Première composition de mathématiques
E.N.S. Lyon – MP

Dans tout le problème, p désigne un nombre entier premier et $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$ des entiers modulo p.
On propose ici une étude des polynômes irréductibles modulo p, c'est-à-dire à coefficients dans $\mathbf{F}_p$.
On montre, en particulier, que pour tout nombre premier p et tout nombre entier n, il existe un polynôme irréductible unitaire sur $\mathbf{F}_p$ de degré n *sans qu'on sache fournir explicitement un tel polynôme*. On étudie également une formule d'inversion de Möbius qui permet de dénombrer l'ensemble de ces polynômes.

PARTIE I : Calculs en caractéristique p

.1) Montrer qu'on a $\binom{p}{i} \equiv 0 \pmod{p}$ pour $0 < i < p$, où $\binom{p}{i}$ désigne le coefficient binomial, coefficient de X^i dans le développement du binôme $(X+1)^p$.

.2) Soit $\mathbf{K}$ un corps commutatif contenant le corps $\mathbf{F}_p$; déduire de la question précédente qu'on a $(x+y)^p = x^p + y^p$ pour x, y dans $\mathbf{K}$ puis qu'on a, pour tout polynôme R *à coefficients dans* $\mathbf{F}_p$ ainsi que pour x dans $\mathbf{K}$ et n dans $\mathbf{N}$, $R\left(x^{p^n}\right) = R(x)^{p^n}$.

PARTIE II : L'anneau quotient $k[X]/(Q)$

Dans cette partie, k désigne un corps commutatif quelconque, Q un polynôme à coefficients dans k, de degré supérieur ou égal à 1, et (Q) l'idéal de $k[X]$ engendré par Q.

On définit une relation d'équivalence $\mathscr{R}$ sur $k[X]$ par $R\,\mathscr{R}\,S \overset{def}{=} R - S \in (Q)$; on note A l'ensemble $k[X]/(Q)$ des classes d'équivalence modulo $\mathscr{R}$ et, pour R dans $k[X]$, $\overline{R}$ la classe de R dans A.

.1) a) Vérifier (rapidement) que les lois suivantes sont bien définies et confèrent à A une structure d'algèbre sur k, commutative et unitaire :

$$\overline{R} + \overline{S} = \overline{R+S}\,; \quad \overline{R} \times \overline{S} = \overline{R \times S}\,; \quad \lambda\overline{R} = \overline{\lambda R} \qquad (R, S \in k[X]\,,\ \lambda \in k)\,.$$

Vérifier également que l'application de k dans A donnée par $\lambda \mapsto \overline{\lambda}$ est un morphisme injectif qui permet d'identifier le corps k à un sous-anneau de A.

b) Montrer que tout élément de A s'écrit $R(\overline{X})$ où R est un polynôme *à coefficients dans* k.

c) Expliciter une base de A en tant qu'espace vectoriel sur k ; quelle est la dimension de cet espace vectoriel ?

.2) a) Caractériser les éléments R dans $k[X]$ tels que $\overline{R}$ soit inversible dans A.

b) En déduire une condition nécessaire et suffisante, portant sur le polynôme Q, pour que $k[X]/(Q)$ soit un corps. À titre d'exemple, quels sont les corps parmi $\mathbf{F}_2[X]/\left(X^2+X+1\right)$, $\mathbf{F}_{11}[X]/\left(X^2+1\right)$, $\mathbf{F}_{13}[X]/\left(X^2+1\right)$?

PARTIE III : Les facteurs irréductibles de $X^{p^n} - X$

Dans cette partie, Q désigne un polynôme *irréductible* de $\mathbf{F}_p[X]$ de degré d ; on note $\mathbf{K}$ le corps $\mathbf{F}_p[X]/(Q)$ et $\overline{X}$ la classe de X dans ce quotient.

.1) Quel est l'ordre du groupe multiplicatif $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$? En déduire $\forall y \in \mathbf{K}^*$, $y^{p^d-1} = 1$.

.2) On suppose, dans cette question que d divise n ; déduire de la question précédente qu'on a $\overline{X}^{p^n} = \overline{X}$ puis que Q divise $X^{p^n} - X$.

.3) On suppose, dans cette question, que Q divise $X^{p^n} - X$.

a) Montrer $\overline{X}^{p^n} = \overline{X}$ puis qu'on a $\forall y \in \mathbf{K}$, $y^{p^n} = y$.

b) Soit r le reste dans la division euclidienne de n par d ; montrer $\forall y \in \mathbf{K}^*$, $y^{p^r-1} = 1$.

c) En déduire que le polynôme $Y^{p^r-1}-1$ est le polynôme nul puis que d divise n.

.4) Montrer que le polynôme $X^{p^n}-X$ est sans facteur carré puis qu'on a $X^{p^n}-X=\prod_{d|n}\prod_{Q\in\mathbf{K}_p^d} Q$, $\mathbf{K}_p^d$ désignant l'ensemble des polynômes irréductibles unitaires de degré d sur $\mathbf{F}_p$.

PARTIE IV : Dénombrement des polynômes irréductibles

On désigne, dans cette partie par I_p^n le nombre de polynômes *irréductibles unitaires* de degré n sur $\mathbf{F}_p$.

.1) En utilisant le résultat de la question III.4., montrer : (*) $p^n=\sum_{d|n} dI_p^d$.

.2) Déduire de la question précédente qu'on a $p^d\geq dI_p^d$, puis qu'on a $I_p^n\geq 1$, autrement dit qu'il existe au moins un polynôme irréductible modulo p en tout degré.

