Agrégation Externe
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. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).

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

F. Liret. *Arithmétique.* Dundod (2011).

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

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

– I – Caractéristique 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 $p \geq 2$, $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ 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 $\mathbb{K}$.

L'application :

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & \mathbb{K} \\ & n & \mapsto & n \cdot 1 \end{array}$$

est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{K}$.

Son noyau étant un idéal de l'anneau principal $\mathbb{Z}$, il existe un unique entier naturel p tel que :

$$\ker(\varphi) = \{n \in \mathbb{Z} \mid n \cdot 1 = 0\} = p\mathbb{Z}$$

Définition 2 *L'entier p ainsi défini est la caractéristique de $\mathbb{K}$.*

On note $\text{caract}(\mathbb{K})$ cette caractéristique.

1. 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 $\mathbb{F}_p$.
2. Soient $\mathbb{K} \subset \mathbb{L}$ deux corps. Montrer qu'ils sont de même caractéristique.
3. Montrer que si $\mathbb{K}$ est fini, il est alors de cardinal p^n, où $p \geq 2$ est un nombre premier.
4. Donner un exemple de corps infini de caractéristique $p \geq 2$.
5. Soit $\mathbb{K}$ un corps commutatif de caractéristique $p \geq 2$.
   (a) Soient n, r deux entiers naturels non nuls et $\lambda_1, \cdots, \lambda_r$ des éléments de $\mathbb{K}$. Montrer que :

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

(b) Soient n un entier naturel non nul et R un polynôme à coefficients dans $\mathbb{K}_0$. Montrer que :

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

– II – Polynômes irréductibles dans $\mathbb{F}_p$

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

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

L'ensemble $\mathcal{U}_n\left(p\right)$ 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. Montrer que pour tout polynôme $P \in \mathcal{U}_n\left(p\right)$, l'anneau quotient $\dfrac{\mathbb{F}_p\left[X\right]}{\left(P\right)}$ est un corps fini de cardinal p^n, ce corps pouvant être muni d'une structure de $\mathbb{F}_p$-espace vectoriel de base $\left(\overline{X}^k\right)_{0\leq k\leq n-1}$.
2. Calculer $I_1\left(p\right)$ et $I_2\left(p\right)$.
3. Donner tous les polynômes unitaires de degré 2 irréductibles dans $\mathbb{F}_2\left[X\right]$ et dans $\mathbb{F}_3\left[X\right]$.
4. Montrer que le polynôme $P\left(X\right) = X^4 + X^3 + 1$ est irréductible dans $\mathbb{F}_2\left[X\right]$. En déduire un corps à 16 éléments.
5. Soient n un entier naturel nul et :

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

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

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

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

(c) Montrer que si $P \in \mathcal{U}_d\left(p\right)$ est un diviseur de P_n, l'entier $d = \deg\left(P\right)$ est alors un diviseur de n.

(d) Montrer que le polynôme $P_n\left(X\right) = X^{p^n} - X$ est sans facteurs carrés dans $\mathbb{F}_p\left[X\right]$ et en déduire que :

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

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

   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 $\mathbb{F}_p\left[X\right]$ à un polynôme dans $\mathbb{K}\left[X\right]$.

   (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, a un isomorphisme près, il n'existe qu'un seul corps à p^n éléments, c'est $\mathbb{F}_{p^n} = \dfrac{\mathbb{F}_p[X]}{(P)}$ où $P \in \mathcal{U}_n(p)$.

10. Montrer qu'un corps fini ne peut être algébriquement clos.
11. Montrer que si $\mathbb{K}$ est un corps fini alors toute application de $\mathbb{K}$ dans $\mathbb{K}$ est polynomiale.
12. 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 α est d'ordre n dans G.
    (c) Montrer que G est un groupe cyclique engendré par α.
13. 31 vacanciers se trouvent sur le même bateau durant le mois de Juillet. Le capitaine peut inviter chaque soir 6 personnes à sa table. Peut-il faire ces invitations chaque soir du mois de Juillet de sorte que chaque vacancier se soit rencontré une fois et une seule ?