Leçon 123 : Corps finis. Applications.

Mathieu Alix

–

1 Rapport du Jury

« La construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Le calcul des degrés des extensions, le théorème de la base télescopique, les injections des divers $\mathbb{F}_q$ sont incontournables. La structure du groupe multiplicatif doit aussi être connue.

Des applications des corps finis (y compris pour $\mathbb{F}_q$ avec q non premier !) ne doivent pas être oubliées. Par exemple, l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont des pistes intéressantes.

Les candidates et candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductiblilité des polynômes à coefficients dans un corps fini. »

2 Questions classiques

1. Donner une façon de construire $\mathbb{F}_4$ puis exhiber un générateur du groupe des éléments inversibles.

   Solution: $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$. En effet, le polynôme X^2+X+1 n'a pas de racine dans $\mathbb{F}_2$, donc il est irréductible sur $\mathbb{F}_2$. $\mathbb{F}_4^\times$. est cyclique d'ordre 3 donc tout élément de $\mathbb{F}_4$ distinct de 0 et 1 engendre $\mathbb{F}_4^\times$. Par conséquent, la classe de X (ou celle de $X+1$) engendre le groupe des inversibles de $\mathbb{F}_2[X]/(X^2+X+1)$.

2. Soit $n \geq 2$ et p un nombre premier. Montrer que $p = 1 \mod [n]$ si et seulement si $\mathbb{F}_p$ contient une racine primitive n-ième de l'unité.

   Solution: Le groupe $\mathbb{F}_p^\times$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$ (c'est un groupe cyclique d'ordre $p-1$). Alors $\mathbb{F}_p$ contient une racine primitive n-ième de l'unité ssi ce groupe admet un élément d'ordre n ssi n divise $p-1$ ssi $p = 1 \mod [n]$.

3. Déterminer le nombre de polynômes unitaires irréductibles de degré 2 sur $\mathbb{F}_3$. Combien y'a-t-il de polynômes unitaire de degré 2 sur $\mathbb{F}_3$, exhiber ceux qui sont irréductibles et en déduire une construction de $\mathbb{F}_9$.

Solution: Le développement classique d'agrégation donne que le nombre de polynôme irréductible de degré n sur $\mathbb{F}_p$ est :

$$I(p,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

On en déduit pour $n = 2, p = 3$, que $I(3,2) = \frac{1}{2}(\mu(2) \times 3 + \mu(1) \times 3^2) = 3$. On vérifie de plus que ces 3 polynômes irréductibles sont X^2+1, X^2+X-1, X^2-X-1. Il y avait au total 9 polynômes unitaires de degré 2 (3 choix pour chaque coefficient). On en déduit par exemple que

$$\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+X-1)$$

4. Soient p premier, $n \in \mathbb{N}^*$ et $q = p^n$. Montrer que toute application f de $\mathbb{F}_q$ dans lui-même, il existe un unique polynôme de degré $\leq q-1$ à coefficients dans $\mathbb{F}_q$ tel que $\forall t \in \mathbb{F}_q, f(t) = P(t)$.

Solution: Notons $\mathbb{F}_q = \{z_1, \dots, z_q\}$. Pour P un polynôme de degré $\leq q-1$ à coefficients dans $\mathbb{F}_q$, noté $P(X) = \sum_{k=0}^{q-1} a_k X^k$, on a l'équivalence

$$\begin{aligned}\forall t \in \mathbb{F}_q, f(t) = P(t) &\Leftrightarrow \forall i \in [\![1,q]\!], f(z_i) = P(z_i) \\ &\Leftrightarrow \forall i \in [\![1,\ q]\!], \sum_{k=0}^{q-1} a_k z_i^k = f(z_i)\end{aligned}$$

La dernière équivalence correspond donc à un système linéaire de q équations à q inconnues $a_0, \dots, a_{q-1}$, dont la matrice est la matrice de Vandermonde $(z_i^k)_{\substack{1\leq i\leq q \\ 0\leq k\leq q-1}}$. Or comme les z_i sont tous distincts, cette matrice est inversible. Le système associé est donc de cramer, il admet une unique solution ; et il existe un unique polynôme de degré $\leq q-1$ à coefficients dans $\mathbb{F}_q$ tel que $\forall t \in \mathbb{F}_q, f(t) = P(t)$.
Remarque : On vient finalement de montrer que toute application de $\mathbb{F}_q$ dans $\mathbb{F}_q$ est une fonction polynomiale.

5. (Théorème de l'élément primitif pour les corps finis) : Soit K un corps fini et L une extension de degré fini de K, alors il existe $\xi \in L$ tel que $L = K(\xi)$.

