

En particulier, si $k \in p\mathbb{Z}, \bar{k} = \bar{0}$ donc $k.1_K = 0_K$.

D'où, par la formule du binôme : $\forall (x, y) \in K^2, (x+y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} = x^p + \sum_{i=1}^{p-1} \binom{p}{i} \times 1_K \times x^i y^{p-i} + y^p$.

Par la question 1. et ce qui précède, pour tout $i \in \llbracket 1, p-1 \rrbracket, \binom{p}{i} \times 1_K = 0_K$. $\text{Donc } \forall (x, y) \in K^2, (x+y)^p = x^p + y^p$.

Supposons que, pour un $m \in \mathbb{N}^*$, on ait : $\forall (x_1, \dots, x_m) \in K^m, \left(\sum_{i=1}^m x_i\right)^p = \sum_{i=1}^m x_i^p$.

Alors : $\forall (x_1, \dots, x_{m+1}) \in K^{m+1}, \left(\sum_{i=1}^{m+1} x_i\right)^p = \left(\sum_{i=1}^m x_i\right)^p + x_{m+1}^p$ d'après ce qui a été vu plus haut.

Puis, par hypothèse : $\left(\sum_{i=1}^{m+1} x_i\right)^p = \sum_{i=1}^{m+1} x_i^p$. Donc, par récurrence : $\forall m \in \mathbb{N}^*, \forall (x_1, \dots, x_m) \in K^m, \left(\sum_{i=1}^m x_i\right)^p = \sum_{i=1}^m x_i^p$.

De façon évidente, $\left(\sum_{i=1}^m x_i\right)^{p^0} = \sum_{i=1}^m x_i^{p^0}$. On suppose ensuite que, pour un $n \in \mathbb{N}$, on a : $\forall m \in \mathbb{N}^*$,

$\forall (x_1, \dots, x_m) \in K^m, \left(\sum_{i=1}^m x_i\right)^{p^n} = \sum_{i=1}^m x_i^{p^n}$. Donc : $\left(\sum_{i=1}^m x_i\right)^{p^{n+1}} = \left(\left(\sum_{i=1}^m x_i\right)^{p^n}\right)^p = \left(\sum_{i=1}^m x_i^{p^n}\right)^p = \sum_{i=1}^m x_i^{p^{n+1}}$ d'après la

proposition précédente. Par récurrence sur n , on a : $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^*, \forall (x_1, \dots, x_m) \in K^m, \left(\sum_{i=1}^m x_i\right)^{p^n} = \sum_{i=1}^m x_i^{p^n}$.

Soit alors $R \in \mathbb{F}_p[X]$; si $R \neq 0$, il existe $m \in \mathbb{N}$ et $(a_0, \dots, a_m) \in (\mathbb{F}_p)^{m+1}$ tels que : $R = \sum_{k=0}^m a_k X^k$.

D'après les calculs précédents : $\forall x \in K, (R(x))^{p^n} = \sum_{k=0}^m a_k^{p^n} x^{k p^n}$. Mais, par le petit théorème de Fermat,

pour tout $k \in \mathbb{Z}, k^p \equiv k \pmod{p}$, donc, par récurrence immédiate : $\forall n \in \mathbb{N}, k^{p^n} \equiv k \pmod{p}$.

Donc : $\forall k \in \llbracket 0, m \rrbracket, a_k^{p^n} = a_k$ et $(R(x))^{p^n} = \sum_{k=0}^m a_k (x^{p^n})^k$, soit $(R(x))^{p^n} = R(x^{p^n})$ (évident si $R = 0$).

Partie II :

On note 0 et 1 respectivement les éléments neutres pour l'addition et la multiplication dans k .

1.a. Soient P, R, S et T dans $k[X]$ tels que : $\overline{P} = \overline{T}$ et $\overline{R} = \overline{S}$. Alors $P - T \in (Q)$ et $R - S \in (Q)$.

Comme (Q) est un sous-groupe additif de $k[X]$, $P + R - (T + S) \in (Q)$ donc $\overline{P + R} = \overline{T + S}$.

On définit donc bien une loi interne en posant $\overline{P} + \overline{R} = \overline{P + R}$.

De même, il existe P_1 et P_2 dans $k[X]$ tels que : $P = T + P_1 \times Q$ et $R = S + P_2 \times Q$.

Donc $PR = TS + (TP_2 + SP_1 + P_1P_2Q) \times Q$ donc $PR - TS \in (Q)$, donc $\overline{P \times R} = \overline{T \times S}$.

On définit donc bien une deuxième loi interne en posant $\overline{P} \times \overline{R} = \overline{P \times R}$.