.3) Donner les valeurs de I_p^1 et de I_p^n pour n premier. Montrer que la formule (*) ci-dessus permet de calculer I_p^n par une formule récurrente en n.

.4) On désire, dans cette question, retrouver directement la valeur de I_p^2 puis « expliciter » les I_p^2 trinômes unitaires irréductibles sur $\mathbf{F}_p$.

a) Donner un argument autre que celui fourni par la relation (*) permettant de calculer I_p^2. Expliciter les I_2^2 polynômes unitaires irréductibles sur $\mathbf{F}_2$.

On suppose maintenant $p\neq 2$.

b) Montrer que l'ensemble des carrés de $\mathbf{F}_p^*$ est un sous-groupe de $\mathbf{F}_p^*$ contenant exactement $(p-1)/2$ éléments.

c) En déduire la forme des I_p^2 trinômes unitaires irréductibles de $\mathbf{F}_p[X]$ puis de nouveau la valeur de I_p^2.

À titre d'exemple, on explicitera les I_5^2 trinômes unitaires irréductibles de $\mathbf{F}_5[X]$.

PARTIE V : La formule d'inversion de Möbius

Soit une relation entre deux fonctions f et g de $\mathbf{N}^*$ dans $\mathbf{C}$ (**) $\forall n\in\mathbf{N}^*,\ f(n)=\sum_{d|n} g(d)$.

On désire exprimer g en fonction de f. Ce résultat sera appliqué au calcul de I_p^n.
On désigne par $\mathfrak{F}$ l'ensemble de toutes les fonctions de $\mathbf{N}^*$ dans $\mathbf{C}$, muni de l'addition ordinaire des fonctions et du produit *arithmétique* défini par :

$$\forall n\in\mathbf{N}^*,\quad (f\star h)(n)=\sum_{d|n} f(d)h\left(\frac{n}{d}\right)\ .$$

.1) Vérifier que $\mathfrak{F}$ est un anneau commutatif et unitaire ; quel est son élément unité, que l'on notera χ ?

.2) Soit f dans $\mathfrak{F}$. Montrer que f est inversible dans $\mathfrak{F}$ si et seulement si $f(1)\neq 0$.

.3) On définit la fonction μ de Möbius par :

$$\begin{cases}\mu(1)=1 & \\ \mu(p_1p_2\cdots p_k)=(-1)^k & \text{si } p_1,\ p_2,\ \ldots,\ p_k \text{ sont des nombres premiers } \textit{distincts}\\ \mu(n)=0 & \text{sinon (c'est-à-dire si } n \text{ est divisible par un carré).}\end{cases}$$

et par cst_1 la fonction de $\mathbf{N}^*$ dans $\mathbf{C}$ constamment égale à 1.

a) Calculer $\mu\star\mathrm{cst}_1$.

b) Soient f et g dans $\mathfrak{F}$, liées par une relation (**) ; déduire de ce qui précède qu'on peut exprimer g en fonction de f par :

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \ .$$

.4) En déduire une formule exprimant I_n^p.

PARTIE VI : De nombreux polynômes ... mais un seul corps

Dans cette partie, on fixe un nombre entier n et on s'intéresse aux corps *commutatifs* à p^n éléments ; on souhaite démontrer que deux tels corps sont isomorphes.

.1) Montrer l'existence d'un corps commutatif ayant p^n éléments et préciser sa construction.
On désigne maintenant par $\mathbf{K}'$ un (autre) corps commutatif « abstrait » à p^n éléments.

.2) a) En utilisant le noyau de l'application de $\mathbf{Z} \to \mathbf{K}'$ qui à m dans $\mathbf{Z}$ associe $m \times 1$ (1 est l'élément unité de $\mathbf{K}'$), montrer l'existence d'un entier *premier* q tel que $qy = 0$ pour tout y dans $\mathbf{K}'$.

b) Montrer $p = q$.

c) En déduire l'existence et l'unicité d'un isomorphisme de corps σ du corps $\mathbf{F}_p$ sur un sous-corps $\sigma(\mathbf{F}_p)$ de $\mathbf{K}'$.
Si Q est un polynôme à coefficients dans $\mathbf{F}_p$ donné par $Q = \sum_i \lambda_i X^i$, on note Q^σ le polynôme $\sum_i \sigma(\lambda_i) X^i$ à coefficients dans $\sigma(\mathbf{F}_p)$, donc dans $\mathbf{K}'$.

.3) Soit y dans $\mathbf{K}'$; vérifier que l'application eval_y de $\mathbf{F}_p[X]$ dans $\mathbf{K}'$ définie par :

$$\mathrm{eval}_y(Q) = Q^\sigma(y)\,,\ Q \in \mathbf{F}_p[X]\,,$$

est un morphisme d'anneaux.

.4) On fixe un polynôme P dans $\mathbf{F}_p[X]$ irréductible de degré n auquel on associe le corps « concret » $\mathbf{K} = \mathbf{F}_p[X]/(P)$; montrer que le polynôme P^σ admet une racine dans $\mathbf{K}'$.

.5) En déduire l'existence d'un isomorphisme du corps $\mathbf{K}$ sur le corps $\mathbf{K}'$.

