

## Agrégation Interne Polynômes et corps finis

On pourra consulter les ouvrages suivants.

P. BOYER, J. J. RISLER : *Algèbre pour la licence 3. Groupes, anneaux, corps*. Dunod (2006).

F. COMBES — *Algèbre et géométrie*. Bréal (2003).

J. P. ESCOFFIER. *Toute l'algèbre de la licence*. Dunod (2006).

S. FRANCINO, H. GIANELLA, S. NICOLAS : *Exercices de mathématiques. Orlaux X-ENS. Algèbre 1*. Cassini (2001).

S. FRANCINO, H. GIANELLA. *Exercices de mathématiques pour l'agrégation. Algèbre 1*. Masson (1994).

F. LIRET. *Arithmétique*. Dunod (2011).

D. PERRIN. *Cours d'algèbre*. Ellipses (1996).

A. SZPIRGLAS. *Mathématiques L3. Algèbre*. Pearson (2009).

### – I – Caractéristique d'un anneau, d'un corps

**Définition 1** *Un corps est un anneau commutatif unitaire dans lequel tout élément non nul est inversible.*

Un corps est donc, a priori, commutatif.

Pour tout nombre premier  $p \geq 2$ ,  $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$  désigne le corps commutatif des classes résiduelles modulo  $p$ .

Pour cette partie,  $(\mathbb{K}, +, \cdot)$  est un corps.

Le sous-corps premier de  $\mathbb{K}$  est le plus petit sous-corps de  $\mathbb{K}$ .

On note  $\mathbb{K}_0$  le sous-corps premier de  $\mathbb{K}$ .

1. Rappeler la définition de la caractéristique d'un anneau commutatif unitaire.
2. Soient  $\mathbb{A} \subset \mathbb{B}$  deux anneaux commutatifs unitaires. Montrer qu'ils sont de même caractéristique.
3. Montrer que si  $\text{caract}(\mathbb{K}) = 0$ , le sous-corps premier  $\mathbb{K}_0$  de  $\mathbb{K}$  est alors infini isomorphe à  $\mathbb{Q}$  et dans le cas contraire, cette caractéristique est un nombre premier  $p \geq 2$  et  $\mathbb{K}_0$  est fini isomorphe à  $\mathbb{F}_p$ .
4. Montrer que si  $\mathbb{K}$  est fini, il est alors de cardinal  $p^n$ , où  $p \geq 2$  est un nombre premier.
5. Donner un exemple de corps infini de caractéristique  $p \geq 2$ .
6. Soit  $\mathbb{A}$  un anneau commutatif unitaire de caractéristique  $p \geq 2$ , où  $p$  est un nombre premier.

(a) Montrer que l'application :

$$\begin{aligned} \varphi : \mathbb{A} &\rightarrow \mathbb{A} \\ a &\mapsto a^p \end{aligned}$$

est un morphisme d'anneaux (morphisme de Frobenius).

(b) Soient  $n, r$  deux entiers naturels non nuls et  $a_1, \dots, a_r$  des éléments de  $\mathbb{A}$ . Montrer que :

$$\left( \sum_{i=1}^r a_i \right)^{p^n} = \sum_{i=1}^r a_i^{p^n}$$

7. Soient  $\mathbb{K}$  un corps de caractéristique  $p \geq 2$ ,  $n$  un entier naturel non nul et  $R$  un polynôme à coefficients dans  $\mathbb{K}_0$ . Montrer que :

$$\forall \lambda \in \mathbb{K}, (R(\lambda))^{p^n} = R(\lambda^{p^n})$$

8. Montrer qu'un corps fini commutatif ne peut être algébriquement clos.
9. Montrer que si  $\mathbb{K}$  est un corps fini commutatif alors toute application de  $\mathbb{K}$  dans  $\mathbb{K}$  est polynomiale.
10. Montrer que tout polynôme irréductible dans un corps de caractéristique nulle est premier avec son polynôme dérivé.  
Que se passe-t-il pour  $\mathbb{K}$  de caractéristique  $p \geq 2$ .

## – II – Polynômes irréductibles dans $\mathbb{F}_p$ et corps finis

Pour cette partie,  $p \geq 2$  est un nombre premier.

Pour tout entier  $n \in \mathbb{N}^*$ , on note  $\mathcal{U}_n(p)$  l'ensemble de tous les polynômes unitaires irréductibles de degré  $n$  dans  $\mathbb{F}_p[X]$  et  $I_n(p)$  le cardinal de  $\mathcal{U}_n(p)$ .

L'ensemble  $\mathcal{U}_n(p)$  peut, a priori, être vide.

Pour tout entier  $n \in \mathbb{N}^*$ , on note  $\mathcal{D}_n$  l'ensemble de tous les diviseurs de  $n$  dans  $\mathbb{N}^*$ .