Enfin, $\lambda P - \lambda T = \lambda(P - T) \in (Q)$ donc $\overline{\lambda P} = \overline{\lambda T}$ donc on définit bien une loi externe à éléments dans k en posant

$$\lambda \overline{P} = \overline{\lambda P}.$$

A l'aide de ces définitions et de la structure de k -algèbre de $k[X]$, on vérifie aisément que $+$ est associative et commutative dans A . $\overline{0}$ est l'élément neutre pour $+$ dans A et le symétrique de \overline{P} pour $+$ dans A est égal à $-\overline{P}$.

De même, \times est associative, commutative et distributive par rapport à $+$ dans A . $\overline{1}$ est l'élément neutre pour \times dans A . Enfin, on vérifie sans problème les quatre propriétés qui permettent d'avoir la structure de k -espace vectoriel de A .

Donc $(A, +, \times, \cdot)$ est une k -algèbre commutative et unitaire.

De plus, par les définitions des opérations $+$ et \times , $\Phi : P \mapsto \overline{P}$ est un morphisme d'algèbres de $k[X]$ dans A .

Par restriction, $\phi : \lambda \mapsto \overline{\lambda}$ est un morphisme d'anneaux de k dans A .

De plus, $\overline{\lambda} = \overline{0} \Leftrightarrow \lambda \in (Q) \Leftrightarrow \exists P \in k[X], \lambda = P \times Q$. Mais, comme $\deg(Q) \geq 1$, cette égalité n'est possible que si $P = 0$ donc $\lambda = 0$. On a $\text{Ker}(\phi) = \{0\}$ donc ϕ est injectif.

1.b. Soit $B \in A$. Il existe $R \in k[X]$ tel que $B = \overline{R}$. On écrit $R = \sum_{i=0}^n a_i X^i$ avec $(a_0, \dots, a_n) \in k^{n+1}$.

Comme Φ est un morphisme d'algèbres : $B = \sum_{i=0}^n \overline{a_i} \overline{X^i}$. Mais, comme on identifie k et $\phi(k)$, on obtient :

$$B = \sum_{i=0}^n a_i \overline{X^i} = R(\overline{X}). \text{ Donc : } \boxed{\forall B \in A, \exists R \in k[X], B = R(\overline{X})}.$$

1.c. Posons $d = \deg(Q)$. $d \geq 1$. Soit $B \in A$; il existe $P \in k[X]$ tel que $B = \overline{P}$.

Par division euclidienne : $\exists!(Q_1, R) \in (k[X])^2, P = Q_1 Q + R$ et $\deg(R) < d$.

Donc $R = \sum_{i=0}^{d-1} a_i X^i$ avec $(a_0, \dots, a_{d-1}) \in k^d$ et $\overline{P} = \overline{R} = \sum_{i=0}^{d-1} a_i \overline{X^i}$ (d'après la question précédente).

Donc $(1, \overline{X}, \dots, \overline{X}^{d-1})$ est une famille génératrice de A .

De plus : $\sum_{i=0}^{d-1} a_i \overline{X^i} = \overline{0} \Leftrightarrow \sum_{i=0}^{d-1} a_i X^i \in (Q) \Leftrightarrow \sum_{i=0}^{d-1} a_i X^i = 0$ car, si $P \in (Q) \setminus \{0\}$, $Q|P$ et $\deg(P) \geq \deg(Q)$.

Puis $\sum_{i=0}^{d-1} a_i X^i = 0 \Leftrightarrow (a_0, \dots, a_{d-1}) = (0, \dots, 0)$. Donc $(1, \overline{X}, \dots, \overline{X}^{d-1})$ est libre.

Donc $(1, \overline{X}, \dots, \overline{X}^{d-1})$ est une base de A et $\dim(A) = d = \deg(Q)$.

2.a. \overline{R} est inversible dans A ssi $\exists \overline{P} \in A, \overline{P} \times \overline{R} = \overline{1} \Leftrightarrow PR - 1 \in (Q) \Leftrightarrow \exists U \in k[X], PR - 1 = QU$
 $\Leftrightarrow \exists (P, U) \in (k[X])^2, PR - QU = 1 \Leftrightarrow R \wedge Q = 1$ d'après le théorème de Bézout.

Donc $R \in k[X]$ vérifie \overline{R} est inversible dans A ssi R est premier avec Q .

2.b. A est un corps ssi tout élément non nul \bar{R} est inversible dans A.

D'après la question précédente, A est un corps ssi tout polynôme de $k[X]$ qui n'est pas multiple de Q, est premier avec Q. Donc A est un corps ssi Q est irréductible sur k.

