Aix-Marseille Université
Préparation à l'agrégation: Option C
https://www.i2m.univ-amu.fr/perso/david.kohel/tch/Agreg/

Polynômes sur $\mathbb{F}_p$ et corps finis

Exercices

1. Combien d'anneaux commutatifs de cardinal 4 existent-ils ? (Indication : Considérer les eventuels homomorphismes surjectifs $\mathbb{Z} \to A$ ou $\mathbb{F}_2[x] \to A$.)

Solution. *Soit A un anneau commutatif (avec 1) de cardinal 4. Alors le caracteristique de A est le générateur positif de l'unique homomorphisme d'anneaux $\pi : \mathbb{Z} \to A$, tel que $\pi(1_\mathbb{Z}) = 1_A$. L'homomorphisme π est également homomorphisme des groupes abéliens $\mathbb{Z}$ et A, et par le théorème de Lagrange, l'image est d'ordre 4 ou 2 (car $1 \neq 0$ dans A). Dans le premier cas, π induit un isomorphisme $\mathbb{Z}/4\mathbb{Z} \to A$, sinon l'image est isomorphe à $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Il suit qu'on a deux possibilités :*

— $A = \mathbb{Z}/4\mathbb{Z}$.
— $A = \mathbb{F}_2[\alpha]$ *ou* $\alpha^2 + a\alpha + b = 0$.

Dans le deuxième cas, si $\alpha \in A \backslash \mathbb{F}_2$ alors $A = \mathbb{F}_2[\alpha]$ est l'espace vectoriel $\mathbb{F}_2 \oplus \mathbb{F}_2\alpha$ sur $\mathbb{F}_2$ avec la base $\{1, \alpha\}$. Par conséquent $\alpha^2 \in \mathbb{F}_2 \oplus \mathbb{F}_2\alpha$ satisfait un polynôme minimal $x^2 + ax + b \in \mathbb{F}_2[x]$ et

$$A = \mathbb{F}_2[\alpha] \cong \mathbb{F}_2[x]/(x^2 + ax + b).$$

Il reste à déterminer des isomorphismes possibles entres les anneaux de la forme $\mathbb{F}_2[x]/(x^2 + ax + b)$ pour $(a, b) \in \mathbb{F}_2^2$:

— $A \cong \mathbb{F}_2[x]/(x^2 + x + 1) = \mathbb{F}_4$, *un corps,*
— $A \cong \mathbb{F}_2[x]/(x^2 + x) \cong \mathbb{F}_2 \times \mathbb{F}_2$, *un produit de corps,*
— $A \cong \mathbb{F}_2[x]/(x^2) = \mathbb{F}_2[\varepsilon]$ *avec* $\epsilon^2 = 0$,
— $A \cong \mathbb{F}_2[x]/((x+1)^2) = \mathbb{F}_2[\mu]$ *avec* $\mu^2 = 1$.

On note que $\mathbb{F}_4$ est un corps car $x^2 + x + 1$ est irreductible, et la factorisation $x^2 + x = x(x+1)$ donne lieu au produit de corps par le théorème chinois. Finalement l'identification $\mu = \varepsilon + 1$ est un isomorphisme d'anneaux.

En conclusion, il n'existe que quatre anneaux de cardinal 4 :

$$\mathbb{Z}/4\mathbb{Z}, \quad \mathbb{F}_4, \quad \mathbb{F}_2 \times \mathbb{F}_2, \quad \mathbb{F}_2[\varepsilon].$$

Finalement, on peut confirmer que ces anneaux sont bien non isomorphes, deux à deux, car ils sont distingués par leurs des invariants : le caracterstique $\mathrm{car}(A)$ et l'ordre $|A^*|$ du groupe d'unités :

A	$\mathrm{car}(A)$	$\lvert A^*\rvert$	A^*
$\mathbb{Z}/4\mathbb{Z}$	4	2	$\{\pm 1\}$
$\mathbb{F}_4$	2	3	$\{1, \alpha, \alpha + 1\}$
$\mathbb{F}_2 \times \mathbb{F}_2$	2	1	$\{(1, 1)\}$
$\mathbb{F}_2[\varepsilon]$	2	2	$\{1, \varepsilon + 1\}$

2. Montre que r divise $\varphi(p^r-1)$. Plus généralement, pour tout entier $a>1$ et $r\geq 1$, démontrer que r divise $\varphi(a^r-1)$. (Indication : utiliser le théorème de Lagrange.)