• • •

Première composition – ENS Lyon 1989

PARTIE I : Calculs en caractéristique p

.1) Pour i entier compris entre 1 et $p-1$, on a $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$. Par suite $p\binom{p-1}{i-1} = i\binom{p}{i}$ et p divise $i\binom{p}{i}$. Étant premier, p est premier avec i puisque $1 \leq i < p$, et donc, d'après le théorème de Gauss,

$\boxed{p \text{ divise } \binom{p}{i}.}$

.2) Puisque $\mathbf{K}$ contient $\mathbf{F}_p$, le morphisme canonique de $\mathbf{Z}$ dans $\mathbf{K}$ admet $p\mathbf{Z}$ comme noyau et donc, pour i entier compris entre 1 et $p-1$, $\binom{p}{i}$ est dans le noyau de ce morphisme. Autrement dit, en identifiant les entiers avec leur image dans $\mathbf{K}$, $\binom{p}{i}$ est nul dans $\mathbf{K}$.

D'après la formule du binôme de Newton, on a, pour x et y dans $\mathbf{K}$

$$\boxed{(x+y)^p = x^p + \sum_{i=1}^{p-1}\binom{p}{i}x^i y^{p-i} + y^p = x^p + y^p\ .}$$

Une récurrence immédiate sur k dans $\mathbf{N}$ montre

$$\forall (x_0, \cdots, x_k) \in \mathbf{K}^{k+1}\,, \quad \left(\sum_{i=0}^{k} x_i\right)^p = \sum_{i=0}^{k} x_i^p$$

et une seconde récurrence, sur n dans $\mathbf{N}$, permet d'obtenir

$$\forall n \in \mathbf{N}\,, \forall (x_0, \cdots, x_k) \in \mathbf{K}^{k+1}\,, \quad \left(\sum_{i=0}^{k} x_i\right)^{p^n} = \sum_{i=0}^{k} x_i^{p^n}$$

Soit maintenant R dans $\mathbf{F}_p[X]$, avec $R = \sum_{i=0}^{n} a_i X^i$. Pour x dans $\mathbf{K}$, il vient :

$$(R(x))^{p^n} = \left(\sum_{i=0}^{k} a_i x^i\right)^{p^n} = \sum_{i=0}^{k}(a_i x^i)^{p^n} = \sum_{i=0}^{k}(a_i)^{p^n}(x^i)^{p^n} = \sum_{i=0}^{k}(a_i)^{p^n}\left(x^{p^n}\right)^i\ .$$

Or, d'après le petit théorème de Fermat [a], pour λ dans $\mathbf{F}_p$, on a $\lambda^p = \lambda$ et donc par récurrence sur n dans $\mathbf{N}$, $\lambda^{p^n} = \lambda$. Il s'ensuit

$$\boxed{(R(x))^{p^n} = \sum_{i=0}^{k} a_i\left(x^{p^n}\right)^i = R\left(x^{p^n}\right)\ .}$$

a. C'est hors-programme et il faut donc en donner la démonstration. Elle se fait rapidement par récurrence en utilisant que $x \mapsto x^p$ est un morphisme additif : $\forall k \in \mathbf{N}$, $k^p \equiv k \pmod p$.

PARTIE II : L'anneau quotient $k[X]/(Q)$

.1) a) Soit R, S, T et U dans A et λ dans k. Les écritures

$$(R+S)-(T+U)=(R-T)+(S-U)\,,\ RS-TU=(R-T)S+(S-U)T\,,\ \lambda R-\lambda T=\lambda(R-T)$$

montrent que si $R-T$ et $S-U$ sont dans (Q), alors il en est de même de $(R+S)-(T+U)$, de $RS-TU$ et de $\lambda R-\lambda T$ puisque (Q) est stable par addition, par multiplication par un élément de $k[X]$ et donc aussi, a fortiori, par un élément de k. Ceci prouve que les trois lois sont bien définies sur A.
Comme $k[X]$ est une k-algèbre associative, commutative et unitaire, l'application surjective φ de $k[X]$ dans A définie par $\varphi(R)=\overline{R}$ permet de définir une structure de même nature sur A par transport de structure. En effet, on a, pour (x,y) dans A^2 et λ dans k

$$x+y=\varphi(\varphi^{-1}(x)+\varphi^{-1}(y))\ ;\quad x\times y=\varphi(\varphi^{-1}(x)\times\varphi^{-1}(y))\ ;\quad \lambda x=\varphi(\lambda\varphi^{-1}(x))$$

et la structure d'algèbre (associative, commutative et unitaire) sur A est une conséquence de celle sur $k[X]$: A est une k-algèbre associative, commutative et unitaire.
La restriction de φ à k est également un morphisme d'algèbre. Le noyau de cette restriction est l'intersection de $\mathrm{Ker}(\varphi)$ avec k, i.e. $(Q)\cap k$. Or tout polynôme non nul de (Q) est de degré supérieur à celui de Q, donc à 1. Il en résulte $\mathrm{Ker}(\varphi_{|k})=\{0\}$ et donc

$\varphi_{|k}$ est un morphisme injectif d'algèbres et on a $k\cong\varphi(k)$.

b) Soit α dans A et soit alors R dans $k[X]$ tel que $\alpha=\overline{R}$. On peut écrire $R=\sum_{i=0}^{n}a_iX^i$, pour n dans $\mathbf{N}$ et $(a_i)_{0\leq i\leq n}\in k^{n+1}$. Comme $k\subset A$ et $R\in k[X]$, on peut voir R comme un polynôme dans $A[X]$ et il vient

$$\alpha=\overline{\sum_{i=0}^{n}a_iX^i}=\sum_{i=0}^{n}\overline{a_iX^i}=\sum_{i=0}^{n}a_i\overline{X}^i=R(\overline{X})\,,$$

puisque $\overline{a_i}=a_i$.

c) Une base de A considéré comme k-espace vectoriel est $\mathcal{B}$ avec $\mathcal{B}=\left(\overline{1},\overline{X},\dots,\overline{X}^{d-1}\right)$, avec $d=\deg(Q)$. En effet :

— Soit α dans A et R dans $k[X]$ tel que $\alpha=\overline{R}$. On écrit la division euclidienne de R par Q sous la forme $R=BQ+R_1$ et alors $BQ\in(Q)$, de sorte qu'on a $R-R_1\in(Q)$ et donc $\alpha=\overline{R}=\overline{R_1}=R_1(\overline{X})$. Comme R_1 est de degré strictement inférieur à $\deg(Q)$, il en résulte que α est combinaison linéaire d'éléments de $\mathcal{B}$.

