Leçon 123 : Corps finis. Applications.

Mémoire de M2 - Prépa Agreg

Jérémy BETTINGER

École Normale Supérieure de Rennes
& Université de Rennes 1

Encadré par Lionel Fourquaux

Année universitaire 2022-2023

Rapport du Jury (2021)

Une construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Les injections des divers $\mathbb{F}_q$ doivent être connues. Les 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. Le calcul des degrés des extensions et le théorème de la base téléscopique sont incontournables. La structure du groupe multiplicatif doit aussi être connue. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont envisageables. S'ils le désirent, les candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductibilité des polynômes à coefficients dans un corps fini.

Introduction

Un corps fini est un corps commutatif qui est de cardinal fini. Nous verrons qu'à isomorphisme près, un corps fini est entièrement déterminé par son cardinal, qui est toujours une puissance d'un nombre premier, ce nombre premier étant sa caractéristique. Cette propriété très intéressante permet de se ramener à des corps connus et plus simples.
Les corps finis sont utilisés dans de nombreux domaines des mathématiques : en théorie algébrique des nombres, en géométrie arithmétique ou encore avec le développement de l'informatique en théorie des codes et en cryptographie.
Dans ce mémoire nous étudierons les propriétés élémentaires des corps finis ainsi que quelques applications, d'une part à savoir si un nombre est un carré ou non, et d'autre part à des applications plus théoriques en algèbre linéaire et bilinéaire via le plus souvent des matrices.

Table des matières

Dans tout ce mémoire, la lettre p désignera un nombre premier, et q désignera une puissance de p : $q = p^n,\ n \in \mathbb{N}$.

1 Construction et propriétés élémentaires des corps finis

1.1 Propriétés élémentaires

Proposition 1.1. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Exemple 1.2. *$\mathbb{Z}/17\mathbb{Z}$ est un corps.*

Contre-Exemple 1.3. *$\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps.*

Définition 1.4. *Le morphisme d'anneaux $\varphi : n \in \mathbb{Z} \mapsto n.1_{\mathbb{K}} \in \mathbb{K}$, où on a noté $1_{\mathbb{K}}$ l'élément unité de $\mathbb{K}$, a pour noyau un idéal. On appelle caractéristique du corps $\mathbb{K}$ l'entier positif engendrant cet idéal.*

Exemple 1.5. *La caractéristique de $\mathbb{R}$ est 0, celle de $\mathbb{Z}/3\mathbb{Z}$ est 3.*

Définition 1.6. *Un corps est dit premier s'il ne contient aucun sous-corps strict. Si $\mathbb{K}$ est un corps, le sous-corps de $\mathbb{K}$ engendré par $1_{\mathbb{K}}$ est un corps premier. C'est le sous-corps premier de $\mathbb{K}$. C'est également l'intersection de tous les sous-corps de $\mathbb{K}$.*

Théorème 1.7. *Soit $\mathbb{F}$ un corps fini quelconque. Alors on a :*

1. *La caractéristique de $\mathbb{F}$ est un nombre premier p.*
2. *Le sous corps premier de $\mathbb{F}$ est $\mathbb{Z}/p\mathbb{Z}$*
3. *Il existe un entier naturel non nul n tel que $|\mathbb{F}| = p^n$. Il est noté $n = [\mathbb{F} : \mathbb{Z}/p\mathbb{Z}]$.*

On peut démontrer que ce corps est en fait unique, on le note alors $\mathbb{F}_q$ où $q = p^n$.

Remarque 1.8. *Ainsi on a une condition suffisante pour conclure à la non-existence de corps de certains cardinaux puisque ce cardinal doit être la puissance d'un nombre premier.*

Contre-Exemple 1.9. *Il n'existe pas de corps de cardinal 6.*

Remarque 1.10. *Il est fréquent, selon les conventions, de ne pas considérer dans la définition la commutativité du corps. Dans le cas des corps finis, la commutativité est une conséquence du théorème suivant.*

Théorème 1.11 (Wedderburn)**.** *Toute algèbre à division finie est commutative.*

1.2 Étude du groupe cyclique $\mathbb{F}_q^*$

De nombreux résultats découlent du fait suivant :

Proposition 1.12. *Pour tout $1 \leqslant k \leqslant p-1$, p divise $\binom{p}{k}$.*

Démonstration. Cela provient de la formule dite « du pion » :

$$\binom{p}{k} = \binom{p-1}{k-1}\frac{p}{k}.$$

En effet, cela donne

$$k\binom{p}{k} = p\binom{p-1}{k-1}.$$

Or puisque p est premier et $1 \leqslant k \leqslant p-1$, p est premier avec k donc p divise $\binom{p}{k}$. □

Nous allons utiliser ce fait afin de démontrer le petit théorème de Fermat.

Théorème 1.13 (Petit théorème de Fermat)**.** *On a pour tout entier relatif a premier avec p l'égalité : $a^p = a \mod(p)$.*

Démonstration. Nous allons utiliser un raisonnement par récurrence sur l'entier a, qu'on peut supposer positif.
Tout d'abord, la proposition $a^p = a \mod(p)$ est vraie pour $a = 1$.
De plus, montrons que tout entier k vérifie : $(k+1)^p = k^p + 1 \mod(p)$. Pour montrer cela il suffit de développer l'expression $(k+1)^p$ et d'utiliser la proposition précédente 1.12.
Ainsi si on suppose la proposition vraie pour un k, on obtient par hypothèse de récurrence les égalités : $a^p = (k+1)^p = k^p + 1 \mod(p) = k + 1 \mod(p) = a \mod(p)$ et achève la démonstration. □

Le fait énoncé en proposition 1.12 permet de montrer que le morphisme suivant, dit de Frobenius, est un morphisme de corps.

