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

Extensions de $\mathbb{F}_p$ et polynômes cyclotomiques

Exercices

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

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.)

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

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

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

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

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

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.

Aix-Marseille Université

Préparation à l'agrégation: Option C

https://www.i2m.univ-amu.fr/perso/david.kohel/tch/Agreg/

Factorisation des polynômes sur $\mathbb{F}_p$

Exercices

1. Soit p un premier et $r \in \mathbb{N}^*$. Montrer que $x^{p^r} - x$ est le produit de tous les polynômes irreducibles de $\mathbb{F}_p[x]$ de degré divisant r.

Indication. On rappelle que

$$x^{p^r} - x = \prod_{\alpha \in \mathbb{F}_{p^r}} (x - \alpha).$$

Or le polynôme minimal de chaque $\alpha \in \mathbb{F}_{p^r}$ est de degré divisant r.

2. Soit $f(x) = x^5 + x + 1 \in \mathbb{F}_3[x]$.

- **a.** Construire la matrice de l'endomorphisme de Frobenius ϕ, agissant sur l'anneau quotient $A = \mathbb{F}_3[x]/(f(x))$, dans la base $\{1, x, x^2, x^3, x^4\}$.
- **b.** Déterminer $\dim_{\mathbb{F}_3}(\ker(\phi - 1))$. Combien de diviseurs irreductibles a-t-il $f(x)$?
- **c.** Factoriser $f(x)$.

3. Soit $f(x) = x^4 + x + 1 \in \mathbb{F}_3[x]$ et poser $A = \mathbb{F}_3[x]/(f(x))$.

- **a.** Factoriser $f(x)$, en notant que 1 est une racine.
- **b.** Déterminer la structure de $A^*[2]$.
- **c.** Calculer des générateurs de $A^*[2]$ en utilisant le théorème chinois.

4. Soit $f(x) = x^4 + 1 \in \mathbb{F}_3[x]$ et poser $A = \mathbb{F}_3[x]/(f(x))$.

- **a.** Décrire la forme de la factorisation de $f(x)$, en notant que $f(x) = \Phi_8(x)$.
- **b.** Déterminer la structure de $A^*[2]$ (sans factoriser $f(x)$).
- **c.** Calculer des générateurs de $A^*[2]$, sachant la forme de la factorisation de $f(x)$.
- **d.** Factoriser $f(x)$ à l'aide des éléments de $A^*[2]$.

5. Soit $f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$.

- **a.** Décrire la forme de la factorisation de $f(x)$, en observant que

$$f(x) = (x^9 - 1)/(x - 1).$$

- **b.** Factorization $f(x)$ en utilisant le pcgd avec des polynômes adaptés.

6. Soit $f(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = \Phi_{15}(x) \in \mathbb{F}_2[x]$ et poser $A = \mathbb{F}_2[x]/(f(x))$.

- **a.** Décrire la forme de la factorisation de $f(x)$.
- **b.** Pour $i = 0, 1, 2, \ldots$, calculer

$$\mathrm{Tr}(x^i) = \sum_{j=0}^{3} x^{ip^j} \bmod f(x) \in A.$$

Pour est-ce qu'on obtient le même résultat pour $i = 1, 2, 4, 8 \ldots$?

- **c.** Expliquer pourquoi ces éléments appartient à un sous-anneau $B \cong \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$.
- **d.** En déduire la factorisation de $f(x)$.