— Soit maintenant $(a_i)_{0\leq i\leq d-1}$ dans k^d tel que $\sum_{i=0}^{d-1}a_i\overline{X}^i=0$. En posant $R=\sum_{i=0}^{d-1}a_iX^i$, il vient $\overline{R}=\overline{0}$, soit $R\in(Q)$, i.e. Q divise R. Or $\deg(R)<\deg(Q)$ et donc $R=0$; autrement dit $a_i=0$ pour tout i dans $[\![0;d-1]\!]$, i.e. $\mathcal{B}$ est libre.

En particulier $\dim(A)=\deg(Q)$.

.2) a) Soit R dans $k[X]$ et $\alpha=\overline{R}$. Alors α est inversible dans A si et seulement s'il existe β dans A tel que $\alpha\beta=1$, ou encore s'il existe S dans $k[X]$ tel que $\overline{RS}=\overline{1}$, i.e. $RS-1$ est un multiple de Q. Cette dernière propriété est équivalente à l'existence d'un B dans $k[X]$ tel que $RS-1=QB$, i.e. $RS-QB=1$.
D'après le théorème de Bézout, il en résulte que

$\overline{R}$ est inversible dans A si et seulement si R est premier à Q.

b) Il résulte de ce qui précède que A est un corps si et seulement si, pour tout R tel que $\overline{R} \neq 0$, R est premier à Q, i.e. pour tout polynôme de $k[X]$, soit c'est un multiple de Q, soit il est premier à Q. Autrement dit $\boxed{A \text{ est un corps si et seulement si } Q \text{ est irréductible.}}$

On remarque par ailleurs qu'un polynôme Q de degré 2 est irréductible si et seulement s'il n'admet pas de diviseur de degré 1, i.e. si et seulement s'il n'admet pas de racine.

— Si $k = \mathbf{F}_2$ et $Q = X^2 + X + 1$, on a $Q(0) = Q(1) = 1$ et donc Q n'a pas de racine dans $\mathbf{F}_2$. Il est donc irréductible et $\boxed{\mathbf{F}_2/\left(X^2 + X + 1\right) \text{ est un corps.}}$

— Si $k = \mathbf{F}_{11}$ et $Q = X^2 + 1$, Q est irréductible si et seulement si -1 n'est pas un carré dans $\mathbf{F}_{11}$. Or en élevant 0, ± 1, …, ± 5 au carré, on obtient que les carrés dans $\mathbf{F}_{11}$ sont 0, 1, 4, 9, 5 et 3. Comme ils sont tous distincts de -1 modulo 11, Q est irréductible et donc $\boxed{\mathbf{F}_{11}[X]/\left(X^2 + 1\right) \text{ est un corps.}}$

— Si $k = \mathbf{F}_{13}$ et $Q = X^2 + 1$, on a $Q = (X - 5)(X + 5)$ et donc Q n'est pas irréductible. Il en résulte que $\boxed{\mathbf{F}_{13}[X]/\left(X^2 + 1\right) \text{ n'est pas un corps.}}$

PARTIE III : Les facteurs irréductibles de $X^{p^n} - X$

.1) D'après II.1.c, le corps $\mathbf{K}$ est un $\mathbf{F}_p$-espace vectoriel de dimension d et est donc isomorphe à $(\mathbf{F}_p)^d$. Il en résulte $\text{Card}(\mathbf{K}) = p^d$ et $\text{Card}(\mathbf{K}^*) = p^d - 1$: $\boxed{\text{le groupe multiplicatif } \mathbf{K}^* \text{ est d'ordre } p^d - 1.}$

D'après le théorème de Lagrange [b], on a donc $\boxed{y^{p^d-1} = 1 \text{ pour tout } y \text{ de } \mathbf{K}^*.}$

.2) Comme d divise n, $p^d - 1$ divise $p^n - 1$. Or, pour tout y de $\mathbf{K}^*$ on a $y^{p^d-1} = 1$ et donc on a aussi $y^{p^n-1} = 1$ et, a fortiori, $y^{p^n} = y$. Comme cette dernière égalité est encore vraie pour $y = 0$, on a donc $y^{p^n} = y$ pour tout élément de $\mathbf{K}$. En particulier pour $y = \overline{X}$, on a $\boxed{\overline{X}^{p^n} = \overline{X}}$.