Proposition 1.14 (Frobenius)**.** *Le morphisme de Frobenius*

$$\begin{array}{rccc} \phi & : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & & x & \mapsto & x^p \end{array}$$

est un automorphisme de corps.

Démonstration. Tout d'abord, on a l'égalité $(x+y)^p = x^p + y^p$ dans $\mathbb{F}_q$. En effet, cela découle de la formule du binôme de Newton et de la proposition 1.12. On en déduit que le Frobenius est un endomorphisme de corps, donc est injectif. Le corps étant fini, l'endomorphisme est bijectif. □

Proposition 1.15. *Soit $P \in \mathbb{F}_p[X]$, $x \in \mathbb{F}_{p^n}$. Pour tout $s \in \mathbb{N}$ on a $P(x^{p^s}) = P(x)^{p^s}$.*

Remarque 1.16. *L'ensemble des points fixes par un automorphisme dans un corps est un sous-corps, et dans le cas de l'automorphisme de Frobenius, ce sous-corps est par définition l'ensemble des racines du polynôme $X^p - X$, de cardinal au plus p, donc c'est le sous-corps premier de $\mathbb{F}_p$.*

Remarque 1.17. *Les automorphismes d'un corps fini sont des itérés de l'automorphisme de Frobenius.*

Proposition 1.18. *$\mathbb{F}_q^*$ est cyclique.*

Démonstration. Le groupe $\mathbb{F}_q^*$ muni de la multiplication est un groupe abélien fini donc son ordre a est l'ordre d'au moins un élément x du groupe. Or le polynôme $X^a - 1$ est de degré a et possède $q-1$ racines distinctes dans $\mathbb{F}_q$ (petit théorème de Fermat), donc $a \geqslant q-1$. Ainsi le sous groupe de $\mathbb{F}_q^*$ engendré par x est égal au groupe $\mathbb{F}_q^*$. □

Remarque 1.19. *$\mathbb{F}_q^*$ est un groupe cyclique fini de cardinal $q-1$, il est donc isomorphe au groupe $\mathbb{Z}/(q-1)\mathbb{Z}$.*

1.3 Existence et unicité des corps finis

Proposition 1.20. *L'anneau $\mathbb{F}_p[X]/(P)$ est un corps si et seulement si P est un polynôme irréductible.*

Remarque 1.21. *La propriété précédente est vraie plus généralement en remplaçant $\mathbb{F}_p$ par n'importe quel corps $\mathbb{K}$ car l'anneau $\mathbb{K}[X]$ est principal.*

Corollaire 1.22. *Le cardinal de $\mathbb{F}_p[X]/(P)$ est $p^{deg(P)}$.*

Démonstration. La propriété d'unicité du reste de la division euclidienne se traduit par le fait que chaque élément de $\mathbb{F}_p[X]/(P)$ est représenté par un unique polynôme de degré inférieur où égal à $deg(P)-1$. Le cardinal de $\mathbb{F}_p[X]/(P)$ est donc $p^{deg(P)}$. □

Corollaire 1.23. *Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme irréductible de degré $n > 0$.*
Alors on a l'isomorphisme $\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_q$ où $q = p^n$.

Remarque 1.24. *Ainsi à isomorphisme près, le corps $\mathbb{F}_q$ est unique.*

Exemple 1.25 (Étude de $\mathbb{F}_4$)**.** *Le polynôme $1 + X + X^2$ est irréductible dans $\mathbb{F}_2[X]$ et est de degré 2. L'extension correspondante est « le » corps $\mathbb{F}_4$. Il a pour éléments : $0, 1,$ et a racine de $X^2 + X + 1 = 0$, ainsi que $a^2 = a + 1$. On peut donner ses tables de lois :*

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	0	a^2	a
a	a	a^2	0	1
a^2	a^2	a	1	0

$\times$	0	1	a	a^2
0	0	0	0	0
1	0	1	a	a^2
a	0	a	a^2	1
a^2	0	a^2	1	a

Nous allons prouver l'existence de polynômes irréductibles de tout degré sur $\mathbb{F}_q$. Pour cela, nous allons introduire quelques résultats issus de la théorie de Dirichlet.

Définition 1.26 (Fonctions arithmétiques et multiplicatives)**.** *Une fonction arithmétique est une fonction $f : \mathbb{N}^* \to \mathbb{C}$. Elle est dite multiplicative si pour tout $m, n \in \mathbb{N}^*$ avec $m \wedge n = 1$, on a $f(mn) = f(m)f(n)$.*

Définition 1.27 (Convolution de Dirichlet)**.** *Le signe $*$ désignera la convolution de Dirichlet, c'est à dire que pour deux fonctions arithmétiques f et g on a pour $n \in \mathbb{N}$:*

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{d_1, d_2 \\ d_1 d_2 = n}} f(d_1) g\left(d_2\right).$$

Notons que la loi $*$ est associative et commutative, d'élément neutre δ où $\delta(n) = 1$ si $n = 1$ et 0 sinon.

Définition 1.28. *On appelle fonction de Möbius la fonction arithmétique μ définie pour $n \in \mathbb{N}^*$ par :*

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers distincts} \\ 0 & \text{si } n \text{ possède un facteur premier carré} \end{cases}.$$

Proposition 1.29. *La fonction de μ est multiplicative et on a la relation :*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}.$$

Remarque 1.30. *Cela signifie que $\mu \star \mathbf{1} = \delta$.*

Énonçons maintenant la formule d'inversion de Möbius, elle servira notamment pour l'application 1.35.