Solution. *On observe que les conditions suivants sont équivalentes :*
— $a^r-1 \bmod n = 0$,
— $a^r \bmod n = 1$,
— *l'ordre* a *dans* $(\mathbb{Z}/n\mathbb{Z})^*$ *divise* r,
En particulier pour $a>1$, *les entiers* $r>1$ *et* $n=a^r-1$ *satisfaient les conditions précédentes, et il n'existe pas* $0<s<r$ *tel que* $a^s-1 \bmod n$ *car*

$$0<a^s-1<a^r-1=n.$$

Par conséquent, il suit que r *est l'ordre exacte de* a. *Par le théorème de Lagrange,*

$$r=|\langle a\rangle| \text{ divise } |(\mathbb{Z}/n\mathbb{Z})^*|=\varphi(n)=\varphi(a^r-1).$$

3. Trouver les premiers p et les entiers $r\geq 1$ tel qu'il existe un seul polynôme primitif de degré r dans $\mathbb{F}_p[x]$.

Solution. *On commence avec un exemple qui motive cet exercice.*
Example. *Soient* $p=2$ *et* $r=2$. *On observre que* $\Phi_3(x)=x^2+x+1\in\mathbb{F}_2[x]$ *est irreductible, et le seul polynôme primitif (et irredictible) de degré* 2. *Par conséquent,*

$$\mathbb{F}_4=\mathbb{F}_2[x]/(x^2+x+1),$$

est la représentation unique de $\mathbb{F}_4$ *en tant que quotient de* $\mathbb{F}_2[x]$.

En plus de généralité, un polynôme irreductible de degré r *dans* $\mathbb{F}_p[x]$ *est primitif si et seulement s'il est un diviseur de* $\Phi_n(x)$, *où* $n=p^r-1$. *Le degré de* $\Phi_n(x)$ *est* $\varphi(n)$, *alors il est nécessaire et suffisant de déterminer* (p,r) *tel que* $r=\varphi(p^r-1)$.

Si $r=1$, *l'égalité* $r=\varphi(p-1)=|(\mathbb{Z}/(p-1)\mathbb{Z})^*|=1$ *est vérifié si et seulement si* $p=2$ *ou* $p=3$. *Les égalités* $\varphi(2-1)=\varphi(3-1)=1$ *sont évidentes. Or si* $p>3$, *il existe un prémier* ℓ *tel que* 2ℓ *divise* $p-1$. *Il suit qu'il y a une surjection :*

$$(\mathbb{Z}/(p-1)\mathbb{Z})^*\longrightarrow(\mathbb{Z}/2\ell\mathbb{Z})^*.$$

Par conséquent $\varphi(2\ell)$ *divise* $\varphi(p-1)$. *Or si* $\ell=2$, *alors* $\varphi(2\ell)=2$ *sinon* $\varphi(2\ell)=\ell-1\geq 2$, *d'où*

$$2\leq\varphi(2\ell)\leq\varphi(p-1)\neq 1.$$

Remarque. *En effet on peut démontrer divisibilité* $2\,|\,\varphi(2\ell)\,|\,\varphi(p-1)$.

On a déterminé trois polynômes qui sont uniques parmi l'ensemble des polynômes primitifs de $\mathbb{F}_p[x]$ *de degré* r *:*

$$x+1\in\mathbb{F}_2[x],\quad x+1\in\mathbb{F}_3[x],\quad x^2+x+1\in\mathbb{F}_2[x].$$

On va démontrer que ces trois polynômes sont les seuls avec cette propriété.

Si $r>1$, *on pose* $n=p^r-1$. *Par la divisibilité de* n *par* $p-1$, *on a une surjection*

$$(\mathbb{Z}/n\mathbb{Z})^*\longrightarrow(\mathbb{Z}/(p-1)\mathbb{Z})^*,$$

ayant le sous-groupe $\langle p\rangle$ d'ordre r dans le noyau, d'où $r\varphi(p-1)\,|\,\varphi(n)$, alors l'inégalité $\varphi(p-1)\neq 1$ est une obstruction à l'égalité $r=\varphi(n)$. Par le calcul précédent, on se réduit à $p=2$ ou $p=3$.

On veut montrer que les seuls couples (p,r) vérifiant $r=\varphi(p^r-1)$ sont

$$(p,r)\in\{(2,1),(3,1),(2,2)\}.$$

Plus généralement, le lemme suivant permet de réduire le problème pour (p,rs) à un cas de base (p,r) dans un tour de divisibilité.

Lemme. *Soient p un premier et r et s des entiers dans $\mathbb{N}^*$ et soient $m=p^r-1$ et $n=p^{rs}-1$. Si la factorisation du polynôme cyclotomique $\Phi_m(x)\in\mathbb{F}_p[x]$ en irreductibles de degré r est :*

$$\Phi_m(x)=\prod_{i=1}^{t} f_i(x),$$

on obtient une factorisation partielle : $\Phi_n(x)=\prod_{i=1}^{t} g_i(x)$, où $g_i(x)$ divise $f_i(x^{n/m})$.