Solution: Notons $m = [L : K] \in \mathbb{N}^*$. Alors L est un K-ev de dimension m, et donc est isomorphe en tant que K-ev à K^m. Il suit que $|L| = |K|^m$, et donc que L est un corps fini. Le groupe multiplicatif L^* est cyclique, dont on note ξ un générateur. En notant p la caractéristique commune à K et L, on a donc la tour d'extension $\mathbb{F}_p \subseteq K \subseteq L$, et par propriété (prop VII.10 [GOZ] par ex.), on tire que $L = \mathbb{F}_p(\xi)$, mais puisque $\mathbb{F}_p \subseteq K$, alors $L = \mathbb{F}_p(\xi) \subseteq K(\xi) \subseteq L$ d'ou l'égalité attendu.

6. Montrer que si K est un corps fini et $n \in \mathbb{N}^*$ alors il existe un polynôme irréductible de degré n sur K.

Solution: Comme K est un corps fini, il existe p premier et $e \in \mathbb{N}^*$ tels que $|K| = p^e$, et que K est $\mathbb{F}_p$ isomorphe à $\mathbb{F}_{p^e}$. Considérons $L = \mathbb{F}_{p^{en}}$, alors par propriété d'inclusion des corps finis, on a $K \subseteq L$. Par le théorème de l'élément primitif, il existe $\zeta \in L$ tel que $L = K(\zeta)$. En notant P le polynôme minimal (irréductible) de ζ dans $K[X]$, dont on note d son degré, alors L est une extension de degré d, et L est K-ev de dimension d, ainsi $L \simeq K^d$, et donc $|L| = |K|^d = p^{ed}$. Or $|L| = p^{en}$, donc $d = n$. Ainsi P convient.

7. Treillis des extensions de $\mathbb{F}_2$ jusqu'au degré 10. (parlez des inclusions CNS ?).

3 Questions plus exotiques

1. Soient p un nombre premier, $n \in \mathbb{N}^*$, et r un entier naturel non-nul.
   (a) Montrer que si r est premier avec $p^n - 1$ alors tout élément de $\mathbb{F}_{p^n}$ est une puissance r-ième.
   (b) Montrer que si $r | p^n - 1$, alors pour $\alpha \in \mathbb{F}_{p^n}^*$, on a l'équivalence

$$\alpha \text{ est une puissance } r - \text{ième} \Leftrightarrow \alpha^{(p^n-1)/r} = 1.$$

Solution: On commence par remarque que $0 = 0^r$. On ne s'intéresse donc seulement qu'aux éléments de $\mathbb{F}_{p^n}^*$, qui est un groupe cyclique d'ordre $p^n - 1$.

a) Comme r est premier avec $p^n - 1$, alors par le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}$, tel que $ur + (p^n - 1)v = 1$. Alors en considérant $\alpha \in \mathbb{F}_{p^n}^*$, par le théorème de Lagrange, $\alpha^{p^n-1} = 1$, ainsi $\alpha = \alpha^{ur+(p^n-1)v} = (\alpha^u)^r$, et donc tout élément est une puissance r-ième.

b) On suppose que $r | p^n - 1$, et on note d le quotient de $p^n - 1$ par r. Considérons $\alpha \in \mathbb{F}_{p^n}^*$.

- S'il existe $\beta \in \mathbb{F}_{p^n}^*$ tel que $\alpha = \beta^r$, alors $\alpha^{(p^n-1)/r} = \beta^{p^n-1} = 1$ par le théorème de Lagrange.
- Supposons maintenant que $\alpha^{(p^n-1)/r} = 1$, et considérons ξ un générateur fixé du groupe cyclique $\mathbb{F}_{p^n}^*$. il existe un unique $j \in [\![0, p^n - 1]\!], \alpha = \xi^j$. Ainsi, $\xi^{j(p^n-1)/r} = 1$ et donc $o(\xi) = p^n - 1 | \frac{j(p^n-1)}{r}$, ce qui revient à dire que $r | j$. On en conclut que $\alpha \in \{\xi^0, \xi^r, \xi^{2r}, \ldots, \xi^{(d-1)r}\}$, c'est-a-dire qu'il existe $k \in [\![0, d-1]\!]$ tel que $\alpha = \xi^{kr} = (\xi^k)^r$ et donc que α est une puissance r-ième.

La suite a un intérêt si la personne connait la réciprocité quadratique - Il serait bien selon moi de s'y intéresser tout de même.

2. Calculer $\left(\frac{23}{59}\right)$. (Déterminer si 23 est un carré dans $\mathbb{F}_{59}$)

Solution: En utilisant la réciprocité quadratique, les propriétés de multiplicativité du symbole de Legendre, et enfin que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ pour tout nombre premier $p > 2$, on tire

$$\left(\frac{23}{59}\right) = (-1)^{11\times 29}\left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = -(-1)^{6\times 11}\left(\frac{23}{13}\right) = -\left(\frac{10}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$$

$$= -(-1)^{21}\left(\frac{5}{13}\right) = (-1)^{12}\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = (-1)^{2}\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$