Proposition 1.31 (Formule d'inversion de Möbius)**.** *Soit $f : \mathbb{N}^* \to \mathbb{C}$ une fonction.*
Soit également $g : \mathbb{N}^* \to \mathbb{C}$ définie pour $n \in \mathbb{N}^*$ par $g(n) = \sum_{d|n} f(d)$.
Alors pour tout $n \in \mathbb{N}^*$, on a

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Définition 1.32 (Corps de décomposition)**.** *On dit qu'une extension $\mathbb{K}$ d'un corps $\mathbb{F}$ est un corps de décomposition pour $P \in \mathbb{F}[X]$ si :*

1. $\exists\, a \in \mathbb{K}, (\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n :\ P(X) = a(X-\alpha_1)\ldots(X-\alpha_n) \in \mathbb{K}[X]$.
2. $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

Proposition 1.33. *On a la décomposition suivante :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in P_q(d)} P(X)$$

où on note $P_q(n)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$.

Démonstration. D'une part, si d divise n et $\mathbb{P} \in P_q(d)$, on pose $K = \mathbb{F}_q[X]/(P)$ qui est un corps de cardinal q^d, et donc, pour tout $x \in K,\ x^{q^d} = x$.
Or on a :

$$x^{q^n} = \underbrace{\left(\ldots (x^{q^d})^{q^d} \ldots\right)^{q^d}}_{n/d \text{ fois}}$$

et donc pour tout $x \in K,\ x^{q^n} = x$. Ainsi $X^{q^n} - X = 0$ dans $K = \mathbb{F}_q[X]/(P)$ c'est à dire P divise $X^{q^n} - X$. Le lemme de Gauss fournit alors :

$$\prod_{d|n} \prod_{P \in P_q(d)} P(X) \mid X^{q^n} - X.$$

Réciproquement, soit P un diviseur irréductible de $X^{q^n} - X$ unitaire de degré d. Puisque $\mathbb{F}_{q^n}$ est le corps de décomposition (rappelé en définition 1.32) de $X^{q^n} - X$ sur $\mathbb{F}_q$, P est scindé sur $\mathbb{F}_{q^n}$. Prenons alors $x \in F_{q^n}$ une racine de P. D'après le théorème de la base télescopique (rappelé ci-après au théorème 1.36) on a :

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)]\ d$$

puisque $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$ en vertu du fait que P est irréductible sur $\mathbb{F}_q$. On a donc montré que d divise n. Enfin, $X^{q^n} - X$ est à facteurs simples car $(X^{q^n} - X)' = -1$ dans $\mathbb{F}_{q^n}$ donc la multiplicité des facteurs irréductibles de $X^{q^n} - X$ est 1.
Ainsi,

$$X^{q^n} - X \mid \prod_{d|n} \prod_{P \in P_q(d)} P(X).$$

Comme on a la divisibilité dans les deux sens et que les polynômes sont unitaires, ils sont égaux, ce qui achève la démonstration. □

Remarque 1.34. *Il en découle le test de Rabin : $P \in \mathbb{F}_q[X]$ est irréductible sur $\mathbb{F}_q$ si et seulement si P divise $X^{q^n} - X$ et que $pgcd(P, X^{q^d} - X) = 1$ pour tout d diviseur strict de n.*

Application 1.35 (Développement 1 : Nombre de polynômes irréductibles sur $\mathbb{F}_q$)**.** *Soient $n \in \mathbb{N}^*$ et $q = p^r$ pour r entier et p premier. Si on désigne par $I(n,q)$ le nombre de polynômes irréductibles unitaires dans $\mathbb{F}_q$, alors :*

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{n\to+\infty}{\sim} \frac{q^n}{n}.$$

En outre, il existe des polynômes irréductibles unitaires de n'importe quel dégré dans $\mathbb{F}_q$.

Démonstration. En prenant les degrés dans l'expression de la proposition 1.33, on obtient :

$$q^n = \sum_{d|n} \sum_{P \in P_q(d)} deg(P) = \sum_{d|n} I(d,q)d.$$

Par inversion de Möbius 1.31 appliquée à $f(d) = dI(d,q)$, on obtient :

$$nI(n,q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

De plus on a l'estimation :

$$\left| \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) q^d \right| \leqslant \sum_{d|n,\, d<n/2} q^d \leqslant \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = q\frac{q^{\lfloor n/2 \rfloor} - 1}{q-1} \leqslant q^{\lfloor n/2 \rfloor + 1}.$$

De l'égalité

$$nI(n,q) = \mu(1)q^n + \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) q^d = q^n + \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) q^d$$

on obtient :

$$q^n - q^{\lfloor n/2 \rfloor + 1} \leqslant nI(n,q) \leqslant q^n + q^{\lfloor n/2 \rfloor + 1}. \tag{1}$$

Le membre de gauche est toujours strictement positif dès que $n \geqslant 3$.
Pour $n = 2$, on a $2I(2,q) = \mu(2)q + \mu(1)q^2 = q^2 - q = q(q-1) > 0$.
Pour $n = 1$, on a $I(1,q) = \mu(1)q = q > 0$. Donc pour tout $n \in \mathbb{N}^*$, $I(n,q) > 0$.
Enfin, puisque $q^{\lfloor n/2 \rfloor + 1} = o(q^n)$ on trouve d'après l'encadrement (1) l'égalité asymptotique $nI(n,q) = q^n + o(q^n)$, soit par définition

$$I(n,q) \underset{n\to+\infty}{\sim} \frac{q^n}{n}.$$

□

Ce résultat fournit une preuve de l'existence de polynômes de degré n quelconque sur $\mathbb{F}_q$.