Démonstration. Par la définition des polynômes cyclotomiques,

$$\prod_{\substack{\ell\mid m\\ \ell\neq 1}}\Phi_{k\ell}(x)\;\Big|\;\frac{x^{km}-1}{x^k-1}=\frac{x^m-1}{x-1}(x^k)=\prod_{\substack{\ell\mid m\\ \ell\neq 1}}\Phi_\ell(x^k).$$

Par récurrence en k et m, on conclut que $\Phi_{km}(x)$ divise $\Phi_m(x^k)$, et la forme de la factorisation suit de la factorization $n=km$. □

On note que les trois propriétés sont équivalentes pour p, r, s et $n=p^{rs}-1$:

$$rs=\varphi(n),\quad \langle p\rangle=(\mathbb{Z}/n\mathbb{Z})^*,\quad \Phi_n(x)\in\mathbb{F}_p[x]\text{ est irreductble.}$$

Ces équivalences concernent un énoncé combinatoire, une égalité en théorie de groupes, et un énoncé en arithmétique des polynômes. Le lemma affirme que si $rs=\varphi(n)$ alors $r=\varphi(m)$ où $m=p^r-1$.

On applique ce lemme à $s>1$ et avec $n=p^{rs}-1$. On l'a déjà utilisé pour $r=1$, à conclure que $\Phi_n(x)$ n'est pas irreducible pour $p>3$ et $n=p^s-1$ car $\Phi_m(x)$ n'est pas irreducible pour $m=p-1$. Dans la suit, on va montrer qu'il n'existe pas $s>1$ premier tel que $\Phi_n(x)$ est pour les trois couples (p,r) connus tel que $\Phi_m(x)$ est irreductble : $(p,r)=(2,1)$ avec $m=1$, $(p,r)=(2,2)$ avec $m=3$, et $(3,1)$ avec $m=2$. On conclut qu'il n'y a pas d'entier $s>1$ tel que $\Phi_n(x)$ reste irreductible.

Notation. *On dit que (p,r) est un couple admissible si $r=\varphi(n)$ où $n=p^r-1$.*

Cas $(p,r)=(2,1)$. On sais que $(2,2)$ est un couple admissible, alors on traite des couples de la forme $(2,2s)$ dans la suite. Si s un premier impair, alors $n=2^s-1$ est impair, donc divisible par un premier ℓ impair. Il suit que

$$\operatorname{pgcd}(\ell-1,s)\,|\,\varphi(n)=\varphi(2^s-1),$$

et alors $\varphi(n)$ est pair, en particulier $2s \mid \varphi(n) \neq s$. Donc $(2, s)$ n'est pas un couple admissible.

Remarque. *Voir, par exemple, la factorisation de $\Phi_7(x) \in \mathbb{F}_2[x]$ pour $s = 3$, dans la suite des exercices.*

Cas $(p, r) = (2, 2)$. Par le cas précédent, on sait que (p, s) n'est pas admissible si s est un premier impair, alors (p, rs) n'est pas admissible non plus. Il reste à étudier $(p, rs) = (2, 4)$ avec $s = 2$, pour lequel

$$\varphi(n) = \varphi(15) = \varphi(3)\varphi(5) = 8 = 2rs,$$

donc $(2, 4)$ n'est pas admissible.

Remarque. *Voir la factorisation de $\Phi_{15}(x) \in \mathbb{F}_2[x]$ dans la suite des exercices.*

Cas $(p, r) = (3, 1)$. Si $s = 2$, le couple $(3, 2)$ n'est pas admissible car $\varphi(3^2 - 1) = \varphi(8) = 4 \neq rs = 2$.

Remarque. *En effet le polynôme $\Phi_8(x) = x^4 + 1 \in \mathbb{F}_3[x]$ factorise en deux polynômes quadratiques :*

$$x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1).$$

On suppose alors que s est un premier impair. Dans ce cas,

$$n = 3^s - 1 \equiv (-1)^s - 1 \equiv 2 \bmod 4,$$

alors $n/2$ est impair et $n/2 \geq (27 - 1)/2 = 13$. Par conséquent, n est divisible par un premier impair ℓ,

$$\operatorname{pgcd}(\ell - 1, s) \mid \varphi(n) = \varphi(3^s - 1),$$

et alors $\varphi(n)$ est pair, en particulier $2s \mid \varphi(n) \neq s$. Donc $(3, s)$ n'est pas un couple admissible.

