

# 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  $F_q$  sont incontournables. La structure du groupe multiplicatif doit aussi être connue. Des applications des corps finis (y compris pour  $F_q$  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'irréductibilité des polynômes à coefficients dans un corps fini.

## Références

- [Cours d'Algèbre - Daniel Perrin](#)
- [Théorie de Galois - Escofier](#)
- [Théorie de Galois - I. Gozard](#)
- [Algèbre - le Grand combat - Berhuy](#)
- [Corps commutatifs et théorie de Galois - Tauvel](#)

## Développements

- [Cyclotomie](#) (réductibilité sur  $F_q$ )
- [Norme d'une extension](#) (carrés de  $\mathbb{F}_q$ )

## Méta-plan

1. Construction des corps finis
  1. Extension de rupture, extension de décomposition
  2. Existence et unicité des corps finis
2. Morphismes et corps finis
  1. Injection de corps finis. Clôture algébrique.
  2. Groupe d'automorphismes. Cyclotomie.

3. Etude des carrés dans les corps finis
  1. Loi de réciprocité quadratique.
  2. Norme d'une extension de corps

## Plan détaillé

### I - Construction des corps finis [Berhuy]

#### 1 - Extension de rupture, extension de décomposition

1. Définition : extension de rupture.
2. Définition : extension de décomposition
3. Exemple : On considère  $P = X^3 - 2 \in \mathbb{Q}[X]$ . Alors  $\mathbb{Q}(\sqrt[3]{2})$  est un corps de rupture de  $P$ .  $\mathbb{Q}(\sqrt[3]{2}, j)$  est un corps de décomposition de  $P$ .  $\mathbb{C}$  n'est ni l'un ni l'autre.
4. Proposition : soit  $L/K$  une extension de corps,  $\alpha \in L$  algébrique sur  $K$ . Alors on a l'isomorphisme d'extensions de  $K$  :

$$K(\alpha) \cong K[X]/\langle \pi_\alpha \rangle$$

5. Théorème : existence et unicité du corps de rupture
6. Théorème : existence et unicité du corps de décomposition

#### 2 - Existence et unicité des corps finis

1. Lemme : soit  $K$  un corps fini. Alors la caractéristique de  $K$  est un nombre premier.
2. Corollaire : si  $K$  est un corps fini, il existe  $p$  un nombre premier, il existe  $n \in \mathbb{N}^*$  tel que  $K$  soit de cardinal  $p^n$ .
3. Application : il n'existe pas de corps de cardinal 6.

| Dans toute la suite, on fixe  $p$  un nombre premier.

4. Lemme : soit  $K$  un corps de cardinal  $p^n$ . Alors, pour  $L/K$  une extension quelconque,  $K$  est l'ensemble des racines de  $X^{p^n} - X$  dans  $L$ .
5. Théorème : existence et unicité des corps finis (version décomposition)
6. Exemple : le corps à 2 éléments  $\mathbb{F}_2$  est isomorphe à  $\mathbb{Z}/2\mathbb{Z}$ . Le corps à 4 éléments  $\mathbb{F}_4$  est une extension de  $\mathbb{F}_2$  dont on donne la table de multiplication en annexe.

**En particulier,  $\mathbb{F}_4$  n'est pas  $\mathbb{Z}/4\mathbb{Z}$ .**

7. Proposition : Soit  $G$  un sous-groupe fini du groupe multiplicatif d'un corps. Alors  $G$  est cyclique.
8. Application : Soit  $L/K$  une extension de corps avec  $L$  un corps fini. Il existe  $\alpha \in L$  tel que  $L = K[\alpha]$ .

## **II - Corps finis, morphismes et polynômes** Théorie de Galois - Escofier

On fixe  $p$  un nombre premier et  $q = p^r$  avec  $r \in \mathbb{N}^*$ .

### **1 - Injection de corps finis.**

1. Théorème : Soit  $L$  un corps fini. Il existe une injection de  $\mathbb{F}_q$  dans  $L$  si, et seulement si,  $L$  est de cardinal  $p^{rs}$ ,  $s \in \mathbb{N}^*$ . Dans ce cas, une telle injection est unique.
2. Corollaire : Les sous-corps de  $\mathbb{F}_q$  sont exactement les  $\mathbb{F}_{p^d}$  avec  $d|r$ .  $\mathbb{F}_q$  contient exactement une copie de chacun de ses corps.
3. Corollaire :  $X^{q^r} - X$  est le produit de tous les irréductibles unitaires de degré  $r$  de  $\mathbb{F}_q[X]$ .
4. Application : soit  $P \in \mathbb{F}_q[X]$  unitaire de degré  $r$ .  $P$  est irréductible si, et seulement si,  $P \mid X^{q^r} - X$  et pour tout  $d$  diviseur strict de  $r$ ,  $P$  ne divise pas  $X^{q^d} - X$ .

