Filière MP - ENS de Paris-Saclay, Lyon, Rennes et Paris - Session 2022
Page de garde du rapport de TIPE

NOM : SPECTOR	Prénoms : Clara, Noémie, Paula, Erna
Classe : MP*1	
Lycée : Louis-le-Grand	Numéro de candidat : 10346
Ville : Paris	

Concours auxquels vous êtes admissible, dans la banque MP inter-ENS (les indiquer par une croix) :

ENS Cachan	MP - Option MP	X	MP - Option MPI	
	Informatique			
ENS Lyon	MP - Option MP	X	MP - Option MPI	
	Informatique - Option M		Informatique - Option P	
ENS Rennes	MP - Option MP	X	MP - Option MPI	
	Informatique			
ENS Paris	MP - Option MP	X	MP - Option MPI	
	Informatique			

Matière dominante du TIPE (la sélectionner d'une croix inscrite dans la case correspondante) :

Informatique		Mathématiques	X	Physique	

Titre du TIPE : Corps finis et polynômes

Nombre de pages (à indiquer dans les cases ci-dessous) :

Texte	5	Illustration	0	Bibliographie	1

Attention, les illustrations doivent figurer dans le corps du texte et non en fin du document !

Résumé ou descriptif succinct du TIPE (6 lignes, maximum) :

Dans ce TIPE, on établit un théorème de classification des corps finis, puis on étudie quelques propriétés de l'anneau $\mathbb{F}_q[X]$, où q est une puissance d'un nombre premier.

À Paris

Le 12/06/2022

Signature du (de la) candidat(e)

Signature du professeur responsable de la classe préparatoire dans la discipline

Nicolas Tosel

Cachet de l'établissement

Lycée Louis le Grand
075 0655 E
123, rue St Jacques
75231 PARIS CEDEX 05
Tél. 01 44 32 82 00

La signature du professeur responsable et le tampon de l'établissement ne sont pas indispensables pour les candidats libres (hors CPGE).

Corps finis et polynômes

SPECTOR Clara

Candidate 10346

Sommaire

1 Introduction

Dans ce TIPE, on s'intéresse en premier lieu à la construction de corps finis. On montre que si p est un entier premier et n un entier quelconque, il existe un unique corps fini à isomorphisme près de cardinal p^n, et que ces cardinaux sont les seuls possibles pour un corps fini. Dans une seconde partie, on étudie l'anneau $\mathbb{F}_q[X]$ où q est une puissance d'un nombre premier. On s'intéresse en particulier au dénombrement des polynômes irréductibles de l'anneau $\mathbb{F}_q[X]$, et à celui du nombre de diviseurs irréductibles d'un polynôme de $\mathbb{F}_q[X]$, pour lequel on établit une loi faible des grands nombres. Enfin, on passe par une réduction modulo des nombres premiers pour montrer qu'un polynôme de $\mathbb{Z}[X]$ est souvent irréductible.

Notations utilisées :

- (P) : idéal engendré par P
- $U_{p,n}$: ensemble des polynômes unitaires de degré n de $\mathbb{F}_p[X]$
- $I_{p,n}$: ensemble des polynômes irréductibles de $U_{p,n}$
- $i_{p,n}$: $|I_{p,n}|$
- $R_{p,n}$: $U_{p,n} \setminus I_{p,n}$ l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_p[X]$ réductibles
- p_i : i-è nombre premier impair

2 Construction de corps finis

2.1 Le corps $\mathbb{F}_{p^n}$

On établit dans cette partie le théorème de classification des corps finis.

Théorème 1 *Le cardinal d'un corps fini est de la forme p^n pour un certain p premier et un certain n entier, et il existe un unique corps (à isomorphisme près) de cardinal p^n.*