Autrement dit $\overline{R} = 0$, si $R = X^{p^n} - X$,, et donc $\boxed{Q \text{ divise } X^{p^n} - X.}$

.3) a) On a $\overline{R} = \overline{0}$, en posant $R = X^{p^n} - X$, soit $\boxed{\overline{X}^{p^n} = \overline{X}.}$

Soit maintenant y dans $\mathbf{K}$. Il existe donc P dans $\mathbf{F}_p[X]$ tel que $y = \overline{P} = P\left(\overline{X}\right)$. Il vient

$$\begin{aligned} y^{p^n} &= P\left(\overline{X}\right)^{p^n} \\ &= P\left(\overline{X}^{p^n}\right) \quad \text{(d'après I.2)} \\ &= P\left(\overline{X}\right) \quad \text{(car } \overline{X}^{p^n} = \overline{X}\text{)} \\ &= y. \end{aligned}$$

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

b) Posons $n = dq + r$ la division euclidienne de n par d. On a

$$p^n - 1 = p^{dq+r} - 1 = p^r\left(p^{dq} - 1\right) + p^r - 1\ .$$

Donc, pour $y \in \mathbf{K}^*$, on a $y^{p^n-1} = \left(y^{p^{dq}-1}\right)^{p^r} y^{p^r-1}$. Or, d'après III.2, puisque d divise dq, $y^{p^{dq}-1} = 1$.

b. Encore un théorème hors-programme, qu'il faut donc démontrer. On le fait en considérant les classes pour la relation $x\mathcal{R}y \equiv xy^{-1} \in H$ avec H un sous-groupe de G. Toutes les classes ont un cardinal égal à $|H|$ et donc $|G|$ est un multiple de $|H|$.

Or, d'après III.3.a, pour $y \in \mathbf{K}^*$ on a $y^{p^n} = y$ et donc, par intégrité, $y^{p^n-1} = 1$. Par suite il vient :

$$1 = y^{p^n-1} = \left(y^{p^{dq}-1}\right)^{p^r} y^{p^r-1} = 1^{p^r} y^{p^r-1} = y^{p^r-1}$$

pour tout y de $\mathbf{K}^*$, i.e. $\boxed{\forall y \in \mathbf{K}^*,\ y^{p^r-1} = 1.}$

c) Soit $Y^{p^r-1} - 1$ dans $\mathbf{K}[Y]$. Son degré est égal à $p^r - 1$ sauf si $r = 0$ auquel cas A c'est le polynôme nul. Or tout $\mathbf{K}^*$ est racine de ce polynôme, ce qui lui confère $p^d - 1$ racines. Comme $p^d - 1 > p^r - 1$, c'est le polynôme nul. Par suite $r = 0$ et d divise n.

Le polynôme $Y^{p^r-1} - 1$ est le polynôme nul de $\mathbf{K}[Y]$ et d divise n.

.4) Supposons que le polynôme P de $\mathbf{F}_p[X]$ donné par $P = X^{p^n} - X$ possède un facteur carré. Soit alors Q irréductible dans $\mathbf{F}_p[X]$ tel que Q^2 divise P. On peut écrire $P = Q^2R$ avec $R \in \mathbf{F}_p[X]$. Il vient alors $P' = 2QQ'R + Q^2R'$ et donc Q divise P'. Mais on a $P' = p^n X^{p^n-1} - \overline{1} = -\overline{1}$ et donc Q divise $-\overline{1}$. Ceci est une contradiction puisque Q est irréductible et donc de degré supérieur à 1. $\boxed{X^{p^n} - 1 \text{ est sans facteur carré.}}$

Les questions précédentes montrent que les facteurs irréductibles de $X^{p^n} - 1$ sont de degré un diviseur de n et réciproquement puisque ce sont des diviseurs de $X^{p^n} - 1$. Par suite, puisque c'est un polynôme unitaire, on a $\boxed{X^{p^n} - X = \prod_{d|n} \prod_{Q \in \mathbf{K}_p^d} Q.}$

PARTIE IV : Dénombrement des polynômes irréductibles

.1) Puisque $n \geq 1$, on a $p^n > 1$ et donc le degré de $X^{p^n} - X$ est p^n. La formule établie en III.4 donne directement, en égalant les degrés :

$$p^n = \sum_{d|n} \sum_{Q \in \mathbf{K}_p^d} \deg(Q) = \sum_{d|n} \sum_{Q \in \mathbf{K}_p^d} d\,,$$

i.e. $\boxed{p^n = \sum_{d|n} d I_p^d.}$

.2) Soit d dans $\mathbf{N}^*$, on a donc $\boxed{p^d = \sum_{\delta|d} \delta I_p^\delta \geq d I_p^d}$ puisque c'est une somme à termes positifs. Mézalor on a

$$p^n = \sum_{d|n} d I_p^d \leq n I_p^n + \sum_{\substack{d|n \\ d \neq n}} p^d \leq n I_p^n + \sum_{d=0}^{n-1} p^d = n I_p^n + \frac{p^n - 1}{p - 1} \leq n I_p^n + p^n - 1$$

et donc $n I_p^n \geq 1$. Il s'ensuit $I_p^n > 0$ et donc $I_p^n \geq 1$.

Il y a au moins un polynôme irréductible unitaire de degré n dans $\mathbf{F}_p[X]$ et ce pour tout $n \in \mathbf{N}^*$.

.3) Tout polynôme Q unitaire de degré 1, i.e. du type $Q = X - \overline{a}$ avec $\overline{a} \in \mathbf{F}_p$, étant irréductible, on a $\boxed{I_p^1 = \text{Card}(\mathbf{F}_p) = p.}$

Si n est premier, ses seuls diviseurs sont 1 et n et la formule établie en IV.1 donne $p^n = I_p^1 + n I_p^n$, i.e. $\boxed{I_p^n = \frac{p^n - p}{n}.}$

Remarque : ce nombre est entier d'après le (petit) théorème de Fermat.

Par ailleurs la formule du IV.1 permet de calculer I_p^1 car elle donne $p = I_p^1$. Et elle permet, les I_p^d étant connus pour $d \in [\![1; n-1]\!]$ de calculer I_p^n, i.e.

la formule $(*)$ permet de calculer I_p^n par récurrence forte sur n.

