# 123. Corps finis. Applications.

**Introduction** : Les corps finis ayant la propriété d'être constructibles de façon effective, ils sont très utilisés en cryptographie et pour les codes correcteurs d'erreurs.

# 1 Construction des corps finis

## 1.1 Corps de cardinal premier

**Théorème 1.** Soit $n \in \mathbb{N}^*$. $\mathbb{Z}/n\mathbb{Z}$ est un corps *ssi* $n$ est premier.

***Application*** (Wilson)**.** *Soit $p \in \mathbb{N}^*$. $p$ est premier* ssi $(p-1)! \equiv -1[p]$.

Pour $p \in \mathbb{N}^*$ premier, on notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Y en a-t-il d'autres ?

***Exemple.*** *$\mathbb{F}_2/(X^2+X+1)$ est un corps à 4 éléments.*

## 1.2 Corps de cardinal primaire

Soit $F$ un corps fini.

**Définition 1.** On appelle sous-corps premier le plus petit sous-corps de $F$.

**Lemme 1.** Soit $\varphi : \mathbb{Z} \to F$ défini par $\varphi(n) = n \cdot 1_F$. C'est un morphisme d'anneaux, son noyau est donc un idéal de $\mathbb{Z}$, de la forme $p\mathbb{Z}$ avec $p$ premier. $p$ est le cardinal du sous-corps premier de $F$, et celui-ci est isomorphe à $\mathbb{F}_p$.

**Définition 2.** $p$ est appelé caractéristique de $F$.

***Contre-exemple.*** *$\mathbb{F}_2(X)$ est un corps infini de caractéristique finie* 2*.*

**Proposition 1.** $F$ possède une structure de $\mathbb{F}_p$-espace vectoriel de dimension finie. Ainsi, il existe $n \in \mathbb{N}^*, |F| = p^n$.

**Proposition 2.** Soit $F$ un corps fini de caractéristique $p$. L'application $\varphi : F \to F$ définie par $\varphi(x) = x^p$ est un automorphisme de $F$ (et l'identité si $F = \mathbb{F}_p$).

***Application*** (Fermat)**.** *Soit $p$ premier, alors pour tout $a \in \mathbb{Z}, a^p \equiv a[p]$.*

**Théorème 2.** Réciproquement, soit $p \in \mathbb{N}^*$ premier, soit $q = p^n$. Il existe un corps de cardinal $q$, c'est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. De plus, si $F, F'$ sont deux corps de cardinal $q$, alors ils sont $\mathbb{F}_p$-isomorphes.

# 2 Structure des corps finis

## 2.1 Éléments inversibles

**Proposition 3.** Soit $p$ premier, soit $q = p^r$. Alors $\mathbb{F}_q^*$ est un groupe cyclique.

**Corollaire 1.** Il existe $\zeta \in \mathbb{F}_q, \mathbb{F}_q = \mathbb{F}_p[\zeta]$.

## 2.2 Éléments carrés

**Définition 3.** Soit $\mathbb{F}_q$ corps fini de caractéristique $p$. On note $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$, on définit de même $(\mathbb{F}_q^*)^2$.

**Proposition 4.** Si $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p > 2$, on a $|F_q^2| = \frac{q+1}{2}$.

**Proposition 5.** On suppose $p > 2$, soit $x \in \mathbb{F}_q^*$. Alors $x \in \mathbb{F}_q^2 \Leftrightarrow x^{\frac{q-1}{2}} = 1$.

**Corollaire 2.** $-1 \in \mathbb{F}_q^2 \Leftrightarrow q \equiv 1[4]$.

***Application.*** *Il existe une infinité de nombres premiers de la norme $4m+1, m \in \mathbb{N}$.*

**Lemme 2.** Pour tous $\alpha, \beta \in \mathbb{F}_q$, l'équation $\alpha x^2 + \beta y^2 = 1$ d'inconnues $x, y \in \mathbb{F}_q$ admet au moins une solution.

**Théorème 3.** Soit $\mathbb{F}_q$ un corps fini de caractéristique différente de 2. Alors il y a $2n+1$ orbites pour l'action de congruence sur $S_n(\mathbb{F}_q)$, représentées par les matrices $A = \begin{pmatrix} I_r & \\ & 0_{n-r} \end{pmatrix}$ et $B = \begin{pmatrix} I_{r-1} & & \\ & \alpha & \\ & & 0_{n-r} \end{pmatrix}$, où $\alpha \in \mathbb{F}_q^* \backslash \mathbb{F}_q^2$.

**Définition 4.** Soit $p$ premier.
On définit pour $a \in \mathbb{F}_p^*$ le symbole de Legendre $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^2 \\ -1 & \text{sinon} \end{cases}$.

**Proposition 6.** On a, pour tout $a \in \mathbb{F}_p^*, \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

**Théorème 4** (Frobenius-Zolotarev)**.** Soit $p \geq 3$ premier, soit $u \in GL_n(\mathbb{F}_p)$. Alors $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

**Théorème 5** (Réciprocité quadratique)**.** Soient $p, q$ premiers.
Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

***Exemple.*** *65 est un carré dans $\mathbb{F}_{29}$.*

### 2.3 Sous-corps

**Proposition 7.** Soit $\mathbb{F}_q$ corps de cardinal $q = p^r$. Si $K$ est un sous-corps de $\mathbb{F}_q$, alors il existe $d$ diviseur de $n$ tel que $|K| = p^d$. Réciproquement, pour tout $d$ diviseur de $n$, $\mathbb{F}_q$ possède un unique sous-corps de cardinal $p^d$.