Soit $\mathbb{K}$ un corps fini, sa caractéristique est un nombre premier p (sans quoi il contiendrait un sous corps isomorphe à $\mathbb{Q}$). $\mathbb{K}$ est naturellement muni d'une structure de $\mathbb{F}_p$-ev, de dimension finie car $\mathbb{K}$ est fini, donc est isomorphe en tant qu'espace vectoriel à $(\mathbb{F}_p)^n$ pour un certain $n \in \mathbb{N}^*$. On en déduit que $|\mathbb{K}| = p^n$.
Réciproquement, on fixe p premier et $n \in \mathbb{N}$, on construit un corps de cardinal p^n. Admettons pour le moment qu'il existe un polynôme irréductible Q de $\mathbb{F}_p[X]$ de degré n. L'anneau quotient $A = \mathbb{F}_p[X]/(Q)$ est un corps, car si $R \in \mathbb{F}_p[X]$ est premier avec Q, on dispose (Bezout) de B, C tels que $BR + CQ = 1$. Dans A, on a alors $\overline{BR} = 1$, donc la classe de R est inversible dans A. En particulier, tous les éléments non nuls de A sont inversibles. On a de plus $|A| = p^n$.
Il nous faut alors montrer l'existence d'un tel polynôme.
On passe par la propriété suivante :

Proposition 1 *: Si $Q \in I_{p,d}$, $Q \mid X^{p^n} - X$ si et seulement si $d \mid n$.*

Preuve : Si $d \mid n$, on étudie $\mathbb{K} = \mathbb{F}_p[X]/(Q)$. C'est un corps de cardinal p^d donc $\mathbb{K}^*$ est (comme groupe) d'ordre $p^d - 1$ et pour tout $x \in \mathbb{K}^*$, $x^{p^d-1} = 1$, ce que l'on réécrit en $x^{p^d} = x$ pour tout $x \in \mathbb{K}$, puis par récurrence, pour tout $k \in \mathbb{N}$, $x^{p^{kd}} = x$. Comme $d \mid n$, on a alors $\overline{X}^{p^n} - \overline{X} = \overline{0}$, ce qui signifie exactement que $Q \mid X^{p^n} - X$.
Réciproquement si $Q \mid X^{p^n} - X$, alors on a $\overline{X}^{p^n} = \overline{X}$ dans $\mathbb{K}$. De plus, si $y \in \mathbb{K}, y = \overline{R(X)} = R(\overline{X})$ pour un certain polynôme R, on a alors (calcul rapide dans $\mathbb{F}_p$) $R(\overline{X})^{p^n} = R(\overline{X}^{p^n}) = R(\overline{X})$ d'où, pour tout $y \in \mathbb{K}$, $y^{p^n} = y$. Alors, si r est le reste de la division euclidienne de n par d et k le quotient, on a $(y^{p^{kd}})^{p^r} = y$ et comme $y^{p^d} = y$ car $\mathbb{K}$ est d'ordre p^d, on a encore $y^{p^{kd}} = y$ et finalement $y^{p^r} = y$, soit $y^{p^r-1} = 1$. Donc les éléments de $\mathbb{K}$, au nombre de p^d, sont racines du polynôme $Y^{p^r-1} - 1$. Si ce polynôme n'est pas le polynôme nul, c'est absurde car son degré est inférieur à p^d. On en déduit donc $p^r - 1 = 0$ soit $p^r = 1$ ce qui impose $r = 0$. Donc $d \mid n$. On montre alors :

Proposition 2 $X^{p^n} - X = \prod_{d|n} \prod_{Q \in I_{p,d}} Q$.

Preuve : La divisibilité $\prod_{d|n} \prod_{Q \in I_{p,d}} Q \mid X^{p^n} - X$ provient de la proposition précédente, car tous ces polynômes sont premiers entre eux. Réciproquement, les facteurs irréductibles de $X^{p^n} - X$ sont les $Q \in I_{p,d}$ où $d \mid n$. De plus $X^{p^n} - X$ est sans facteur carré, car il se dérive en -1 et est donc premier avec son polynôme dérivé. On en déduit alors $X^{p^n} - X \mid \prod_{d|n} \prod_{Q \in I_{p,d}} Q$, et comme ces deux polynômes sont unitaires, on a l'égalité. En passant aux degrés, on a alors

Proposition 3 $p^n = \sum_{d|n} d i_{p,d}$

Cette propriété sera utile en 3.1. Ici, on en déduit que pour tout $d \in \mathbb{N}$, $di_{p,d} \leq p^d$. Supposons alors $i_{p,n} = 0$. On a alors $p^n = \sum_{d|n} di_{p,d} \leq \sum_{k=0}^{n-1} p^k = \frac{p^n - 1}{p - 1} < p^n$, c'est absurde et donc $i_{p,n} \neq 0$: **il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$**. Nous avons donc établi l'existence d'un corps fini de cardinal p^n.