On remarque qu'un polynôme de degré 2 de $k[X]$ n'est pas irréductible sur k ssi il est divisible par un polynôme de degré 1 ssi il admet une racine dans k.

Donc un polynôme de degré 2 de $k[X]$ est irréductible sur k ssi il n'admet aucune racine dans k.

Si $k = \mathbb{F}_2$, $\bar{0}^2 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$ et $\bar{1}^2 + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}$. Donc $X^2 + X + 1$ est irréductible sur \mathbb{F}_2 .

D'après ce qui précède, $\mathbb{F}_2/(X^2 + X + 1)$ est un corps.

Si $k = \mathbb{F}_{11}$, on a le tableau suivant :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
$x^2 + 1$	$\bar{1}$	$\bar{2}$	$\bar{5}$	$\bar{10}$	$\bar{6}$	$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{10}$	$\bar{5}$	$\bar{2}$

On constate que $X^2 + 1$ n'a pas de racine dans \mathbb{F}_{11} , donc il est irréductible sur \mathbb{F}_{11} .

D'après ce qui précède, $\mathbb{F}_{11}/(X^2 + 1)$ est un corps.

Si $k = \mathbb{F}_{13}$, $\bar{5}^2 + \bar{1} = \bar{0}$ donc $X^2 + 1 = (X - \bar{5})(X + \bar{5})$ et $X^2 + 1$ n'est pas irréductible sur \mathbb{F}_{13} .

Donc $\mathbb{F}_{13}/(X^2 + 1)$ n'est pas un corps.

Partie III :

1. D'après **II.1.c.**, K est un espace vectoriel sur \mathbb{F}_p de dimension d. Il est donc isomorphe à $(\mathbb{F}_p)^d$.

Donc $|K| = |(\mathbb{F}_p)^d| = p^d$. D'où $|K^*| = p^d - 1$.

Or, (K^*, \times) est un groupe et, par théorème, dans un groupe fini G de cardinal n, pour tout élément $g \in G$, on a :

$g^n = e$. Donc : $\forall y \in K^*, y^{p^d-1} = 1$.

Par hypothèse, il existe $m \in \mathbb{N}^*$ tel que $m d = n$. D'après la question précédente : $\bar{X}^{p^d-1} = 1$ donc $\bar{X}^{p^d} = \bar{X}$.

On vérifie ensuite, par récurrence immédiate sur k, que $\bar{X}^{p^{dk}} = \bar{X}$. En particulier si $k = m$, on a : $\bar{X}^{p^n} = \bar{X}$;

mais ceci équivaut à $\bar{X}^{p^n} - \bar{X} = 0$, soit Q divise $X^{p^n} - X$.

3.a. D'après ce qui précède, si Q divise $X^{p^n} - X$, alors $\bar{X}^{p^n} = \bar{X}$.

D'après **II.1.b.**, pour tout $y \in K$, il existe $R \in \mathbb{F}_p[X]$ tel que $y = R(\bar{X})$.

De plus, d'après **II.1.a.**, $\mathbb{F}_p \subset K$. En appliquant **I.2.**, il vient que : $y^{p^n} = R(\bar{X}^{p^n}) = R(\bar{X}) = y$.

Donc : $\forall y \in K, y^{p^n} = y$.

3.b. On peut écrire $n = q d + r$ avec $(q, r) \in \mathbb{N} \times [0, d - 1]$. D'après la question **1.**, pour tout $y \in K^*$, $y^{p^d} = y$.

Par récurrence immédiate sur q : $y^{p^{dq}} = y$ donc $y^{p^n} = y^{p^r}$. Mais, d'après **a.**, $y^{p^n} = y$ donc $y^{p^r} = y$.

Puis, comme K est un corps : $\forall y \in K^*, y^{p^r-1} = 1$.

3.c. Le polynôme $B = Y^{p^r-1} - 1$ est de degré $p^r - 1$ sauf si $r = 0$ auquel cas $B = 0$.

Donc, si $r \neq 0$, B a au plus $p^r - 1$ racines. Or, d'après la question précédente, B admet tous les éléments de K^* comme racines soit $p^d - 1$ racines. Or, si $r \neq 0$, $p^d - 1 > p^r - 1$: contradiction.

Donc $X^{p^r-1} - 1$ est le polynôme nul et $r = 0$ donc $d \mid n$.

