Concours E.N.S. de LYON - 1989

PREMIÈRE COMPOSITION DE MATHÉMATIQUES

Dans tout le problème, p désigne un nombre entier premier et $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p.

On propose ici une étude des polynômes irréductibles à coefficients dans $\mathbb{F}_p$. On montre, en particulier, que pour tout nombre premier p et tout nombre entier n, il existe un polynôme irréductible unitaire sur $\mathbb{F}_p$ 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 que $\binom{p}{i} \equiv 0 \pmod{p}$ 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 K un corps commutatif contenant le corps $\mathbb{F}_p$; déduire de la question précédente que $(x+y)^p = x^p + y^p$ pour $x, y \in K$ puis que $R\left(x^{p^n}\right) = R(x)^{p^n}$ pour tout $x \in K$, pour tout $n \in \mathbb{N}$ et tout polynôme R *à coefficients dans* $\mathbb{F}_p$.

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 ≥ 1, et (Q) l'idéal de $k[X]$ engendré par Q.

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

— Les lois suivantes sont bien définies et confèrent à $A = k[X]/(Q)$ une structure d'algèbre sur k, commutative et unitaire :
$$\overline{R} + \overline{S} = \overline{R+S}\,; \qquad \overline{R} \times \overline{S} = \overline{R \times S}\,; \qquad \lambda\overline{R} = \overline{\lambda R} \qquad (R, S \in k[X],\ \lambda \in k)$$
— L'application $\lambda \in k \mapsto \overline{\lambda} \in A$ est un morphisme injectif qui permet d'identifier le corps k à un sous-anneau de A.
— Tout élément de A s'écrit $R(\overline{X})$ où R est un polynôme *à coefficients dans* k.

1. Expliciter une base de A en tant qu'espace vectoriel sur k ; quelle est la dimension de cet espace vectoriel ?
2. Caractériser les éléments $R \in k[X]$ tels que $\overline{R} \in A$ soit inversible dans A.

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

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

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

1. Quel est l'ordre du groupe multiplicatif $K^* = K \setminus \{0\}$? En déduire que $y^{p^d-1} = 1$, $\forall y \in K^*$.
2. On suppose, dans cette question que $d = \deg Q$ divise n ; déduire de la question précédente que $\overline{X}^{p^n} = \overline{X}$ puis que Q divise $X^{p^n} - X$.
3. On suppose, dans cette question, que Q divise $X^{p^n} - X$.
   a. Montrer que $\overline{X}^{p^n} = \overline{X}$ puis que $y^{p^n} = y$, $\forall y \in K$.
   b. Soit r le reste dans la division euclidienne de n par d ; montrer que : $y^{p^r-1} = 1$, $\forall y \in K^*$.
   c. En déduire que le polynôme $Y^{p^r-1} - 1$ est le polynôme nul puis que $d = \deg Q$ divise n.
4. Montrer que le polynôme $X^{p^n} - X$ est sans facteur carré puis que : $X^{p^n} - X = \prod\limits_{d|n} \prod\limits_{Q \in K_p^d} Q$,
   K_p^d désignant l'ensemble des polynômes irréductibles unitaires de degré d sur $\mathbb{F}_p$.

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 $\mathbb{F}_p$.

1. En utilisant le résultat de la question III.4., montrer que : $(*)\ p^n = \sum\limits_{d|n} d I_p^d$.
2. Déduire de la question précédente que $p^d \geq d I_p^d$, puis que $I_p^n \geq 1$, 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 $\mathbb{F}_p$.
   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 $\mathbb{F}_2$.
   On suppose maintenant $p \neq 2$.

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

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

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

PARTIE V : La formule d'inversion de Möbius

Soit une égalité : $\quad (**) \quad f(n) = \sum_{d|n} g(d),\ n \geq 1$

où f et g sont deux fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$; 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 $\mathbb{N}^*$ dans $\mathbb{C}$, muni de l'addition ordinaire des fonctions et du produit *arithmétique* défini par :

$$(f \star h)(n) = \sum_{d|n} f(d) h\left(\frac{n}{d}\right),\ n \geq 1.$$

1. Vérifier que $\mathfrak{F}$ est un anneau commutatif et unitaire ; quel est son élément unité, que l'on notera χ ?
2. Montrer que $f \in \mathfrak{F}$ est inversible dans $\mathfrak{F}$ si et seulement si $f(1) \neq 0$.
3. On définit la fonction μ de Möbius par :
$$\begin{cases} \mu(1) = 1 \\ \mu(p_1 p_2 \ldots p_k) = (-1)^k \text{ si } p_1, p_2, \ldots, p_k \text{ sont des premiers } \textit{distincts} \\ \mu(n) = 0 \text{ sinon (c'est-à-dire si } n \text{ est divisible par un carré).} \end{cases}$$
et par cst_1 la fonction de $\mathbb{N}^*$ dans $\mathbb{C}$ constamment égale à 1.

   a. Calculer $\mu \star cst_1$.

   b. Soient f et g dans $\mathfrak{F}$, liées par une égalité $(**)$; 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 K' un (autre) corps commutatif « abstrait » à p^n éléments.

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

   b. Montrer que $p = q$.

   c. En déduire l'existence et l'unicité d'un isomorphisme de corps σ du corps $\mathbb{F}_p$ sur un sous-corps $\sigma(\mathbb{F}_p)$ de K'.

   Si Q $= \sum_i \lambda_i X^i$ est un polynôme à coefficients dans $\mathbb{F}_p$, on note Q^σ le polynôme $\sum_i \sigma(\lambda_i) X^i$ à coefficients dans $\sigma(\mathbb{F}_p) \subset K'$.

3. Soit $y \in K'$; vérifier que l'application $eval_y$ de $F_p[X]$ dans K' définie par :
$$eval_y(Q) = Q^\sigma(y),\ Q \in \mathbb{F}_p[X],$$
est un morphisme d'anneaux.

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

5. En déduire l'existence d'un isomorphisme du corps K sur le corps K'.

∴