Montrons alors son unicité à isomorphisme près. Soit $\mathbb{K}$ un corps quelconque de cardinal p^n, et $Q \in I_{p,n}$. On a $X^{p^n} - X = \prod_{x \in \mathbb{K}} (X - x)$ (car par Lagrange, pour $x \in \mathbb{K}, x^{p^n} = x$ d'où une divisibilité puis l'égalité par les degrés). De plus, par la proposition 1, $Q \mid X^{p^n} - X$. On en déduit que Q a une racine x dans $\mathbb{K}$. Si on pose $\begin{array}{cccc} \Phi & : & \mathbb{F}_p[X] & \to & \mathbb{K} \\ & & Q & \mapsto & Q(x) \end{array}$, Φ est un morphisme et $\mathrm{Ker}(\Phi)$ est un idéal de $\mathbb{F}_p[X]$ contenant Q ; comme celui-ci admet un unique générateur irréductible unitaire, on en déduit $\mathrm{Ker}(\Phi) = (Q)$ puis si $\overline{\Phi}$ est le morphisme induit de $\mathbb{F}_p[X]/(Q)$ vers $\mathbb{K}$, $\overline{\Phi}$ est injective et par égalité des cardinaux, bijective. On en déduit donc que $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/(Q)$. Donc tous les corps de cardinal p^n sont isomorphes.

3 Polynômes à coefficients dans un corps fini

On se fixe un entier premier p dans cette partie, et on note q une quelconque puissance de p. On note dans la suite $\mathbb{F}_q$ un corps de cardinal q (que l'on peut, par la précédente partie, construire de façon concrète en trouvant un polynôme de degré n irréductible sur $\mathbb{F}_p$). On va étudier quelques propriétés de l'anneau $\mathbb{F}_q[X]$.

3.1 Dénombrement des polynômes irréductibles de $\mathbb{F}_q[X]$

On a obtenu dans la précédente partie la formule $p^n = \sum_{d|n} di_{p,d}$ pour tout n. On a exactement par la même démarche $q^n = \sum_{d|n} di_{q,d}$. Dans cette section, on utilise cette formule pour donner une estimation asymptotique de $i_{q,n}$ quand n tend vers l'infini.
On peut exprimer $i_{q,n}$ à l'aide de cette formule et de la formule d'inversion de Moebius. Soit μ la fonction de Moebius, définie de la manière suivante :

- $\mu(1) = 1$
- $\mu(n) = (-1)^r$ si n est le produit de r nombres premiers distincts
- $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier.

On a alors :

Proposition 4 *:* $ni_{q,n} = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ *(formule d'inversion de Moebius)*

On a alors la majoration suivante : $|ni_{q,n} - q^n| \leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} q^k < \frac{q^{\frac{n}{2}+1} - 1}{q - 1} < \frac{q}{q-1} q^{\frac{n}{2}}$ et alors :

$|i_{q,n} - \frac{q^n}{n}| \leq \frac{q}{q-1} \frac{q^{\frac{n}{2}}}{n}$, ce qui nous donne l'estimation $i_{q,n} \underset{n \to +\infty}{\sim} \frac{q^n}{n}$. Comme le cardinal de l'ensemble des polynômes unitaires de $\mathbb{F}_q[X]$ de degré n est q^n, cela s'interprète en terme de probabilités : si P_n est une variable aléatoire suivant la loi uniforme sur $U_{q,n}$, on a $\mathbb{P}(P_n \text{ est irréductible}) \underset{n \to +\infty}{\sim} \frac{1}{n}$.

3.2 Nombre moyen de diviseurs irréductibles

On s'intéresse dans cette section au nombre de diviseurs irréductibles d'un polynôme P non nul de $U_{q,n}$. Plaçons nous dans un cadre probabiliste : on munit $U_{q,n}$ de la loi uniforme. Pour P irréductible, on définit sur $U_{q,n}$ une variable aléatoire $X_{P,n}$ telle que $X_{P,n}(Q) = 1$ si $P \mid Q$ et 0 sinon. Si d=deg P, comme le cardinal de l'ensemble des polynômes de $U_{q,n}$ divisibles par P est q^{n-d}, cela donne que $X_{P,n} \sim \mathcal{B}(q^{-d})$, et si $X_n = \displaystyle\sum_{d=1}^{n} \sum_{Q \in I_{q,d}} X_{Q,n}$. La variable aléatoire X_n compte le nombre de diviseurs irréductibles distincts d'un polynôme. L'estimation précédente nous permet alors d'établir la