.4) a) Un trinôme du second degré est irréductible si et seulement s'il n'admet par de racine. Les polynômes réductibles du second degré sont soit à racines distinctes, soit avec une (seule) racine double. On dénombre donc :

— L'ensemble des trinômes unitaires du second degré de $\mathbf{F}_p[X]$, i.e. de la forme $Q = X^2 + \overline{a}X + \overline{b}$, est en bijection avec $\mathbf{F} \times \mathbf{F}$, donc est de cardinal p^2.

— L'ensemble des trinômes unitaires du second degré ayant une racine double, i.e. de la forme $Q = (X - \overline{\alpha})^2$, est en bijection avec $\mathbf{F}$, donc est de cardinal p.

— L'ensemble des trinômes unitaires du second degré ayant deux racines simples, i.e. de la forme $Q = (X - \overline{\alpha})\left(X - \overline{\beta}\right)$ avec $\overline{\alpha} \neq \overline{\beta}$, est en bijection avec les classes d'équivalence de $\mathbf{F}_p \times \mathbf{F}_p$ privé de sa diagonale, pour la relation d'équivalence $\mathcal{R}$ définie par $(x, y)\mathcal{R}(x', y') \equiv ((x, y) = (x', y') \vee (x, y) = (y', x'))$. Il est donc de cardinal $(p^2 - p)/2$, i.e. $\dfrac{p(p-1)}{2}$.

Puisque, joint aux deux précédents, $\mathbf{K}_p^n$ forme une partition du premier ensemble, on a

$$\boxed{I_p^2 = p^2 - p - \frac{p(p-1)}{2} = \frac{p(p-1)}{2}.}$$

Pour $p = 2$, le cas d'une racine double fournit $(X + \overline{1})^2$, i.e. $X^2 + \overline{1}$, et X^2. Le cas de deux racines simples fournit $X(X + \overline{1})$, i.e. $X^2 + X$. Et donc

le seul trinôme du second degré unitaire irréductible est l'unique trinôme non encore écrit, i.e. $X^2 + X + \overline{1}$.

Remarque : c'est aussi une conséquence de IV.3 qui assure $I_p^2 = 1$ et de II.2.b qui assure que $X^2 + X + \overline{1}$ est irréductible dans $\mathbf{F}_2[X]$.

b) On note $\mathcal{C}(\mathbf{F}_p^*)$ l'ensemble des carrés d'éléments de $\mathbf{F}_p^*$. Comme $\mathbf{F}_p^*$ est un groupe multiplicatif commutatif, l'application $\varphi : \mathbf{F}_p^* \to \mathbf{F}_p^*$, définie par $\varphi(x) = x^2$ est un morphisme de groupes d'image $\mathcal{C}(\mathbf{F}_p^*)$ et de noyau $\left\{\overline{1}, -\overline{1}\right\}$. En particulier $\mathcal{C}(\mathbf{F}_p^*)$ est un groupe puisque c'est l'image d'un groupe par un morphisme de groupes. Comme $p > 2$, $\mathrm{Ker}(\varphi)$ possède exactement deux éléments. Le théorème de factorisation canonique, ou encore le théorème de Lagrange, donne

$$p - 1 = \mathrm{Card}(G) = \mathrm{Card}(\mathrm{Im}(\varphi))\,\mathrm{Card}(\mathrm{Ker}(\varphi))$$

et donc $\boxed{\mathrm{Card}\left(\mathcal{C}\left(\mathbf{F}_p^*\right)\right) = \dfrac{p-1}{2}.}$

c) Soit T un trinôme du second degré unitaire arbitraire de $\mathbf{F}_p[X]$, avec $T = X^2 + \alpha X + \beta$ et α et β dans $\mathbf{F}_p$. On l'écrit sous forme canonique : puisque $p \neq 2$, $\overline{2}$ est inversible et on pose u son inverse, et il vient

$$T = (X + u\alpha)^2 - u^2\left(\alpha^2 - 4\beta\right) .$$

Posons $x = -u\alpha$ et $y = u^2(\alpha^2 - 4\beta)$, de sorte qu'on a

$$T = (X - x)^2 - y .$$

Remarquons que, réciproquement, si x et y sont dans $\mathbf{F}_p$, on a

$$(X - x)^2 - y = X^2 + \alpha X + \beta$$

pour $\alpha = -2x$ et $\beta = x^2 - y$. On a donc une bijection entre l'ensemble des trinômes du second degré unitaires de $\mathbf{F}_p[X]$ et $\mathbf{F}_p^2$ donné par $T \mapsto (x, y)$. De plus un tel trinôme admet une racine si et seulement si l'équation $(X - x)^2 = y$ admet une solution, i.e. si et seulement si y est un carré. Dans ce cas, la racine est double si et seulement si y est nul.

Les trinômes du second degré unitaires irréductibles dans $\mathbf{F}_p[X]$ sont les trinômes de la forme $(X - x)^2 - y$ avec y qui n'est pas un carré dans $\mathbf{F}_p$.

Il en résulte que $\mathbf{K}_p^n$ est en bijection avec $\mathbf{F}_p \times \left(\mathbf{F}_p^* \setminus \mathcal{C}(\mathbf{F}_p^*)\right)$ et donc $\boxed{I_p^2 = p\dfrac{p-1}{2}.}$

On a $\mathcal{C}(\mathbf{F}_5^*) = \{\overline{1}, -\overline{1}\}$ et donc les dix trinômes du second degré unitaires irréductibles de $\mathbf{F}_5[X]$ sont de la forme $(X - x)^2 \pm \overline{2}$ pour x dans $\mathbf{F}_5$, i.e.