4. Soit $P = X^{p^n} - X$. Supposons que P possède un facteur carré. Il existe donc $Q \in \mathbb{F}_p[X]$ et $Q_1 \in \mathbb{F}_p[X]$ tels que $P = Q^2 Q_1$ et $\deg(Q) \geq 1$. Alors son polynôme dérivé vaut $P' = 2QQ_1Q' + Q_1' Q^2$ donc $Q \mid P'$; mais, d'autre part, $P' = p^n X^{p^n-1} - 1 = -1$ car $p^n = 0$ (car $\mathbb{F}_p \subset K$). D'où $Q \mid (-1)$: impossible. Donc P est sans facteur carré.

Comme P est unitaire, par théorème, il se décompose en produit de polynômes unitaires irréductibles sur \mathbb{F}_p . Or, d'après les questions 2. et 3., Q est un polynôme irréductible sur \mathbb{F}_p qui divise P ssi $\deg(Q) \mid n$.

$$X^{p^n} - X = \prod_{d \mid n} \prod_{Q \in K_p^d} Q.$$

Partie IV

1. D'après III.4., $\deg(P) = p^n = \sum_{d \mid n} \sum_{Q \in K_p^d} \deg(Q)$. Mais, pour tout $Q \in K_p^d$, $\deg(Q) = d$ et $|K_p^d| = I_p^d$.

Donc : $p^n = \sum_{d \mid n} d I_p^d$.

2. En particulier : $\forall d \geq 1, p^d = I_p^1 + \dots + d I_p^d$. Donc $\forall d \geq 1, p^d \geq d I_p^d$ car $\sum_{\substack{k \mid d \\ k \neq d}} k I_p^k \geq 0$.

Supposons que $I_p^n = 0$. Alors : $p^n = \sum_{\substack{d \mid n \\ d \neq n}} d I_p^d \leq \sum_{\substack{d \mid n \\ 1 \leq d < n}} p^d \leq \sum_{d=1}^{n-1} p^d = p \times \frac{p^{n-1} - 1}{p - 1}$ car $p \geq 2$.

Mais $p \times \frac{p^{n-1} - 1}{p - 1} = \frac{p^n - p}{p - 1} \leq p^n - p < p^n$: contradiction. Donc $I_p^n \geq 1$.

3. Il y a p polynômes irréductibles sur \mathbb{F}_p unitaires de degré 1, ce sont les polynômes $X - x$ où $x \in \mathbb{F}_p$.

Donc $I_p^1 = p$.

Si n est premier, ses seuls diviseurs sont 1 et n. Donc on a : $p^n = I_p^1 + n I_p^n$, soit $I_p^n = \frac{1}{n}(p^n - 1)$.

D'après la formule (*), si $n = 1$, on retrouve $I_p^1 = p$. Puis, si on suppose connus tous les I_p^k pour $k \in [1, n - 1]$ avec un $n \geq 2$, on a : $n I_p^n = p^n - \sum_{\substack{d \mid n \\ d < n}} d I_p^d$ donc on peut calculer I_p^n .

La formule (*) permet donc le calcul de tous les nombres I_p^n , par récurrence forte.

4.a. Un polynôme unitaire de degré 2 de \mathbb{F}_p est de la forme $X^2 + aX + b$ avec $(a, b) \in (\mathbb{F}_p)^2$. Comme $|\mathbb{F}_p| = p$, il y a donc p^2 polynômes unitaires de degré 2 à coefficients dans \mathbb{F}_p . Un tel polynôme n'est pas irréductible ssi il est de la forme $(X - \alpha)^2$ avec $\alpha \in \mathbb{F}_p$ ou de la forme $(X - \alpha)(X - \beta)$ avec α et β dans \mathbb{F}_p et distincts. Or, il y a p polynômes de la forme $(X - \alpha)^2$ et $\frac{p(p-1)}{2}$ polynômes de la forme $(X - \alpha)(X - \beta)$ avec α et β distincts.

Donc $I_p^2 = p^2 - p - \frac{p(p-1)}{2}$, soit $I_p^2 = \frac{p(p-1)}{2}$.

D'après ce qui précède, il n'y a qu'un seul polynôme irréductible de degré 2 unitaire sur \mathbb{F}_2 , c'est le polynôme $X^2 + X + 1$ (cf. II.2.b.).

4.b. On note C l'ensemble des carrés de \mathbb{F}_p^* . $C \subset \mathbb{F}_p^*$ car, si $a \in \mathbb{F}_p$, $a \neq \bar{0} \Rightarrow a^2 \neq \bar{0}$ (\mathbb{F}_p est un corps donc est intègre). $\bar{1} = \bar{1}^2 \in C$.