Proposition 5 *:* $\mathbb{E}(X_n) = \ln n + O(1)$

En effet, par linéarité de l'espérance, on a $\mathbb{E}(X_n) = \displaystyle\sum_{d=1}^{n} i_{q,d}q^{-d}$, et $i_{q,d}q^{-d} = \frac{1}{d} + O\left(\frac{1}{dq^{\frac{d}{2}}}\right)$, donc $(\mathbb{E}(X_n) - H_n)$ converge. Avec la relation classique $H_n = \ln n + O(1)$ on obtient la proposition 5.
Ainsi, la bonne échelle pour étudier le nombre de diviseurs irréductibles d'un polynôme unitaire de degré n est l'échelle logarithmique. On établit alors une loi faible des grands nombres pour le nombre de diviseurs irréductibles.

Théorème 2 *: La suite* $\left(\dfrac{X_n}{\ln(n)}\right)_{n\geq 1}$ *converge en probabilités vers 1.*

Preuve : Au vu de la proposition 5, il nous suffit d'établir que la suite $\left(\dfrac{X_n}{\mathbb{E}(X_n)}\right)_{n\geq 1}$ converge en probabilités vers 1. Fixons $\varepsilon > 0$. Par l'inégalité de Bienaymé-Tchebycheff, on a pour tout $n \geq 1$ $\mathbb{P}(|X_n - \mathbb{E}(X_n)| > \varepsilon\mathbb{E}(X_n)) \leq \dfrac{\mathbb{V}(X_n)}{\varepsilon^2 \mathbb{E}(X_n)^2}$. On veut montrer que ce terme tend vers 0 lorsque $n \to +\infty$ pour conclure. C'est en fait un $O(\frac{1}{\ln n})$, ce que l'on établit en montrant que la suite $(\mathbb{V}(X_n) - \ln n)_{n\geq 1}$ est majorée. Pour ce faire, il suffit de voir que :

- $\displaystyle\sum_{d=1}^{n} \sum_{Q \in I_{q,d}} \mathbb{V}(X_{Q,n}) = \ln n + O(1)$
- $\mathrm{Cov}(X_{Q,n}, X_{R,n}) \leq 0$ pour tout couple (Q, R) de polynômes irréductibles distincts de $\mathbb{F}_q[X]$

La première égalité s'établit en observant que la somme en question est $\displaystyle\sum_{d=1}^{n} i_{q,d}(q^d - q^{-2d})$ et que la série de terme général $i_{q,d}q^{-2d}$ converge (par l'estimation faite en 3.1).
La seconde s'établit en calculant explicitement la covariance : pour (Q, R) un tel couple, de degrés respectifs a et b, on a $\mathbb{E}(X_{Q,n}X_{R,n}) = \mathbb{E}(X_{QR,n})$ car Q et R sont premiers entre eux ; cette quantité vaut donc 0 si $a + b > n$ et $q^{-(a+b)}$ sinon, et $\mathbb{E}(X_{Q,n})\mathbb{E}(X_{R,n}) = q^{-a}q^{-b}$, ce qui donne finalement $\mathrm{Cov}(X_{Q,n}, X_{R,n}) = 0$ si $a + b \leq n$ et $\mathrm{Cov}(X_{Q,n}, X_{R,n}) = -q^{-a-b}$ sinon.

3.3 Un polynôme de $\mathbb{Z}[X]$ est souvent irréductible

Dans cette section, on montre qu'un polynôme de $\mathbb{Z}[X]$ est souvent irréductible sur $\mathbb{Z}$. Il convient de donner un sens à "souvent". L'énoncé que l'on va montrer est donc le suivant.