1. Soient  $\mathbb{K}$  un corps et  $P \in \mathbb{K}[X]$  un polynôme unitaire de degré  $n \geq 1$ .
  - (a) Montrer que l'algèbre  $\frac{\mathbb{K}[X]}{(P)}$  est de dimension  $n$  et  $(\overline{X^k})_{0 \leq k \leq n-1}$  en est une base.
  - (b) Montrer que les conditions suivantes sont équivalentes :
    - i.  $\frac{\mathbb{K}[X]}{(P)}$  est un corps ;
    - ii. l'anneau  $\frac{\mathbb{K}[X]}{(P)}$  est intègre ;
    - iii. le polynôme  $P$  est irréductible.
2. Montrer que pour tout polynôme  $P \in \mathcal{U}_n(p)$ , l'anneau quotient  $\frac{\mathbb{F}_p[X]}{(P)}$  est un corps fini de cardinal  $p^n$  et peut être muni d'une structure de  $\mathbb{F}_p$ -espace vectoriel de dimension  $n$ .
3. Calculer  $I_1(p)$  et  $I_2(p)$ .
4. Donner tous les polynômes unitaires de degré 2 irréductibles dans  $\mathbb{F}_2[X]$  et dans  $\mathbb{F}_3[X]$ .
5.
  - (a) Montrer que le polynôme  $P(X) = X^4 + X^3 + 1$  est irréductible dans  $\mathbb{F}_2[X]$ . En déduire un corps à 16 éléments. Nous noterons  $\mathbb{F}_{16}$  ce corps.
  - (b) Montrer que le groupe multiplicatif  $\mathbb{F}_{16}^*$  est cyclique engendré par un élément  $\omega$  de  $\mathbb{F}_{16}^*$  racine du polynôme  $P$ .
  - (c) Montrer que  $\omega, \omega^2, \omega^4$  et  $\omega^8$  sont les racines du polynôme  $X^4 + X^3 + 1$  dans  $\mathbb{F}_{16}$ .
  - (d) Montrer que la famille  $(\omega, \omega^2, \omega^4, \omega^8)$  est une base de  $\mathbb{F}_{16}$  sur  $\mathbb{F}_2$ .
6. Soient  $n$  un entier naturel nul et :

$$P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$$

- (a) Soient  $d \in \mathbb{N}^*$ ,  $P \in \mathcal{U}_d(p)$  et  $\mathbb{F}_{p^d} = \frac{\mathbb{F}_p[X]}{(P)}$ . Montrer que :

$$\forall k \in \mathbb{N}, \forall \overline{Q} \in \mathbb{F}_{p^d}, \overline{Q}^{p^{kd}} = \overline{Q}$$

- (b) Montrer que, pour tout  $d \in \mathcal{D}_n$ ,  $\mathcal{U}_d(p)$  est l'ensemble de tous les polynômes unitaires irréductibles de degré  $d$  dans  $\mathbb{F}_p[X]$  qui divise le polynôme  $P_n$ .

- (c) Montrer que si  $P \in \mathcal{U}_d(p)$  est un diviseur de  $P_n$ , l'entier  $d = \deg(P)$  est alors un diviseur de  $n$ .
- (d) Montrer que le polynôme  $P_n(X) = X^{p^n} - X$  est sans facteurs carrés dans  $\mathbb{F}_p[X]$  et en déduire que :

$$X^{p^n} - X = \prod_{d \in \mathcal{D}_n} \prod_{P \in \mathcal{U}_d(p)} P$$

7. Déduire de ce qui précède un algorithme de calcul des  $I_n(p) = \text{card}(\mathcal{U}_n(p))$ .
8. Donner tous les polynômes unitaires de degré 4 irréductibles dans  $\mathbb{F}_2[X]$ .
9. Montrer que pour tout entier  $n \in \mathbb{N}^*$ , il existe dans  $\mathbb{F}_p[X]$  des polynômes irréductibles de degré  $n$ .
10. Soient  $n$  un entier naturel non nul,  $P$  un polynôme unitaire et irréductible de degré  $n$  dans  $\mathbb{F}_p[X]$  et  $\mathbb{F}_{p^n}$  le corps  $\frac{\mathbb{F}_p[X]}{(P)}$ .

On désigne par  $\mathbb{K}$  un autre corps à  $p^n$  éléments.

Comme  $\mathbb{K}$  est de caractéristique  $p$ , le corps  $\mathbb{F}_p$  peut être identifié au sous-corps premier de  $\mathbb{K}$  et un polynôme dans  $\mathbb{F}_p[X]$  à un polynôme dans  $\mathbb{K}[X]$ .

- (a) Montrer que le polynôme  $P$  a des racines dans  $\mathbb{K}$ .
- (b) En déduire l'existence d'un isomorphisme de corps de  $\mathbb{F}_{p^n}$  sur  $\mathbb{K}$ .

Donc, à un isomorphisme près, il n'existe qu'un seul corps à  $p^n$  éléments, c'est  $\mathbb{F}_{p^n} = \frac{\mathbb{F}_p[X]}{(P)}$

où  $P \in \mathcal{U}_n(p)$ .

11. On se donne un entier  $n \geq 1$  et on note  $G$  le groupe des automorphismes de corps de  $\mathbb{F}_{p^n}$ .
- (a) Montrer que l'application  $\alpha : \lambda \mapsto \lambda^p$  est un automorphisme de corps de  $\mathbb{F}_{p^n}$ .
- (b) Montrer que  $\alpha$  est d'ordre  $n$  dans  $G$ .
- (c) Montrer que  $G$  est un groupe cyclique engendré par  $\alpha$ .