1.4 Sous corps

Théorème 1.36 (Théorème de la base télescopique)**.** *Soient $\mathbb{L}$ une extension finie de $\mathbb{K}$ et $\mathbb{M}$ une extension finie de $\mathbb{L}$. On pose $(e_i)_{i\in I}$ une $\mathbb{K}$-base de $\mathbb{L}$ et $(f_j)_{j\in J}$ une $\mathbb{L}$-base de $\mathbb{M}$. Alors, $(e_i f_j)_{(i,j)\in I\times J}$ est une $\mathbb{K}$-base de $\mathbb{M}$. En particulier, $\mathbb{M}/\mathbb{K}$ est une extension finie et on a la formule dite de multiplicativité :*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Théorème 1.37. *Soit $\mathbb{F}_q$ un corps fini de caractéristique p de cardinal $q = p^n$. Alors pour tout diviseur d de n, il existe un unique sous-corps de $\mathbb{F}_q$ de cardinal p^d, i.e. isomorphe à $\mathbb{F}_{p^d}$.*

Exemple 1.38. *Les sous corps de $\mathbb{F}_{256} = \mathbb{F}_{2^8}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$ et $\mathbb{F}_{16}$.*

Théorème 1.39 (Théorème de l'élément primitif)**.** *Dans tout corps fini $\mathbb{F}_q$ de caractéristique p, il existe un élément $\alpha \in \mathbb{F}_q$ tel que $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. On appelle élément primitif sur $\mathbb{F}_p$ l'élément α.*

Exemple 1.40. *$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$, alors en notant a l'image de $X \in \mathbb{F}_2[X]$ dans le quotient $\mathbb{F}_4$, alors $\mathbb{F}_4 = \mathbb{F}_2(a)$.*

Donnons pour conclure cette partie un exemple de calculs dans les corps finis.

Exemple 1.41 (Calculs dans les corps finis)**.** *Le polynôme $P = X^2 + X - 1 \in \mathbb{F}_3[X]$ est irréductible car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_3$. On obtient alors un corps $\mathbb{L} = \mathbb{F}_3[X]/(P)$ de caractéristique 3. $\mathbb{L}$ est une extension de $\mathbb{F}_3$ et $[\mathbb{L} : \mathbb{F}_3] = 2$ donc $Card(\mathbb{L}) = 3^2 = 9$.*
Notons x la classe dans $\mathbb{L}$ du polynôme X.
Les éléments de $\mathbb{L}$ s'écrivent de manière unique sous la forme $a + bx$ avec $a, b \in \mathbb{F}_3$. On a donc :

$$\mathbb{L} = \{0, 1, -1, x, -x, 1 + x, 1 - x, -1 + x, -1 - x\}. \tag{2}$$

L'élément x vérifie la relation $x^2 + x - 1 = 0$, ce qui permet de calculer les puissances de x. Par exemple $x^4 = (x^2)^2 = (1 - x)^2 = 1 - 2x + x^2 = 1 - 2x + 1 - x = 2 = -1$ et $x^8 = 1$.
Puisque $x \neq 0$, $x \in \mathbb{L}^*$. Comme $\mathbb{L}$ est fini, le groupe $\mathbb{L}^*$ est cyclique. L'ordre de x dans $\mathbb{L}^*$ est un diviseur de $Card(\mathbb{L}^*) = 8$. Puisque x, x^2, x^4 sont différents de 1, alors x est d'ordre 8. Cela signifie que x est un générateur de $\mathbb{L}^*$.
Ainsi :

$$\mathbb{L} = \{0, 1, x, x^2, x^3, x^4, x^5, x^6, x^7\}. \tag{3}$$

En écrivant la relation $x^2 + x - 1 = 0$ sous la forme $x(x + 1) = 1$, on voit que $x^{-1} = x + 1$. Continuons à exprimer les puissances de x sous la forme $a + bx$: $x^3 = x \times x^2 = x(1 - x) = x - x^2 = 2x - 1 = -x - 1$; $x^5 = x^4 \times x = -x$; $x^6 = x^4 \times x^2 = -x^2 = x - 1$; $x^7 = x^{-1} = x + 1$.
Les deux présentations (2) et (3) sont utiles : (2) se prête plus aux calculs dans l'espace vectoriel $\mathbb{L}$ alors que (3) est plus adapté à $\mathbb{L}^*$.

Enfin, explicitions un isomorphisme entre deux corps de même cardinal.

Exemple 1.42. *Les polynômes X^3+X+1 et X^3+X^2+1 sont irréductibles dans $\mathbb{F}_2[X]$. Alors $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1) \simeq \mathbb{F}_2[X]/(X^3+X^2+1)$. Explicitons un isomorphisme entre ces deux derniers corps. Soit φ un isomorphisme de $\mathbb{F}_2[X]/(X^3+X^2+1)$ vers $\mathbb{F}_2[X]/(X^3+X+1)$. Ainsi, α est racine de X^3+X+1 où α est la classe de X dans $\mathbb{F}_2[X]/(X^3+X+1)$. Cherchons une racine de X^3+X+1 dans $\mathbb{F}_2[X]/(X^3+X^2+1)$. En notant β la classe de X dans $\mathbb{F}_2[X]/(X^3+X^2+1)$ on remarque que $\beta+1$ est racine. On prend alors $\varphi : P(\alpha) \in \mathbb{F}_2[X]/(X^3+X^2+1) \mapsto P(\beta+1) \in \mathbb{F}_2[X]/(X^3+X+1)$. Réciproquement, c'est bien un morphisme de corps.*