$\mathbf{K}_5^2$ est constitué de $X^2 - \overline{2}$ et $X^2 + \overline{2}$, $X^2 - \overline{2}X - \overline{1}$ et $X^2 - \overline{2}X - \overline{2}$, $X^2 + X + \overline{2}$ et $X^2 + X + \overline{1}$, $X^2 - X + \overline{2}$ et $X^2 - X + \overline{1}$, $X^2 + \overline{2}X - \overline{1}$ et $X^2 + \overline{2}X - \overline{2}$.

PARTIE V : La formule d'inversion de Möbius

.1) Puisque $\mathbf{C}^{\mathbf{N}^*}$ est un groupe commutatif pour l'addition, il en va de même pour $\mathfrak{F}$. De plus la loi $\star$ est une loi interne par définition même.

Soit f et h dans $\mathfrak{F}$, on a

$$\forall n \in \mathbf{N}^*, \quad (f * h)(n) = \sum_{\substack{1 \leq d_1, d_2 \leq n \\ d_1 d_2 = n}} f(d_1)h(d_2)$$

de sorte que la loi $\star$ est manifestement commutative puisque f et h jouent le même rôle et $\star$ est distributive par rapport à l'addition puisque la multiplication l'est dans $\mathbf{C}$.

Par ailleurs la fonction χ égale à 1 en 1 et nulle sur les autres entiers vérifie $f \star \chi = \chi \star f = f$ et est donc un élément neutre pour $\star$.

Enfin, pour g dans $\mathfrak{F}$, on a

$$\forall n \in \mathbf{N}^*, \quad (f * g) * h(n) = \sum_{\substack{1 \leq d_1, d_2, d_3 \leq n \\ d_1 d_2 d_3 = n}} f(d_1)g(d_2)h(d_3)$$

et donc $\star$ est associative puisque la multiplication l'est dans $\mathbf{C}$.

Finalement $\boxed{\mathfrak{F} \text{ est un anneau commutatif.}}$

.2) Si f est inversible, notons h son inverse. On a alors $f \star h(1) = f(1)h(1) = \chi(1) = 1$ et donc $f(1) \neq 0$.

Réciproquement, si $f(1) \neq 0$, on définit h par récurrence forte. On pose $h(1) = 1/f(1)$ et, pour n dans $\mathbf{N}$ supérieur à 2, si h est défini sur $[\![1; n-1]\!]$, on pose

$$h(n) = \frac{-1}{f(1)} \sum_{\substack{d \mid n \\ d \neq n}} f\left(\frac{n}{d}\right) h(d) \, .$$

On définit ainsi une fonction de $\mathbf{N}^*$ dans $\mathbf{C}$. De plus on a $f \star h(1) = f(1)h(1) = 1$ et, pour n entier supérieur à 2, $f \star h(n) = 0$ par construction de $h(n)$. Donc $f \star h = \chi$ et, par commutativité, $h \star f = \chi$, i.e. f est inversible d'inverse h.

La fonction f est inversible dans $\mathfrak{F}$ si et seulement si $f(1) \neq 0$.

.3) On a $\mu * \mathrm{cst}_1(1) = \mu(1)\mathrm{cst}_1(1) = 1$. Soit maintenant n un entier supérieur à 2 et $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sa décomposition primaire. On a

$$\begin{aligned}
(\mu * \mathrm{cst}_1)(n) &= \sum_{d|n} \mu(d) \\
&= \sum_{0\le\beta_1\le\alpha_1} \cdots \sum_{0\le\beta_k\le\alpha_k} \mu\left(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}\right) \\
&= \sum_{0\le\beta_1\le 1} \cdots \sum_{0\le\beta_k\le 1} \mu\left(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}\right) \\
&= \sum_{J\subset[\![1;k]\!]} \mu\left(\prod_{j\in J} p_j\right) \\
&= \sum_{J\subset[\![1;k]\!]} (-1)^{\mathrm{Card}(J)} \\
&= \sum_{j=0}^{k} \binom{k}{j} (-1)^j \\
&= (1-1)^k \quad \text{par la formule du binôme de Newton} \\
&= 0\,.
\end{aligned}$$

Par suite $\boxed{\mu * \mathrm{cst}_1 = \chi.}$

.4) On a $f = g \star \mathrm{cst}_1$ et donc $f \star \mu = g \star (\mathrm{cst}_1 \star \mu) = g \star \chi = g$. Et donc $g = f \star \mu = \mu \star f$. En particulier, pour n dans $\mathbf{N}^*$, $\boxed{g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).}$

.5) On applique ce qui précède pour f l'application $n \mapsto p^n$ et g l'application $n \mapsto nI_p^n$. On a bien $f = g \star \mathrm{cst}_1$ d'après IV.1. Donc, d'après la formule d'inversion de Möbius,

$\boxed{\text{on a, pour tout } n \text{ dans } \mathbf{N}^*,\ nI_p^n = \sum_{d|n} \mu(d) p^{n/d}, \text{ i.e. } I_p^n = \sum_{d|n} \frac{\mu(d)}{n} p^{n/d}.}$

Pour $n = 1$ on retrouve bien $I_p^1 = \mu(1)\, p^1 = p$. Pour n entier supérieur à 2 de décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, on a : $\boxed{I_p^n = \sum_{J\subset[\![1;k]\!]} \frac{(-1)^{\mathrm{Card}(J)}}{n} p^{n/\prod_{j\in J} p_j}.}$

PARTIE VI : De nombreux polynômes ... mais un seul corps

.1) D'après IV.2, il existe au moins un polynôme unitaire P irréductible modulo p de degré n. Si P est un tel polynôme, d'après II.2.b, $\mathbf{F}_p[X]/(P)$ est un corps commutatif et son cardinal est p^n, d'après la question III.1.

