

123 Corps finis. Applications.

Soient p un nombre premier, n un nombre entier, et $q = p^n$.

I – Construction

1. Caractéristique, sous-corps premier

DÉFINITION 1

Soit A un anneau. L'application

$$f_A : \begin{array}{ccc} \mathbb{Z} & \rightarrow & A \\ n & \mapsto & \underbrace{1 + \cdots + 1}_{n \text{ fois}} \end{array}$$

On note $\text{car}(A)$ l'unique $n \in \mathbb{N}$ tel que $\text{Ker}(f_A) = n\mathbb{Z}$: c'est la **caractéristique** de A .

[GOZ]
p. 7

EXEMPLE 2

La caractéristique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est n .

PROPOSITION 3

- (i) Soit A un anneau intègre. Alors, $\text{car}(A) = 0$ ou p avec p premier.
- (ii) Soit A un anneau fini. Alors, $\text{car}(A) \neq 0$ et $\text{car}(A) \mid |A|$.
- (iii) Un anneau et un quelconque de ses sous-anneaux ont la même caractéristique.

REMARQUE 4

- Le Point (i) est en particulier vrai pour un corps.
- Si $\text{car}(A) = 0$, A est infini.

DÉFINITION 5

Soit $\mathbb{K}$ un corps.

- $\mathbb{K}$ est dit **premier** s'il n'a pas d'autre sous-corps que lui-même.
- Le **sous-corps premier** de $\mathbb{K}$ est le sous-corps de $\mathbb{K}$ engendré par 1 (ie. l'intersection de tous les sous-corps de $\mathbb{K}$) : c'est un corps premier.

REMARQUE 6

Un corps et l'un de ses sous-corps ont le même sous-corps premier.

PROPOSITION 7

Soient $\mathbb{K}$ un corps et $\mathbb{P}$ son corps premier. Alors, si $\text{car}(\mathbb{K}) = 0$, $\mathbb{P} \cong \mathbb{Q}$.

2. Construction de $\mathbb{F}_p$

PROPOSITION 8

Les conditions suivantes sont équivalentes :

- (i) n est un nombre premier.
- (ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
- (iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

p. 3

NOTATION 9

On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

PROPOSITION 10

Soit $\mathbb{K}$ un corps fini.

- (i) $\text{car}(\mathbb{K})$ est un nombre premier p .
- (ii) Le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{F}_p$.
- (iii) $|\mathbb{K}| = p^m$ pour $m \geq 2$.

p. 81

EXEMPLE 11

- Il n'existe pas de corps fini à 6 éléments.
- $\mathbb{F}_p(X)$, est un corps infini de caractéristique p .

PROPOSITION 12

Tout corps fini à p éléments est isomorphe à $\mathbb{F}_p$.

p. 8

3. Construction de $\mathbb{F}_q$

PROPOSITION 13

Soit $\mathbb{K}$ un corps de caractéristique p . L'application

$$\text{Frob} : \begin{array}{ccc} \mathbb{K} & \rightarrow & \mathbb{K} \\ x & \mapsto & x^p \end{array}$$

est un morphisme de corps.

- (i) Si $\mathbb{K}$ est fini, c'est un automorphisme.
- (ii) Si $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

p. 85

COROLLAIRE 14

Dans un corps fini de caractéristique p , chaque élément admet exactement une racine p -ième.

APPLICATION 15

Petit théorème de Fermat.

$$\forall x \in \mathbb{Z}, x^p \equiv x \pmod{p}$$

THÉORÈME 16

- (i) Il existe un corps $\mathbb{K}$ à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
- (ii) $\mathbb{K}$ est unique à isomorphisme près : on le note $\mathbb{F}_q$.

COROLLAIRE 17

Le produit des éléments de $\mathbb{F}_q^*$ vaut -1 .

APPLICATION 18

Théorème de Wilson.