2 Carrés dans les corps finis

2.1 Premières caractérisations

Définition 2.1. *On note $\mathbb{F}_q^2 := \{x^2,\, x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{2*} := \{x^2,\, x \in \mathbb{F}_q^*\}$.*

Proposition 2.2. *On a l'alternative :*

1. *Si $q = 2^n$ alors $\mathbb{F}_q^2 = \mathbb{F}_q$.*
2. *Sinon, $|\mathbb{F}_q^{2*}| = (q-1)/2$ et $|\mathbb{F}_q^2| = (q+1)/2$.*

Proposition 2.3. *On a la caractérisation des carrés de $\mathbb{F}_q$: $x \in \mathbb{F}_q^2 \iff x^{(q-1)/2} = 1$.*

Corollaire 2.4. *Il existe une infinité de nombres premiers de la forme $4n+1$.*

Démonstration. Soit $a \in \mathbb{N}^*$ et a pair. Soit p premier divisant a^2+1.
Ainsi $a^2 = -1 \bmod(p)$ donc $a^4 = 1 \bmod(p)$. Cela montre également que p ne divise pas a. Ainsi, d'après le petit théorème de Fermat $a^{p-1} = 1 \bmod(p)$.

Comme a^2+1 est impair, tout premier p le divisant est de la forme $4n+3$ ou $4n+1$.
Si $p = 4n+3$, alors $p-1 = 4n+2$ d'où l'égalité $a^{p-1} = (a^4)^n.a^2 = -1 \bmod(p)$ et donc $1 = -1 \bmod(p)$ soit p divise 2. C'est impossible car p est impair, ainsi $p = 4n+1$.

Maintenant soit $N \in \mathbb{N}, N \geqslant 2$. On pose $a = N!$. D'après ce qui précède, p ne divise pas $a = N!$ donc $p > N$. Ainsi il existe des nombres premiers de la forme $4n+1$ aussi grands que l'on veut. □

2.2 Symbole de Legendre

Dans toute la suite, p désignera un nombre premier impair.

Définition 2.5. *Soit $x \in \mathbb{F}_p^*$. On définit le symbole de Legendre $\left(\frac{x}{p}\right)$ par :*

$$\left(\frac{x}{p}\right) = 1 \text{ si } x \in \mathbb{F}_p^{2*} \ ; \ -1 \text{ sinon.}$$

Exemple 2.6. *Puisque $2 = 3^2$ dans $\mathbb{F}_7$ alors $\left(\frac{2}{7}\right) = 1$.*

Proposition 2.7. *On a les propriétés suivantes sur le symbole de Legendre :*

1. *Pour tout $x \in \mathbb{F}_p^*$ on a $x^{(p-1)/2} = \left(\frac{x}{p}\right)$ dans $\mathbb{F}_p^*$.*
2. *Pour tout x, y tels que p ne divise ni x ni y on a la formule :*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

Lemme 2.8. *L'application*

$$\begin{array}{ccc} \mathbb{F}_p^* & \to & \{-1,1\} \\ x & \mapsto & \left(\frac{x}{p}\right) \end{array}$$

est l'unique morphisme de groupe non trivial de F_p^* sur $\{-1,1\}$.

Théorème 2.9 (Frobenius-Zolotarev)**.** *Soit $u \in GL_n(\mathbb{F}_p)$. On a l'égalité :*

$$\varepsilon(u) = \left(\frac{det(u)}{p}\right)$$

où ε désigne le morphisme signature.

Application 2.10. *La signature du Frobenius ϕ sur $GL_n(\mathbb{F}_p)$ est $\varepsilon(\phi) = (-1)^{(n+1)(p-1)/2}$.*

Lemme 2.11. *Pour tout nombre premier $p > 2$, 8 divise $p^2 - 1$.*

Énonçons quelques règles de calculs du symbole de Legendre.

Proposition 2.12. *On a les propriétés du symbole de Legendre suivantes :*

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

Lemme 2.13. *Si p est un nombre premier impair et $a \in \mathbb{F}_p^*$, alors :*

$$|\{x \in \mathbb{F}_p \,|\, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Démonstration. Cela découle du fait a est un carré modulo p si et seulement si a^{-1} est un carré modulo p. De plus, si a^{-1} est un carré alors le polynôme $X^2 - a^{-1}$ admet deux racines distinctes, cela démontre la formule annoncée. □

Théorème 2.14 (Développement 2 : Loi de réciprocité quadratique)**.** *Soient p, q deux nombres premiers impairs distincts. Alors on a :*

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

Démonstration. L'idée de la démonstration est de calculer de deux manières différentes le cardinal de l'ensemble suivant :

$$X = \left\{ (x_1, \ldots, x_p) \in \mathbb{F}_q^p \;\middle|\; \sum_{i=1}^{p} x_i^2 = 1 \right\}.$$

D'une part, on fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation des coordonnées : si $k \in \mathbb{Z}/p\mathbb{Z}$ et $(x_1, \ldots, x_p) \in X$:

$$k \cdot (x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{p+k})$$

où les indices sont pris modulo p. On étudie alors les orbites de cette action. Puisque $\mathbb{Z}/p\mathbb{Z}$ n'a que des sous groupes triviaux, les seuls stabilisateurs possibles d'un élément sont $\{1\}$ et $\mathbb{Z}/p\mathbb{Z}$. Les orbites dont le stabilisateur des éléments est $\mathbb{Z}/p\mathbb{Z}$ sont les singletons $\{(x, \ldots, x)\}$ avec $x \in \mathbb{F}_q$ tels que $px^2 = 1$.