***Contre-exemple.*** *$\mathbb{F}_{16}$ n'a pas de sous-corps de cardinal 8.*

## 3 Applications

### 3.1 Irréductibilité et factorisation de polynômes

**Théorème 6.** Soit $p$ premier, $q = p^n, n \in \mathbb{N}^*$. Alors, pour tout $P \in \mathbb{F}_p[X]$ irréductible de degré $n$, $\mathbb{F}_q$ est isomorphe à $\mathbb{F}_p/(P)$.

**Corollaire 3.** Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$. De plus, si $P \in \mathbb{F}_p[X]$ irréductible, son corps de rupture est aussi son corps de décomposition.

**Lemme 3.** Soit $P \in \mathbb{F}_q[X], \deg(P) = n$, soit $E = \mathbb{F}_q[X]/(P)$. On a $\dim(E) = n$ et si $\phi : E \to E$ est définie par $\phi(Q) = Q^q$, $\phi$ est linéaire.

On note $S_P$ la matrice de $\phi$.

**Algorithme 1** (Berlekamp)**.** Soit $P \in \mathbb{F}_q[X]$ unitaire sans facteur carré.

1. On calcule $S_P - I_n$ et si $r := n - \mathrm{rg}(S_p - I) = 1$, on retourne $P$.
2. Sinon, calculer $V \in \ker(S_p - I_n)$ non constant modulo $P$ et pour tout $\alpha \in \mathbb{F}_q$, calculer $D_\alpha = P \wedge (V - \alpha)$. Appliquer l'algorithme à $D_\alpha$.

**Théorème 7.** L'algorithme de Berlekamp termine et retourne la décomposition de $P$ en facteurs irréductibles.

**Algorithme 2.** Soit $P \in \mathbb{F}_q[X]$.

1. Calculer $D = P \wedge P'$.
2. Si $D = P$, calculer $R$ tel que $P = R^p$ et appliquer l'algorithme à $R$. Si $D = 1$, appliquer Berlekamp à $P$. Sinon, appliquer Berlekamp à $P/D$ et retourner en 1 avec $D$.

**Théorème 8.** Cet algorithme termine et retourne la décomposition de $P$ en facteurs irréductibles.

**Théorème 9.** Soit $P \in \mathbb{Z}[X]$, soit $p$ premier. On note $\overline{P}$ le polynôme obtenu en réduisant modulo $p$ les coefficients de $P$. Alors, si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$ et $\deg(\overline{P}) = \deg(P)$, alors $P$ est irréductible dans $\mathbb{Q}[X]$.

***Exemple.*** *$P = 3X^2 + 17X - 11$ est irréductible dans $\mathbb{Q}[X]$.*

***Contre-exemple.*** *$X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_p[X]$ pour tout $p \in \mathbb{N}^*$ premier.*

### 3.2 Codes correcteurs d'erreurs

La transmission d'informations peut parfois être entachée d'erreurs. Les codes correcteurs permettent, dans une certaine mesure, de détecter voire de corriger ces erreurs.

**Définition 5.** Soit $E$ un ensemble, on appelle mot de longueur $k$ d'alphabet $E$ un $k$-uplet $(b_0, \cdots, b_{k-1}) \in E^k$.

***Exemple.*** *Dans un ordinateur, les informations sont envoyées par mots de 7 caractères à valeurs dans $\mathbb{F}_2$ (bits). On ajoute à chaque mot $(b_0, \cdots, b_6)$ un huitième bit, appelé bit de parité, donné par $b_7 = b_0 + \cdots + b_6$ (mod 2). Ce bit permet de détecter si un des bits a été mal transmis.*

On adoptera $\mathbb{F}_q$ comme alphabet.

**Définition 6.** On appelle code correcteur de longueur $n$ une sous-partie de $\mathbb{F}_q^n$. Si cette sous-partie est un sous-espace vectoriel de dimension $m$, on parlera de code linéaire de dimension $m$.

Le code correcteur contient l'ensemble des mots que l'on peut produire par codage. Ainsi, un mot reçu contient une erreur s'il n'est pas dans le code.

**Définition 7.** Soient $x, y$ deux mots de $\mathbb{F}_q^n$. On définit leur distance de Hamming, notée $d(x, y)$, comme le nombre de coefficients non nuls de $x - y$.

**Définition 8.** Un code est dit $t$-correcteur, pour $t \in \mathbb{N}$, si les boules de centre un mot du code et de rayon $t$ sont disjointes.

Ainsi, si un mot reçu se situe dans une des boules, on le corrige en le mot du centre de la boule.

**Proposition 8.** Soit $\mathcal{C}$ un code correcteur, on pose $\delta = \min\{d(x, y), x, y \in \mathcal{C}, x \neq y\}$. Si $\delta \geq 2t + 1$, alors $\mathcal{C}$ est $t$-correcteur.

***Exemple*** (Un code de Hamming)**.** *Soit* $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}^T$.
*On considère le code linéaire de taille 7, de dimension 4 sur $\mathbb{F}_2$ défini par $\mathcal{C} = \{Gx, x \in \mathbb{F}_2^4\}$. Ce code est 1-correcteur.*

## Développements

— Algorithme de Berlekamp.
— Loi de réciprocité quadratique.

## Références

[1] V. Beck, J. Malick, G. Peyré, Objectif Agrégation, H&K.
[2] I. Gozard, Théorie de Galois, Ellipses.
[3] D. Perrin, Cours d'algèbre, Ellipses.
[4] A. Szpirglas et al., Algèbre L3, Pearson.