Soit $n \geq 2$ un entier. Alors,

$$n \text{ est premier} \iff (n-1)! + 1 \equiv 0 \pmod{n}$$

II – Propriétés

1. Commutativité

DÉFINITION 19

L'ensemble des générateurs de μ_n , noté μ_n^* , est formé des **racines primitives n -ièmes de l'unité**.

PROPOSITION 20

- (i) $\mu_n^* = \{e^{\frac{2ik\pi}{n}} \mid k \in \llbracket 0, n-1 \rrbracket, \text{pgcd}(k, n) = 1\}$.
- (ii) $|\mu_n^*| = \varphi(n)$, où φ désigne l'indicatrice d'Euler.

DÉFINITION 21

On appelle **n -ième polynôme cyclotomique** le polynôme

$$\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$$

THÉORÈME 22

- (i) $X^n - 1 = \prod_{d|n} \Phi_d$.
- (ii) $\Phi_n \in \mathbb{Z}[X]$.
- (iii) Φ_n est irréductible sur $\mathbb{Q}$.

p. 67

THÉORÈME 23

Théorème de Wedderburn.
Tout corps fini est commutatif.

[GOU21]
p. 100

2. Sous-corps

THÉORÈME 24

Tout sous-corps de $\mathbb{F}_q$ est de cardinal p^d avec $d \mid n$. Réciproquement, pour tout $d \mid n$, $\mathbb{F}_q$ admet un unique sous-corps de cardinal p^d .

[ULM18]
p. 122

EXEMPLE 25

Les sous-corps de $\mathbb{F}_{2^{12}}$ sont $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^2}$ et $\mathbb{F}_2$.

COROLLAIRE 26

Le polynôme $X^q - X \in \mathbb{F}_p[X]$ est produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ dont le degré divise n .

COROLLAIRE 27

Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_q[X]$.

COROLLAIRE 28

Un corps de rupture d'un polynôme irréductible de $\mathbb{F}_q[X]$ sur $\mathbb{F}_q$ est aussi un corps de décomposition pour ce polynôme sur $\mathbb{F}_q$.

3. Groupe multiplicatif

THÉORÈME 29

Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

[GOZ]
p. 83

COROLLAIRE 30

Le groupe multiplicatif d'un corps fini est cyclique.

COROLLAIRE 31

$$\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

4. Groupe des automorphismes

THÉORÈME 32

Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique, engendré par Frob, et d'ordre n .

PROPOSITION 33

Pour chaque application $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$, il existe un unique polynôme $P \in \mathbb{F}_q[X]$ de degré inférieur ou égal à $q - 1$ tel que $\forall x \in \mathbb{F}_q, P(x) = f(x)$. Il est donné par

$$P = \sum_{u \in \mathbb{F}_q} f(u)(1 - (X - u)^{q-1})$$

PROPOSITION 34

Les sous-groupes additifs de $\mathbb{F}_q$ sont les sous- $\mathbb{F}_p$ -espaces vectoriels. Ils sont au nombre de

$$\sum_{s=0}^n \frac{(p^n - 1)(p^{n-1} - 1) \dots (p^{n-s+1} - 1)}{(p^s - 1)(p^{s-1} - 1) \dots (p - 1)}$$

5. Carrés

PROPOSITION 35

On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Alors $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$.

p. 93

PROPOSITION 36

(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$, donc $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.

(ii) Si $p > 2$, alors :

- $\mathbb{F}_q^{*2}$ est le noyau de l'endomorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto x^{\frac{q-1}{2}}$.
- $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.
- $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
- $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 \pmod{4}$.

On suppose, pour la suite de cette sous-section, $p > 2$.

p. 155

DÉFINITION 37

On définit le **symbole de Legendre** $\left(\frac{x}{p}\right)$ pour $x \in \mathbb{F}_p^*$ par :

$$\left(\frac{x}{p}\right) = \pm 1 \text{ avec } \left(\frac{x}{p}\right) = 1 \iff x \in \mathbb{F}_p^{*2}$$

PROPOSITION 38

$x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupes non constant et,

$$\forall x \in \mathbb{F}_p^{\times 2}, \left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$$

THÉORÈME 39

Loi de réciprocité quadratique.