Soient p_1 et q_1 dans C. Alors : $\exists (p, q) \in (\mathbb{F}_p^*)^2, p_1 = p^2$ et $q_1 = q^2$. Comme \mathbb{F}_p^* est un groupe, q et q_1 sont inversibles et $q_1^{-1} = (q^{-1})^2$ donc $p_1 q_1^{-1} = (p q^{-1})^2 \in C$. Par caractérisation, C est un sous-groupe de \mathbb{F}_p^* .

De plus, si $a \in \mathbb{F}_p^*$, $x^2 = a^2 \Leftrightarrow x^2 - a^2 = 0 \Leftrightarrow (x - a)(x + a) = 0 \Leftrightarrow x \in \{a, -a\}$ et $a \neq -a$ car $p \neq 2$ et $a \neq \bar{0}$.

Donc tout carré non nul a exactement 2 "racines carrées". Comme $|\mathbb{F}_p^*| = p - 1$ (est pair car p premier et $p \neq 2$),

$$|C| = \frac{p-1}{2}$$

4.c. $p \neq 2$ donc $\bar{2}$ est inversible dans \mathbb{F}_p . Soit $P = X^2 + aX + b \in \mathbb{F}_p[X]$. On a : $P = (X + a\bar{2}^{-1}) - (b - (a\bar{2}^{-1})^2)$. P est irréductible dans $\mathbb{F}_p[X]$ ssi $(b - (a\bar{2}^{-1})^2) \notin (C \cup \{\bar{0}\})$ ssi $b = (a\bar{2}^{-1})^2 + c$ avec $c \notin (C \cup \{\bar{0}\})$.

Donc P est irréductible sur \mathbb{F}_p ssi $a \in \mathbb{F}_p$ (p choix possibles) et $b = (a\bar{2}^{-1})^2 + c$ avec $c \notin (C \cup \{\bar{0}\})$ ($p - \frac{p+1}{2}$

choix possibles). Donc $I_p^2 = p \times (p - \frac{p+1}{2}) = \frac{p(p-1)}{2}$. On retrouve le résultat de 4.a..

Dans \mathbb{F}_5 , les carrés sont $\bar{0}$, $\bar{1}$ et $\bar{4}$. Voici le tableau donnant les b possibles (on a $\bar{2}^{-1} = \bar{3}$) :

$c \setminus a$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{3}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{4}$	$\bar{4}$	$\bar{2}$

D'où les polynômes irréductibles de degré 2 unitaires de $\mathbb{F}_5[X]$: $X^2 + \bar{2}$, $X^2 + \bar{3}$, $X^2 + X + \bar{1}$, $X^2 + X + \bar{2}$, $X^2 + \bar{2}X + \bar{3}$, $X^2 + \bar{2}X + \bar{4}$, $X^2 + \bar{3}X + \bar{3}$, $X^2 + \bar{3}X + \bar{4}$, $X^2 + \bar{4}X + \bar{1}$ et $X^2 + \bar{4}X + \bar{2}$.

Partie V

1. Comme $(\mathbb{C}, +)$ est un groupe commutatif, $(\mathcal{F}, +)$ est un groupe commutatif (addition usuelle des fonctions).

La loi $*$ est interne par définition. De plus : $\forall n \in \mathbb{N}^*, \forall d \in \mathbb{N}^*, d$ divise n ssi $d' = \frac{n}{d}$ divise n .

Donc : $\forall n \in \mathbb{N}^*, (f * h)(n) = \sum_{d|n} f(d)h(\frac{n}{d}) = \sum_{d'|n} f(\frac{n}{d'})h(d') = (h * f)(n)$. La loi $*$ est commutative.

Soient f, g et h dans \mathcal{F} . On a : $\forall n \in \mathbb{N}^*, ((f * h) * g)(n) = \sum_{d|n} (f * h)(d)g(\frac{n}{d}) = \sum_{d|n} \sum_{k|d} f(k)h(\frac{d}{k})g(\frac{n}{d})$.

Or, si $d|n$ et $k|d$, alors il existe $m \in \mathbb{N}^*$ et $q \in \mathbb{N}^*$ tels que : $n = m d$ et $d = q k$ donc $n = m q k$, $\frac{n}{d} = m$ et $\frac{d}{k} = q$.

Réciproquement, si $(m, q, k) \in (\mathbb{N}^*)^3$ vérifie $m q k = n$, on peut poser $d = q k$ et l'on a : $d|n$ et $k|d$.