Il y en a exactement $1 + \left(\frac{p}{q}\right)$ d'après le lemme précédent.

Par la relation orbite stabilisateur (rappelée ci-après au théorème 3.8), les orbites dont le stabilisateur des éléments est trivial sont de cardinal $|Orb| = |\mathbb{Z}/p\mathbb{Z}|/\{1\}| = p$.

Ainsi, par la formule des classes (rappelée ci-après au théorème 3.8), on a modulo p l'égalité :

$$|X| = 1 + \left(\frac{p}{q}\right) \bmod(p). \tag{4}$$

D'autre part, on va utiliser une forme quadratique équivalente sur $\mathbb{F}_q^p$ à $f(x) = \sum_i x_i^2$ dont la matrice dans la base canonique est I_p. On considère la matrice

$$A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & (0) & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & (0) & & 1 & 0 & \\ & & & & & a \end{pmatrix}$$

où on pose $a = (-1)^d$ avec $d = (p-1)/2$.
Les matrices A et I_p ont même rang p et même déterminant 1, donc même discriminant, elles définissent donc des formes quadratiques équivalentes.
Si P est la matrice de changement de base pour passer de l'une à l'autre, on a alors $X' = PX$ et donc $|X| = |X'|$ où on a posé

$$X' = \left\{ (y_1, \ldots, y_d, z_1, \ldots, z_d, t) \in \mathbb{F}_q^p \;\middle|\; 2(y_1 z_1 + \cdots + y_d z_d) + at^2 = 1 \right\}.$$

On distingue alors deux types d'éléments $(y_1, \ldots, y_d, z_1, \ldots, z_d, t)$ de X :

- Ceux dont tous les y_i sont nuls. Il reste le choix des éléments $(z_1, \ldots, z_d)$ qui donne q^d possibilités et celui de t sachant que t doit vérifier la relation $at^2 = 1$. D'après le lemme, il y a $1 + \left(\frac{a}{q}\right)$ possibilités pour t. D'où $q^d(1 + \left(\frac{a}{q}\right))$ possibilités pour les éléments de X' de cette forme.
- Ceux dont au moins un des y_i est non nul. On choisit donc un vecteur non nul de $\mathbb{F}_q^d$: il y a $q^d - 1$ possibilités puis on choisit t de manière quelconque dans $\mathbb{F}_q$: il y a q possibilités. Il reste ainsi à choisir $(z_1, \ldots, z_d)$ dans l'hyperplan affine d'équation $2(y_1 z_1 + \cdots + y_d z_d) + at^2 - 1 = 0$: il y a donc q^{d-1} possibilités. On obtient alors $(q^d - 1) \times q \times q^{d-1} = q^d(q^d - 1)$ possibilités pour les éléments de X' de cette forme.

Par conséquent, le nombre d'éléments dans X' est

$$q^d \left(1 + \left(\frac{a}{q}\right)\right) + q^d(q^d - 1) = q^d \left(q^d + \left(\frac{a}{q}\right)\right). \tag{5}$$

Or $|X'| = |X|$ on obtient alors d'après les égalités (4) et (5) :

$$q^d \left(q^d + \left(\frac{a}{q}\right)\right) = 1 + \left(\frac{p}{q}\right) \bmod(p).$$

De plus, d'après la propriété 2.7 on a : $\left(\frac{a}{q}\right) = a^{(q-1)/2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ et $\left(\frac{q}{p}\right) = q^{(p-1)/2} = q^d$.

Cela fournit ainsi :

$$\left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) = 1 + \left(\frac{p}{q}\right) \bmod(p)$$

et en multipliant par $\left(\frac{q}{p}\right)$ on obtient puisque $\left(\frac{q}{p}\right)^2 = 1$:

$$\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{q}{p}\right) + \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \bmod(p)$$

soit

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

Or comme tous les éléments mis en jeu sont égaux à 1 ou -1 l'égalité est également vraie dans $\mathbb{Z}$. On trouve le résultat en multipliant par $\left(\frac{p}{q}\right)$. □

Exemple 2.15. *Des propriétés précédentes et de la loi de réciprocité quadratique découlent les égalités :*

$$\left(\frac{5}{19}\right) = -\left(\frac{19}{5}\right) = -\left(\frac{-1}{5}\right) = -1$$

c'est à dire que 5 *n'est pas un carré modulo* 19.

3 Algèbre linéaire et bilinéaire

3.1 Algèbre linéaire

En dénombrant le nombre de vecteurs formant une base de $GL_n(\mathbb{F}_q)$ on obtient la proposition suivante.

Proposition 3.1. *On a*

$$|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}}(q-1)\dots(q^n-1).$$

et en appliquant le morphisme **det** : $GL_n(\mathbb{F}_q) \to \mathbb{F}_q^*$ on trouve

Lemme 3.2.

$$|SL_n(\mathbb{F}_q)| = |GL_n(\mathbb{F}_q)|/(q-1) = q^{\frac{n(n-1)}{2}}(q^2-1)\dots(q^n-1).$$

De plus, puisqu'on a les isomorphismes $PGL_n(\mathbb{F}_q) \simeq GL_n(\mathbb{F}_q)/\mathbb{F}_q^\times$ et $PSL_n(\mathbb{F}_q) \simeq SL_n(\mathbb{F}_q)/\mu_n(\mathbb{F}_q)$ où $\mu_n(\mathbb{F}_q)$ désigne l'ensemble des racines $n-$ièmes primitives de l'unité, on a les cardinaux suivants :

Lemme 3.3.
1. $|PGL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^2-1)\dots(q^n-1)$.
2. $|PSL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^2-1)\dots(q^n-1)/pgcd(n, q-1)$.