Soit $q \neq p$ un premier impair. Alors,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

REMARQUE 40

Cela signifie qu'il est équivalent d'avoir p résidu quadratique modulo q ou q résidu quadratique modulo p , sauf si $p \equiv q \equiv 3 \pmod{4}$ auquel cas ces propositions s'excluent mutuellement.

PROPOSITION 41

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)^2}{8}}$$

EXEMPLE 42

$$\left(\frac{17}{41}\right) = (-1)^{8 \times 20} \left(\frac{41}{17}\right) = \left(\frac{7}{17}\right) = (-1)^{3 \times 8} \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = (-1)^3 \left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

III – Applications

1. Irréductibilité de polynômes

THÉORÈME 43

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur un corps $\mathbb{K}$.

- Il existe un corps de rupture de P .
- Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P , alors il existe un unique $\mathbb{K}$ -isomorphisme $\varphi : \mathbb{L} \rightarrow \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.
- $\mathbb{K}[X]/(P)$ est un corps de rupture de P .

LEMME 44**Lemme de Gauss.**

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est égal à 1).

(ii) $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

p. 10

THÉORÈME 45**Critère d'Eisenstein.**

Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p premier tel que :

(i) $p \mid a_i, \forall i \in \llbracket 0, n-1 \rrbracket$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

APPLICATION 46

Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER]
p. 67**THÉORÈME 47****Critère d'irréductibilité modulo p .**

Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Soit p un premier. On suppose $p \nmid a_n$.

Si $\bar{P}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

[GOZ]
p. 12**EXEMPLE 48**

Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

2. Entiers sommes de deux carrés

NOTATION 49

On note

$$N: \begin{array}{ccc} \mathbb{Z}[i] & \rightarrow & \mathbb{N} \\ a+ib & \mapsto & a^2+b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P]
p. 137**REMARQUE 50**

$n \in \Sigma \iff \exists z \in \mathbb{Z}[i] \text{ tel que } N(z) = n.$

THÉORÈME 51**Deux carrés de Fermat.**

Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \pmod{4}$ (où $v_p(n)$ désigne la valuation p -adique de n).

3. En algèbre linéaire

LEMME 52

Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie. Les dilatations engendrent $\text{GL}(V)$.

[I-P]
p. 203

DEV

THÉORÈME 53

Théorème de Frobenius-Zolotarev.

Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \text{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p} \right)$$

où u est vu comme une permutation des éléments de V .

On se place pour la suite de cette sous-section dans le cadre d'un espace vectoriel E de dimension m sur le corps $\mathbb{F}_q$.

[ULM21]
p. 124

PROPOSITION 54

Les groupes précédents sont finis, et :

(i) $|\text{GL}(E)| = q^{\frac{m(m-1)}{2}} ((q^m - 1) \dots (q - 1)).$

(ii) $|\text{PGL}(E)| = |\text{SL}(E)| = \frac{|\text{GL}(E)|}{q-1}.$

(iii) $|\text{PSL}(E)| = \frac{|\text{SL}(E)|}{\text{pgcd}(m, q-1)} = \frac{|\text{GL}(E)|}{(q-1) \text{pgcd}(m, q-1)}.$

APPLICATION 55

Pour tout entier $p \in \llbracket 1, m \rrbracket$, il y a

$$\frac{\prod_{k=m-(p-1)}^n (q^k - 1)}{\prod_{k=1}^p (q^k - 1)}$$

sous-espaces vectoriels de dimension p dans E .