Théorème 3 *: Si on note, pour $n \in \mathbb{N}^*$ et $N \in \mathbb{N}, E_{N,n}$ l'ensemble des polynômes de $\mathbb{Z}[X]$ unitaires de degré n dont les coefficients d'indice $< n$ sont dans $[-N, N]$ (de cardinal $(2N+1)^n$) et $I_{N,n}$ les polynômes irréductibles sur $\mathbb{Z}$ de cet ensemble, à n fixé, on a* $\lim\limits_{N\to+\infty} \dfrac{|I_{N,n}|}{|E_{N,n}|} = 1.$

Preuve : Fixons $n \in \mathbb{N}$. On va exploiter le fait qu'un polynôme de $\mathbb{Z}[X]$ réductible sur $\mathbb{Z}$ est réductible modulo n'importe quel nombre premier, pour montrer qu'il y en a peu. L'observation suivante est alors essentielle :

Proposition 6 *: Si p est un nombre premier impair, si on munit $U_{p,n}$ de la loi uniforme, la probabilité qu'un polynôme P de $U_{p,n}$ soit réductible sur $\mathbb{F}_p$ est majorée par $c_n = 1 - \frac{1}{2n}$.*

Cette probabilité vaut $1 - \frac{i_{p,n}}{p^n}$. Or on a, par l'étude de 3.1, $\dfrac{n i_{p,n}}{p^n} = 1 - \sum\limits_{d|n, d\neq n} \mu(\dfrac{n}{d}) p^{d-n} > 1 - \sum\limits_{k=1}^{\lfloor \frac{n}{2} \rfloor} p^{k-n} >$ $1 - \dfrac{p^{\frac{n}{2}} - 1}{p^n(p-1)} > 1 - \dfrac{1}{p^{\frac{n}{2}}} > \dfrac{1}{2}$. D'où $1 - \frac{i_{p,n}}{p^n} < 1 - \frac{1}{2n}$. On en tire en particulier que le nombre de polynômes unitaires de degré n réductibles sur $\mathbb{F}_p$ est majoré par $p^n(1 - \frac{1}{2n})$.

Retour à la démonstration : pour $r \in \mathbb{N}$, soit m le produit des r premiers nombres premiers impairs. On considère Φ la restriction à $E_{N,n}$ de la surjection canonique de $\mathbb{Z}[X]$ sur $\mathbb{Z}/m\mathbb{Z}[X]$, qui est un morphisme d'anneaux. Si P est dans l'image de Φ, $\Phi^{-1}(\{P\})$ est de cardinal majoré par $(\frac{2N+1}{m} + 1)^n$. De plus comme Φ est un morphisme, l'image par Φ d'un élément réductible sur $\mathbb{Z}$ est réductible sur $\mathbb{Z}/m\mathbb{Z}$. Enfin ,

$$\begin{array}{cccc} \Psi & : & \mathbb{Z}/m\mathbb{Z}[X] & \rightarrow & \prod\limits_{i=1}^{r} \mathbb{Z}/p_i\mathbb{Z}[X] \\ & & P \mod m & \mapsto & (P \mod p_1, ..., P \mod p_r) \end{array}$$

est un isomorphisme (théorème chinois des restes) ; on en déduit alors que l'ensemble des polynômes unitaires réductibles de $\mathbb{Z}/m\mathbb{Z}[X]$ est de cardinal majoré par $\prod\limits_{i=1}^{r} |R_{p_i,n}| \leq \prod\limits_{i=1}^{r} \left(p_i^n \left(1 - \dfrac{1}{2n} \right) \right) = m^n \left(1 - \dfrac{1}{2n} \right)^r$ d'après la proposition 6. D'où $|\Phi(R_{N,n})| \leq m^n(1 - \frac{1}{2n})^r$ puis $|R_{N,n}| \leq (\frac{2N+1}{m} + 1)^n m^n (1 - \frac{1}{2n})^r$.

Ainsi, si on prend N tel que $2N + 1 > m$, on a alors $\dfrac{|R_{N,n}|}{|E_{N,n}|} \leq (\frac{2N+1+m}{2N+1})^n (1 - \frac{1}{2n})^r \leq 2^n (1 - \frac{1}{2n})^r$. Ce dernier terme tend vers 0 quand r tend vers $+\infty$, donc quand N tend vers $+\infty$, ce qui conclut la preuve du théorème.

4 Bibliographie

[1] Xavier Gourdon, *Les maths en Tête, Algèbre.*

[2] Lindsay N. Childs, *A Concrete Introduction to Higher Algebra* (Chapter 27, *Irreducible polynomials*). (URL : http://people.dm.unipi.it/gianni/AlgebraII/libri/irriducibili.pdf)

[3] Michel Demazure, *Cours d'Algèbre.*

[4] R. Lidl et H. Niederreiter, *Introduction to Finite Fieds.*