Proposition 3.4. *Tout groupe fini de cardinal n s'injecte dans $GL_n(\mathbb{F}_p)$.*

Proposition 3.5. *Le cardinal des matrices triangulaires supérieures (resp. strictes) sur le corps $\mathbb{F}_p$ est $p^{n(n+1)/2}$ (resp. $p^{n(n-1)/2}$).*

On peut se servir de ce résultat pour montrer le théorème de Sylow, en effet c'est un sous-groupe de Sylow si q est premier.

Application 3.6. *Tout groupe fini G d'ordre fini ayant p premier comme diviseur de son ordre admet un $p-$Sylow.*

Enfin, on peut ajouter une propriété qui illustre quelques isomorphismes remarquables.

Proposition 3.7. *On a les isomorphismes :*

1. $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.
2. $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ *et* $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$.
3. $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$.
4. $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ *et* $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

En algèbre linéaire, et en mathématiques plus généralement, on aime se ramener à des objets que l'on connaît bien. En particulier, on apprécie étudier les matrices diagonales puisqu'elles ont de nombreuses propriétés sympathiques : le produit est aisé, tout comme une éventuelle inversion. De plus, ces matrices sont régulièrement utilisées en analyse numérique.

On va ainsi apprécier les matrices diagonalisables puisqu'elles seront dans la même classe de conjugaison que leur matrice diagonale de valeurs propres associée. Nous allons alors essayer de dénombrer le nombre de matrices diagonalisables sur $\mathbb{F}_q$.

Tout d'abord, rappelons un résultat plutôt élémentaire mais fondamental.

Théorème 3.8. *(Équation aux classes) Pour l'action d'un groupe fini G sur un ensemble X, on a*

$$|X| = \sum_{x \in \mathcal{R}} |\mathcal{O}(x)| = \sum_{x \in \mathcal{R}} \frac{|G|}{|Stab(x)|}$$

où $\mathcal{R}$ désigne un système de représentants des orbites.

Application 3.9 (Développement 3 : Nombre de matrices diagonalisables dans $\mathbb{F}_q$)**.** *Notons $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de taille n à coefficients dans $\mathbb{F}_q$. Alors*

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1+\dots n_q=n \\ n_i \geqslant 0}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)| \dots |GL_{n_q}(\mathbb{F}_q)|}$$

et on a l'estimation asymptotique

$$\frac{|\mathcal{D}_n(\mathbb{F}_q)|}{|\mathcal{M}_n(\mathbb{F}_q)|} \underset{q \to +\infty}{\sim} \frac{1}{n!}.$$

Démonstration. Notons $\mathbb{F}_q = \{x_1, \dots, x_q\}$. On appellle q-partition de n la donnée d'un q-uplet $(n_1, \dots, n_q)$ d'entiers positifs tels que $n_1 + \cdots + n_q = n$.
Pour λ une q-partition, on pose $D_\lambda = Diag(\underbrace{x_1, \dots, x_1}_{n_1}, \dots, \underbrace{x_q, \dots, x_q}_{n_q})$.

$GL_n(\mathbb{F}_q)$ agit par conjugaison sur $\mathcal{D}_n(\mathbb{F}_q)$: $P \cdot M = PMP^{-1}$.
D'après l'équation aux classes, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{D \in \mathcal{R}} |\mathcal{O}(D)| = \sum_{D \in \mathcal{R}} \frac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}(D)|}$$

où $\mathcal{R}$ désigne un système de représentants des orbites.

$\mathcal{R} = \{D_\lambda;\ \lambda \text{ une } q - \text{partition de } n\}$ est un bon système de représentant des orbites car les x_i de multiplicités n_i caractérisent totalement les éléments de chaque orbite via le polynôme caractéristique.

On obtient alors :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1 + \dots n_q = n \\ n_i \geqslant 0}} \frac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}(D_\lambda)|}.$$

Or $P \in Stab(D_\lambda) \iff D_\lambda = PD_\lambda P^{-1} \iff D_\lambda P = PD_\lambda \iff P \in Com(D_\lambda) \cap GL_n(\mathbb{F}_q)$.
Si $P \in Com(D_\lambda)$, P commute avec D_λ donc chaque sous espace propre de D_λ est stable par P. Puisque D_λ est diagonale, P est diagonale par blocs de taille n_i : $P = Diag(P_{n_1}, \dots, P_{n_q})$.
De plus, comme $P \in GL_n(\mathbb{F}_q)$, on a : $P = Diag(P_{n_1}, \dots, P_{n_q})$ avec $P_{n_i} \in GL_n(\mathbb{F}_q)$.

Réciproquement, ces matrices sont dans le commutant de D_λ et sont inversibles.

Ainsi, choisir un élement du stabilisateur de D_λ c'est exactement choisir les élements diagonaux P_{n_i} de P : $|Stab(D_\lambda)| = |GL_{n_1}(\mathbb{F}_q)| \dots |GL_{n_q}(\mathbb{F}_q)|$.

On obtient donc la formule :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1 + \dots n_q = n \\ n_i \geqslant 0}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_\mathfrak{q})| \dots |GL_{n_q}(\mathbb{F}_q)|}.$$

Cherchons désormais un équivalent lorsque q tend vers l'infini.