Donc :
$$\sum_{d|n} \sum_{k|d} f(k) h\left(\frac{d}{k}\right) g\left(\frac{n}{d}\right) = \sum_{\substack{1 \leq k, q, m \leq n \\ kqm=n}} f(k) h(q) g(m) = \sum_{k|n} f(k) \sum_{q|(n/k)} h(q) g\left(\frac{n}{kq}\right) = \sum_{k|n} f(k) (h * g)\left(\frac{n}{k}\right).$$

D'où : $\forall n \in \mathbb{N}^*, ((f * h) * g)(n) = (f * (g * h))(n)$. Donc la loi $*$ est associative.

On a également : $\forall n \in \mathbb{N}^*, (f * (h + g))(n) = \sum_{k|n} f(k) (h + g)\left(\frac{n}{k}\right) = \sum_{k|n} f(k) h\left(\frac{n}{k}\right) + \sum_{k|n} f(k) g\left(\frac{n}{k}\right)$ donc

$\forall n \in \mathbb{N}^*, (f * (h + g))(n) = (f * h)(n) + (f * g)(n)$: la loi $*$ est distributive sur la loi $+$.

Posons $\chi : \mathbb{N}^* \longrightarrow \mathbb{C}$ défini par : $\chi(1) = 1$ et $\chi(n) = 0$ si $n \in \mathbb{N}^* \setminus \{1\}$.

Il est clair que : $\forall n \in \mathbb{N}^*, (f * \chi)(n) = f(n)$. Donc $*$ admet χ comme élément neutre.

Donc $(\mathcal{F}, +, *)$ est un anneau commutatif et unitaire.

2. Soit $f \in \mathcal{F}$ avec f inversible. Il existe donc $g \in \mathcal{F}$ telle que : $\forall n \in \mathbb{N}^*, (f * g)(n) = \chi(n)$. En particulier : $f(1) g(1) = 1$ donc $f(1) \neq 0$.

Réciproquement, soit $f \in \mathcal{F}$ telle que $f(1) \neq 0$. On cherche $g \in \mathcal{F}$ telle que : $\forall n \in \mathbb{N}^*, (f * g)(n) = \chi(n)$.

On a alors $f(1) g(1) = 1$, soit $g(1) = \frac{1}{f(1)}$.

On raisonne par récurrence forte sur n . Supposons que, pour un $n \in \mathbb{N}^*$ et pour tout $p \in \llbracket 1, n \rrbracket$, on connaisse $g(p)$.

On a $n + 1 \geq 2$ donc on doit avoir $(g * f)(n + 1) = \chi(n + 1) = 0$, soit $\sum_{d|(n+1)} g(d) f\left(\frac{n+1}{d}\right) = 0$, soit

$f(1) g(n + 1) = - \sum_{\substack{d|(n+1) \\ d < (n+1)}} g(d) f\left(\frac{n+1}{d}\right)$. Donc $g(n + 1) = - \sum_{\substack{d|(n+1) \\ d < (n+1)}} \frac{g(d)}{f(1)} f\left(\frac{n+1}{d}\right)$ est déterminé.

Par récurrence forte, si $f(1) \neq 0$, il existe $g \in \mathcal{F}$ telle que : $\forall n \in \mathbb{N}^*, (f * g)(n) = \chi(n)$. Donc f est inversible.

D'où : $f \in \mathcal{F}$ est inversible ssi $f(1) \neq 0$.

3.a. On a : $(\mu * \text{cst}_1)(1) = \mu(1) \times (\text{cst}_1)(1) = 1$.

Soit $n \geq 2$. D'après la décomposition en produit d'irréductibles, $n = \prod_{i=1}^k p_i^{\alpha_i}$ avec $k \in \mathbb{N}^*$, les p_i premiers avec $p_1 < p_2 < \dots < p_k$ et $\alpha_i \in \mathbb{N}^*$ pour tout i de 1 à k . Donc $d | n$ ssi $d = \prod_{i=1}^k p_i^{\beta_i}$ et, pour tout i de 1 à k , $\beta_i \in \llbracket 0, \alpha_i \rrbracket$.

Si $\beta_i \geq 2$, $\mu(d) = 0$. On a donc : $(\mu * \text{cst}_1)(n) = \sum_{d|n} \mu(d) = \mu(1) + \sum_{j=1}^k \sum_{1 \leq i_1 < \dots < i_j \leq k} \mu(p_{i_1} \dots p_{i_j}) = 1 + \sum_{j=1}^k \binom{k}{j} (-1)^j$, soit

$(\mu * \text{cst}_1)(n) = (1 + (-1))^k = 0$ par la formule du binôme. D'où : $\mu * \text{cst}_1 = \chi$.

3.b. Si f et g sont liées par une relation (**), on a : $g * \text{cst}_1 = f = \text{cst}_1 * g$.

Par associativité : $(\mu * \text{cst}_1) * g = \mu * f$ c'est-à-dire : $g = \mu * f$. Donc : $\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$.