[ROM21]
p. 157

4. Codes correcteurs

DÉFINITION 56

On appelle :

- **Mot** un vecteur à coefficients dans $\mathbb{F}_q$.
- **Code correcteur** de taille m un sous-ensemble de $\mathbb{F}_q^m$.
- **Code linéaire** de taille m et de dimension r un sous-espace vectoriel de dimension r de $\mathbb{F}_q^m$.
- **Code cyclique** de taille m , un code linéaire stable par décalage circulaire.

[BMP]
p. 190

EXEMPLE 57

Soit un code linéaire $\mathcal{C}$ de taille m et de dimension r . On peut décrire $\mathcal{C}$ avec une matrice $G \in \mathcal{M}_{m \times r}(\mathbb{F}_q)$, dont les colonnes forment une base de $\mathcal{C}$, de la manière suivante :

$$\mathcal{C} = \{Gx \mid x \in \mathbb{F}_q^r\}$$

G est la **matrice génératrice** de $\mathcal{C}$. Le codage consiste alors à transformer un mot m du message d'origine en un mot $c \in \mathcal{C}$.

DÉFINITION 58

- Le **poids** d'un mot $x \in \mathbb{F}_q^m$, noté $\omega(x)$, est le nombre de coefficients non nuls de x .
- La **distance de Hamming** entre deux mots $x, y \in \mathbb{F}_q^m$ est définie par $d_H(x, y) = \omega(x - y)$.

Cette distance permet de mesurer la qualité d'un code comme l'atteste la remarque ci-dessous.

REMARQUE 59

d_H est une distance, elle quantifie la notion de "mot le plus proche".

DÉFINITION 60

Un code $\mathcal{C}$ est dit t -correcteur si les boules de centre un mot du code et de rayon t (pour d_H) sont disjointes : les mots de $\mathcal{C}$ sont à une distance d'au moins $2t + 1$ les uns des autres.

PROPOSITION 61

Soit $\mathcal{C}$ un code correcteur. On note d la **distance minimale** de $\mathcal{C}$:

$$d = \min_{\substack{x, y \in \mathcal{C} \\ x \neq y}} \{d_H(x, y)\}$$

Alors $\mathcal{C}$ est t -correcteur si et seulement si $d \geq 2t + 1$.

EXEMPLE 62

On considère le code $\mathcal{C}$ de taille 7 et de dimension 4 sur $\mathbb{F}_2$ dont la matrice génératrice est

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

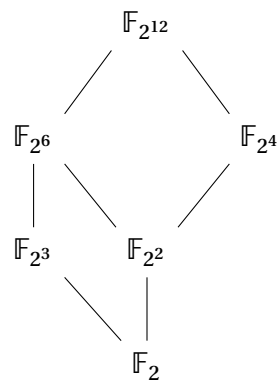
$\mathcal{C}$ est un code linéaire, dont chacun des mots non nuls est de poids supérieur à 3 : il est 1-correcteur.

PROPOSITION 63**Borne de Singleton.**

Soit $\mathcal{C}$ un code linéaire de longueur m , de dimension r et de distance minimale d . Alors,

$$d = \min_{x \in \mathcal{C} \setminus \{0\}} \{\omega(x)\} \leq m + 1 - r$$

Annexes



[ULM18]
p. 122

FIGURE 1 : Sous-corps de $\mathbb{F}_{2^{12}}$.

Bibliographie

Objectif agrégation

[BMP]

Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ. *Objectif agrégation*. 2^e éd. H&K, 22 août 2005.
<https://objectifagregation.github.io>.

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.
<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

Théorie de Galois

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2^e éd. Ellipses, 1^{er} avr. 2009.
<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

L'oral à l'agrégation de mathématiques

[I-P]

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2^e éd. Ellipses, 26 mars 2024.
<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

Cours d'algèbre

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

Mathématiques pour l'agrégation

[ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 20 avr. 2021.
<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

Anneaux, corps, résultants

[ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.
<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html>.

Felix ULMER. *Théorie des groupes. Cours et exercices*. 2^e éd. Ellipses, 3 août 2021.

<https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html>.