Notons m le nombre de $n_i \neq 0$. Par construction, $1 \leqslant m \leqslant n$. Il y a m choix parmi les q nombres n_i pour avoir m n_i non nuls.
En enlevant les n_i nuls on peut peut écrire la q partition de n $(n_1, \dots, n_q)$ par $(n_{i_1}, \dots, n_{i_q})$ où $n_{i_j} > 0$.
Ainsi,

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{m=1}^{n} \binom{q}{m} \sum_{\substack{n_{i_1} + \dots n_{i_q} = n \\ n_{i_j} > 0}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_{i_1}}(\mathbb{F}_\mathfrak{q})| \dots |GL_{n_{i_q}}(\mathbb{F}_q)|}.$$

Il s'agit désormais de remarquer que $|\mathcal{D}_n(\mathbb{F}_q)|$ est un polynôme en q.

Déjà, il est clair que $|\mathcal{D}_n(\mathbb{F}_q)|$ est une fraction rationnelle en q qui s'écrit de la forme : $|\mathcal{D}_n(\mathbb{F}_q)| = A(q)/B(q)$ avec B unitaire et $A, B \in \mathbb{Z}[X]$ (c.f. l'expression de $GL_k(\mathbb{F}_q)$ en proposition 3.1).

On effectue la division euclidienne de A par rapport à B dans $\mathbb{Z}[X]$ pour écrire l'égalité : $A(q)/B(q) = Q(q) + R(q)/B(q)$ avec $\deg(R) < \deg(Q)$, $Q \in \mathbb{Z}[X]$. Le quotient $A(q)/B(q)$ étant un cardinal, il ne prend que des valeurs entières tout comme $Q(q)$. Ainsi $R(q)/B(q)$ est à valeurs entières. De plus, $R(q)/B(q)$ tend vers 0 lorsque q tend vers l'infini du fait de son degré. Donc à partir d'un certain rang il s'annule une infinité de fois, ce qui est possible uniquement si R/B est nul. Ce qui prouve que $|\mathcal{D}_n(\mathbb{F}_q)| = A(q)/B(q) = Q(q) \in \mathbb{Z}[q]$.

Ainsi, il suffit de trouver le terme de degré dominant pour trouver l'équivalent.

Or le degré en q de

$$\binom{q}{m} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_{i_1}}(\mathbb{F}_q)| \dots |GL_{n_{i_q}}(\mathbb{F}_q)|}$$

est (c.f. l'expression de $GL_k(\mathbb{F}_q)$ en proposition 3.1) $m+n^2-\sum_{j=1}^{m} n_{i_j}^2 \leqslant n+n^2-\sum_{j=1}^{m} n_{i_j} = n^2$.

Il y a égalité si et seulement si toutes les inégalités sont des égalités, à savoir lorsque $m = n$ et que tous les n_i valent 1.

On obtient donc l'équivalent :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \binom{q}{n} \frac{|GL_n(\mathbb{F}_q)|}{|GL_1(\mathbb{F}_q)|^n} \underset{q\to+\infty}{\sim} \frac{q^n}{n!} \times \frac{q^{n^2}}{(q-1)^n} \underset{q\to+\infty}{\sim} \frac{q^{n^2}}{n!}.$$

Autrement dit, la probabilité d'avoir une matrice diagonalisable de taille n sur $\mathbb{F}_q$ tend vers $1/n!$ lorsque q tend vers l'infini. □

On peut énoncer un critère pour montrer qu'une matrice est diagonalisable sur $\mathbb{F}_q$:

Proposition 3.10. *Une matrice $A \in \mathcal{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si elle vérifie la relation $A^q = A$.*

Démonstration. D'une part cela provient que pour tout $x \in \mathbb{F}_q$: $x^q = x$ et de d'autre part cela provient du fait que le polynôme $X^q - X$ est scindé à racines simples sur $\mathbb{F}_q$. □

3.2 Algèbre bilinéaire

Lemme 3.11. *L'équation $ax^2 + by^2 = c$ avec $a, b, c \in \mathbb{F}_q^*$ admet des solutions dans $\mathbb{F}_q$.*

Proposition 3.12. *Soit b une forme bilinéaire symétrique non dégénérée sur un espace vectoriel V de dimension supérieure ou égale à 2 à valeur dans $\mathbb{F}_q$ avec $p \neq 2$. Alors la forme quadratique associée q est surjective.*

Théorème 3.13. *Soit $\mathbb{F}_q$ de caractéristique différente de 2 et E un $\mathbb{F}_q$ espace vectoriel de dimension n. Soit $\alpha \in \mathbb{F}_q^*$ et $\alpha \notin \mathbb{F}_q^{2*}$. Il y a deux classes d'équivalence de formes quadratiques non dégénérées sur E, représentées par ces matrices :*

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \quad ou \quad \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \alpha \end{pmatrix}.$$

Une forme quadratique est de l'un ou de l'autre type suivant que son discriminant est un carré ou non dans $\mathbb{F}_q$.

Références

[Rom17] Jean-Etienne Rombaldi. *Mathématiques pour l'agrégation : algèbre et géométrie*. De Boeck, 2017.

[Lir11] François Liret. *Arithmétique*. Dunod, 2011.

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.

[CG13] Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométrie*. Tome premier. Calvage & Mounet, 2013.

[FG97] Serge Francinou et Hervé Gianella. *Exercices de mathématiques pour l'agrégation, Algèbre 1*. Masson, 1997.