4. On pose : $\forall n \in \mathbb{N}^*, f(n) = p^n$ et $g(n) = n I_p^n$. D'après la partie IV, on a : $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$.

En appliquant le résultat de la question précédente : $\forall n \in \mathbb{N}^*, n I_p^n = \sum_{d|n} \mu(d) p^{n/d}$, soit $I_p^n = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$.

Partie VI

1. D'après la partie **IV**, il existe des polynômes unitaires irréductibles de degré n sur \mathbb{F}_p . Soit Q l'un d'eux. D'après la partie **II** et la question **III.1.**, $\mathbb{K} = \mathbb{F}_p[X]/(Q)$ est un corps de cardinal p^n .

2.a. Soit $\varphi : \mathbb{Z} \longrightarrow \mathbb{K}'$ définie par : $\forall m \in \mathbb{Z}, \varphi(m) = m \times 1$. φ est un morphisme d'anneaux donc $\text{Ker}(\varphi)$ est un idéal de \mathbb{Z} . Si $\text{Ker}(\varphi) = \{0\}$, φ est injectif donc \mathbb{K}' est infini, ce qui est faux. Donc, par caractérisation des idéaux de \mathbb{Z} , il existe $q \in \mathbb{N}^*$ tel que $\text{Ker}(\varphi) = q\mathbb{Z}$. $q = 1 \Rightarrow \text{Ker}(\varphi) = \mathbb{Z} \Rightarrow 1 = 0$: impossible. Donc $q \geq 2$.

S'il existe $(d, r) \in (\mathbb{N}^*)^2$ tel que $q = dr$, on a : $\varphi(q) = 0 = \varphi(d) \times \varphi(r)$ donc $\varphi(d) = 0$ ou $\varphi(r) = 0$ car \mathbb{K}' est un corps donc est intègre. Donc $d \in \text{Ker}(\varphi)$ ou $r \in \text{Ker}(\varphi)$, donc $q \mid d$ ou $q \mid r$, c'est-à-dire $q = d$ ou $q = r$ car $d \mid q$ et $r \mid q$.

Donc q est un nombre premier. Par définition de φ , **pour tout $y \in \mathbb{K}'$, $qy = (q \times 1) \times y = 0$.**

2.b. Soit $y \in \mathbb{K}' \setminus \{0\}$; $(\{0, y, \dots, (q-1)y\}, +)$ est un sous-groupe de $(\mathbb{K}', +)$ de cardinal q .

En effet, si $ky = my$ avec $(k, m) \in \llbracket 0, q-1 \rrbracket^2$, $(k-m)y = 0$ donc $(k-m) \times 1 = 0$ puisque $y \neq 0$.

Donc $(k-m) \in \text{Ker}(\varphi)$ donc $q \mid (k-m)$ donc $k-m = 0$ car $(k-m) \in \llbracket 1-q, q-1 \rrbracket$.

Or, par théorème, l'ordre de tout élément d'un groupe fini divise l'ordre du groupe. Donc $q \mid p^n$.

Comme q est premier, $q \mid p$ donc **$q = p$** car p est également premier.

2.c. On rappelle que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On pose alors : $\forall \bar{k} \in \mathbb{F}_p, \sigma(\bar{k}) = \varphi(k)$.

On a : $\forall \bar{k} \in \mathbb{F}_p, \forall \bar{m} \in \mathbb{F}_p, \bar{k} = \bar{m} \Leftrightarrow (k-m) \in p\mathbb{Z} = \text{Ker}(\varphi) \Leftrightarrow \varphi(k) = \varphi(m) \Leftrightarrow \sigma(\bar{k}) = \sigma(\bar{m})$.

Donc σ est bien définie et elle est injective.

Comme φ est un morphisme d'anneaux et par définition des lois $+$ et \times dans $\mathbb{Z}/p\mathbb{Z}$, on a :

$\forall \bar{k} \in \mathbb{F}_p, \forall \bar{m} \in \mathbb{F}_p, \sigma(\bar{k} + \bar{m}) = \sigma(\overline{k+m}) = \varphi(k+m) = \varphi(k) + \varphi(m) = \sigma(\bar{k}) + \sigma(\bar{m})$ et

$\sigma(\bar{k} \times \bar{m}) = \sigma(\overline{k \times m}) = \varphi(k \times m) = \varphi(k) \times \varphi(m) = \sigma(\bar{k}) \times \sigma(\bar{m})$. De plus, $\sigma(\bar{1}) = 1$.