### **2 - Groupe d'automorphismes**

1. Définition (morphisme de Frobenius) : soit  $L/\mathbb{F}_q$  une extension finie. Le morphisme  $F_q : x \mapsto x^q$  est un automorphisme de l'extension appelé morphisme de Frobenius
2. Lemme : soit  $L$  un corps fini dont le cardinal est une puissance de  $q$ . L'ensemble des points fixes de  $F_q$  est un sous-corps de  $L$  isomorphe à  $\mathbb{F}_q$ .
3. Corollaire : soit  $P$  un polynôme sans facteur irréductible carré de  $\mathbb{F}_q[X]$ . L'ensemble des points fixes de l'application  $\mathbb{F}_q$ -linéaire  $x \mapsto x^q$  de l'algèbre  $\mathbb{F}_q[X]/\langle P \rangle$  est un  $\mathbb{F}_q$ -espace vectoriel dont la dimension est le nombre de facteurs carrés de  $P$ .
4. Application : algorithme de Berlekamp
5. Théorème : soit  $L/\mathbb{F}_q$  une extension finie. Le groupe d'automorphismes  $\text{Aut}_{\mathbb{F}_q}(L)$  est cyclique d'ordre  $[L : \mathbb{F}_q]$ , engendré par  $F_q$ . (DVT 1)

6. Définition : polynôme cyclotomique
7. Lemme : relation de récurrence
8. Lemme : Soit  $n$  premier avec  $p$ .  $\Phi_{n, \mathbb{F}_q}$  est à coefficients dans  $\mathbb{F}_p$ , et vaut  $\overline{\Phi_{n, \mathbb{Q}}}$ .
9. Théorème : Si  $n$  est premier avec  $p$ , les facteurs irréductibles de  $\Phi_{n, \mathbb{F}_q}$  dans  $\mathbb{F}_q[X]$  sont tous de degré  $s$ , où  $s$  est l'ordre de  $q$  dans  $\mathbb{Z}/n\mathbb{Z}$ . (DVT 1)
10. Application :  $\Phi_{8, \mathbb{Q}}$  est un polynôme irréductible dans  $\mathbb{Q}[X]$  et  $\mathbb{Z}[X]$  mais dont le projeté dans n'importe quel corps fini est réductible. (DVT 1)

### III - Etude des carrés d'un corps fini

On suppose dans toute cette partie que  $p$  est un nombre premier **impair**.

#### 1 - Le groupe des carrés [Mathématiques pour l'Agrégation \(Algèbre\) - J.E. Rombaldi](#)

1. Lemme : l'ensemble  $K^\times$  des carrés de  $\mathbb{F}_q^\times$  est un groupe de cardinal  $\frac{q-1}{2}$ . Ses éléments sont exactement les racines de  $X^{\frac{q-1}{2}} - 1$ .
2. Corollaire : Pour tout  $a, b \neq 0$  et  $c \in \mathbb{F}_q$ , l'équation  $ax^2 + by^2 = c$  d'inconnue  $x, y \in \mathbb{F}_q$  admet au moins une solution.
3. Application : Soit  $(E, \phi)$  un  $\mathbb{F}_q$ -espace quadratique de dimension finie et  $(1, \alpha)$  un système de représentants de  $\mathbb{F}_q^\times / K^\times$ . Il existe un unique  $r \in \mathbb{N}$  et un unique  $\delta \in \{1, \alpha\}$  tels que, dans une certaine base de  $E$ , la matrice de  $\phi$  ait pour forme

$$\begin{pmatrix} I_{r-1} & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

4. Corollaire : Le discriminant détermine complètement les orbites de congruences dans  $GL_n(\mathbb{F}_q)$ .

#### 2 - Loi de réciprocité quadratique [Berhuy]

1. Définition (symbole de Legendre)
2. Lemme : le symbole de Legendre  $(a/p)$  ne dépend que de la classe de  $a$  modulo  $p$ . De plus  $a^{\frac{p-1}{2}} \equiv (a/p)[p]$ .
3. Théorème (loi de réciprocité quadratique, admis)
4. Théorème (lois complémentaires)
5. Exemple explicite

### 3- Carrés de $\mathbb{F}_q$ [Tauvel + de mémoire]

Soit  $L/K$  une extension de corps algébrique.

1. Lemme :

$$\begin{aligned}\mathbb{L} &\rightarrow \text{Hom}_K(L) \\ \alpha &\mapsto (m_\alpha : x \mapsto \alpha x)\end{aligned}$$

est un morphisme de  $K$  algèbres injectif.

2. Définition : Norme

3. Exemples :  $N(0)$ .  $N(K)$ .

4. Proposition : Multiplicativité de la norme (DVT 2)

5. Proposition :  $N(\alpha) = (-1)^n (\pi_\alpha(0))^{n/d}$ . Si de plus  $\pi_\alpha$  est scindé dans  $L$ , on a l'égalité avec les racines. (DVT 2)

On fixe  $q$  une puissance non nulle de  $p$ .

6. Théorème :  $\alpha$  est un carré dans  $\mathbb{F}_q$  si, et seulement si,  $N(\alpha)$  est un carré dans  $\mathbb{F}_p$ . (DVT 2)

7. Exemple : calculs explicites