.2) a) Soit $\varphi : \mathbf{Z} \to \mathbf{K}'$ l'application définie par $\varphi(m) = m.1$, l'itéré additif d'ordre m de l'unité 1 de $\mathbf{K}'$. Alors φ est un morphisme d'anneaux et il n'est pas injectif puisque $\mathbf{Z}$ est infini alors que $\mathbf{K}'$ est fini. Son noyau est donc un idéal non nul de $\mathbf{Z}$, i.e. c'est $q\mathbf{Z}$ pour un certain entier q dans $\mathbf{N}^*$. Comme $\mathbf{K}'$ est un corps, q en est la caractéristique et est donc premier.

Par définition de φ, $m.1 = 0$ pour tout m dans $q\mathbf{Z}$ et donc, pour y dans $\mathbf{K}'$, on a $my = (m1)y = 0y = 0$. D'où : $\boxed{\text{il existe } q \text{ dans } \mathbf{N}^*, \text{ premier, tel que } qy = 0 \text{ pour tout } y \text{ dans } \mathbf{K}'.}$

b) L'image de $\mathbf{Z}$ par le morphisme précédent est un sous-corps de $\mathbf{K}'$ isomorphe à $\mathbf{F}_q$ et donc $\mathbf{K}'$ a une structure canonique d'espace vectoriel sur $\mathbf{F}_q$. Il est donc linéairement isomorphe à $\mathbf{F}_q^k$ pour un certain entier k et alors $\mathrm{Card}(\mathbf{K}') = q^k$. Comme p et q sont premiers, par unicité de la décomposition en facteurs premiers, il vient $k = n$ et $\boxed{p = q.}$

c) D'après le théorème de factorisation canonique il existe un unique morphisme $\sigma : \mathbf{F}_p \to \mathbf{K}'$ qui factorise le diagramme

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\varphi} & \mathbf{K}' \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\sigma} & \\ & \mathbf{F}_p & \end{array}$$

En tant que morphisme de corps, σ est injectif et réalise donc un isomorphisme du corps $\mathbf{F}_p$ sur le sous-corps $\sigma(\mathbf{F}_p)$ de $\mathbf{K}'$.

.3) L'application σ étant un morphisme de corps d $\mathbf{F}_p$ dans $\mathbf{K}'$, il est injectif et induit un morphisme d'anneaux injectif $\widetilde{\sigma}$ de $\mathbf{F}_p[X]$ dans $\mathbf{K}'[X]$ défini par $\widetilde{\sigma}(Q) = Q^\sigma$.

Par ailleurs la spécialisation en y est un morphisme de $\mathbf{K}'$-algèbres de $\mathbf{K}'[X]$ dans $\mathbf{K}'$. Par composition $\boxed{\mathrm{eval}_y \text{ est donc un morphisme d'anneaux de } \mathbf{F}_p[X] \text{ dans } \mathbf{K}'.}$

.4) D'après III.2, P divise $X^{p^n} - X$. Donc P^σ divise $\left(X^{p^n} - X\right)^\sigma$, i.e. divise $X^{p^n} - X$ dans $\mathbf{K}'[X]$.

D'après III.1, mutatis mutandis, tout élément de $(\mathbf{K}')^*$ est racine de $X^{p^n} - X$ et donc en fait tous les éléments de $\mathbf{K}'$ sont racines de ce polynôme. Il est donc simplement scindé sur $\mathbf{K}'$. Mais alors P^σ, étant un diviseur d'un polynôme simplement scindé, l'est aussi. Comme il est de degré supérieur à 1, $\boxed{P^\sigma \text{ admet au moins une racine dans } \mathbf{K}'.}$

.5) Soit y une racine de P^σ. L'application eval_y associée à ce choix de y est alors un morphisme d'anneaux de $\mathbf{F}_p[X]$ dans $\mathbf{K}'$ dont le noyau est un idéal principal de $\mathbf{F}_p[X]$. Comme $\mathbf{F}_p[X]$ est infini, eval_y n'est pas injective et donc son noyau n'est pas nul. Soit alors M un générateur unitaire de $\mathrm{Ker}(\mathrm{eval}_y)$. Son degré est supérieur à 1 puisque les polynômes constants non nuls ne sont pas dans $\mathrm{Ker}(\mathrm{eval}_y)$.

Or $\mathrm{eval}_y(P) = P^\sigma(y) = 0$ et donc $P \in (M)$, i.e. M divise P. Comme P est irréductible et comme M n'est pas constant et est unitaire, on a $M = P$. Il en résulte que l'application de $\mathbf{F}_p[X]/(P)$ dans $\mathbf{K}'$ est bien définie et est un morphisme injectif d'anneaux et donc de corps. Par cardinalité, c'est donc un isomorphisme et donc tous les corps commutatifs [c] sont isomorphe au corps concret $\mathbf{K}$.

$\boxed{\text{Il existe un isomorphisme de corps entre } \mathbf{K} \text{ et } \mathbf{K}', \text{ i.e. à isomorphisme prés il existe un seul corps commutatif de cardinal } p^n \text{ pour } p \text{ premier et } n \text{ dans } \mathbf{N}^*.}$

c. Par ailleurs le théorème de Wedderburn assure que tout corps fini est commutatif.