4. Montrer qu'il existe un polynôme primitif de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r.

Solution. *On pose $q = p^r$ et $n = q - 1$. On a démontré que le polynôme cyclotomique $\Phi_n(x)$ se factorise en polynômes irreductibles de degrée r, qui sont primitifs (leurs racines sont d'ordre n dans $\overline{\mathbb{F}}_p$). Or, le degré $\varphi(n) = \deg(\Phi_n)$ est positif. Par conséquent, il existe au moins un polynôme primitif divisant Φ_n.*

5. Montrer qu'il existe un polynôme irréductible de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r.

Solution. *Cet exercice suit de l'exercice précédent. On note que tout polynôme irreductible de degré r est diviseur de $\Phi_m(x)$, où m divise $p^r - 1$ mais ne divise pas $p^s - 1$ pour $0 < s < r$.*

6. Démontrer l'unicité du corps de $q = p^r$ éléments en le décrivant comme corps de décomposition de $x^q - x$.

Solution. *Soit $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, et posons*

$$\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\}.$$

Alors $\mathbb{F}_q$ est l'ensemble de q racines du polynôme $x^q - x$. Soit $\pi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ l'automorphisme de Frobenius, donné pas $\pi(\alpha) = \alpha^p$. L'ensemble $\mathbb{F}_q$ est l'ensemble d'éléments satisfaisant $\pi^r(\alpha) = \alpha$ Le fait que π soit un homomorphisme implique que $\mathbb{F}_q$ est un sous-anneaux. Réciproquement, si K est un corps de q éléments, K est un corps de décomposition de $x^q - x$, et donc isomorphe à $\mathbb{F}_q$. (Ici on utilise l'isomorphisme des corps de décomposition d'un polynôme.)

7. Montrer que $x^p - x - a$ est irréductible dans $\mathbb{F}_p[x]$ pour tout a dans $\mathbb{F}_p^*$.

Solution. *Soit $A = \mathbb{F}_p[x]/(x^p - x - a)$, et écrire α pour l'image de x. On note que $\alpha^p = \alpha + a$ dans A. Si $f(x) \in \mathbb{F}_p[x]$ est une diviseur irreducible de $x^p - x - a$, on obtient un homomorphisme,*

$$\iota : A \longrightarrow K = \mathbb{F}_p[x]/(f(x)),$$

où K est un corps et $f(\iota(\alpha)) = 0$. On écrit ρ pour $\iota(\alpha)$, d'où

$$f(\rho^p) = f(\rho)^p = 0,$$

alors ρ^p est une autre racine de $f(x)$. Or

$$\rho^p = \iota(\alpha^p) = \iota(\alpha + a) = \iota(\alpha) + a = \rho + a.$$

Il suit que

$$\{\rho^{p^k} \mid k \in \mathbb{N}\} = \{\rho + ka \mid k \in \mathbb{F}_p\} = \rho + \mathbb{F}_p$$

est un ensemble de p racines de $f(x)$, et donc $f(x) = x^p - x - a$ car $\deg(f) = p$.

8. Déterminer la factorisation de $\Phi_7(x)$ dans $\mathbb{F}_2[x]$.

9. Décrire les éléments primitifs de $\mathbb{F}_{2^3}/\mathbb{F}_2$ et de $\mathbb{F}_{2^3}^*$ en termes de racines des polynômes cyclotomiques.

10. Déterminer la factorisation de $\Phi_{15}(x)$ dans $\mathbb{F}_2[x]$.

11. Décrire les éléments primitifs de $\mathbb{F}_{2^4}/\mathbb{F}_2$ et de $\mathbb{F}_{2^4}^*$ en termes des racines des polynômes cyclotomiques.

12. Trouver des isomorphismes :

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_5] = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1),$$

et

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x^3 + 1).$$

13. Montrer que $\phi(\alpha) = \alpha^p$ est un homomophisme d'anneaux $A \to A$ pour tout anneau A de caractéristique p premier. Il s'appelle l'endomorphisme de Frobenius (ou l'automorphisme de Frobenius lorsqu'il est un isomorphisme).

14. Montrer que tout homorphisme d'un corps K est injectif, et conclure que l'endomorphisme de Frobenius est un automorphisme dans le cas d'un corps fini.

15. Soit $\phi : \mathbb{F}_q \to \mathbb{F}_q$ l'automorphisme de Frobenius, où $q = p^r$. Déterminer les éléments fixés par ϕ et par ϕ^r.

16. Démontrer que $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle\phi\rangle$, un groupe cyclique d'ordre r.