Donc σ est un morphisme d'anneaux. Comme \mathbb{F}_p est un corps, **$\sigma(\mathbb{F}_p)$ est un sous-corps de \mathbb{K}'** et **σ induit donc un isomorphisme de corps de \mathbb{F}_p sur $\sigma(\mathbb{F}_p)$.**

Si τ est un isomorphisme de corps de \mathbb{F}_p sur un sous-corps F' de \mathbb{K}' , on doit avoir : $\tau(\bar{1}) = 1 = \varphi(1)$ et, pour tout $\bar{k} \in \mathbb{F}_p, \tau(\bar{k}) = \tau(k \times \bar{1}) = k \tau(\bar{1}) = k \times 1 = \varphi(k)$. Donc $\tau = \sigma$. **D'où l'unicité.**

3. Il est clair que : $eval_y(1) = 1$. On utilise les propriétés de morphisme d'anneaux de σ .

Pour Q et R dans $\mathbb{F}_p[X]$: $eval_y(Q + R) = (Q + R)^\sigma(y)$. Si $Q = \sum_{k=0}^{+\infty} a_k X^k$ et $R = \sum_{k=0}^{+\infty} b_k X^k$ avec $(a_k)_k$ et $(b_k)_k$ des

familles presque nulles d'éléments de \mathbb{F}_p , alors $Q + R = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$ donc

$$eval_y(Q + R) = \sum_{k=0}^{+\infty} \sigma(a_k + b_k) y^k = \sum_{k=0}^{+\infty} \sigma(a_k) y^k + \sum_{k=0}^{+\infty} \sigma(b_k) y^k = Q^\sigma(y) + R^\sigma(y) = eval_y(Q) + eval_y(R).$$

De plus : $QR = \sum_{n=0}^{+\infty} c_n X^n$ où $c_n = \sum_{k=0}^n a_k b_{n-k}$. Donc $eval_y(QR) = (QR)^\sigma(y) = \sum_{n=0}^{+\infty} \sigma(c_n) y^n$ et

$$\sigma(c_n) = \sum_{k=0}^n \sigma(a_k) \sigma(b_{n-k}). \text{ D'où : } eval_y(QR) = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^n \sigma(a_k) \sigma(b_{n-k}) \right) y^n = \sum_{k=0}^{+\infty} \sigma(a_k) y^k \times \sum_{k=0}^{+\infty} \sigma(b_k) y^k \text{ donc}$$

$eval_y(QR) = eval_y(Q) \times eval_y(R)$. **$eval_y$ est bien un morphisme d'anneaux.**

4. D'après **III.2.**, P divise le polynôme $B = X^{p^n} - X$. Donc P^σ divise $B^\sigma = (X^{p^n} - X)^\sigma = X^{p^n} - X$ dans $K'[X]$.
 D'après **III.3.a.**, tout élément de K est racine de B , donc tout élément de K' est racine de B^σ .
 Donc B^σ est scindé sur K' . Comme P^σ divise B^σ , P^σ est scindé sur K' . Or, $\deg(P^\sigma) = \deg(P) \geq 1$.
Donc P^σ admet au moins une racine dans K' .

5. Soit alors y une racine de P^σ dans K' . D'après **3.**, $eval_y$ est un morphisme d'anneaux de $\mathbb{F}_p[X]$ dans K' .
 Donc $\text{Ker}(eval_y)$ est un idéal de $\mathbb{F}_p[X]$. Par théorème (limite du programme), il existe $Q \in \mathbb{F}_p[X]$, nul ou unitaire, tel que $\text{Ker}(eval_y) = Q\mathbb{F}_p[X]$. Mais $Q = 0 \Rightarrow eval_y$ injective $\Rightarrow K'$ infini car $\mathbb{F}_p[X]$ est infini. Ceci est impossible.
 Donc $Q \neq 0$. $Q \neq 1$ car $eval_y(1) = 1 \neq 0$. Donc $\deg(Q) \geq 1$ et Q est unitaire.
 De plus, par choix de y , $eval_y(P) = P^\sigma(y) = 0$ donc $P \in \text{Ker}(eval_y)$, donc $Q \mid P$. Mais, comme P est irréductible et unitaire, $Q = P$. On peut alors "factoriser" $eval_y$ en posant : $\forall \bar{A} \in K = \mathbb{F}_p[X]/(P)$, $\psi(\bar{A}) = eval_y(A)$.
 On vérifie, de la même manière que pour σ , que ψ est bien définie, qu'elle est injective et que c'est un morphisme d'anneaux. Mais $|K| = |K'| = p^n$. Par théorème, ψ est bijective.
Donc ψ est un isomorphisme de corps de K sur K' .