Corps finis

Marc Abboud

Les références pour ce cours sont le cours d'algèbre de Daniel Perrin et le cours d'arithmétique de Jean Pierre Serre.

1 Construction des corps finis

Proposition 1.1. *Soit* $\mathbf{F}$ *un corps fini, alors la caractéristique de* F *est un nombre premier* $p > 0$*. Il existe alors un entier* $N > 0$ *tel que* $\mathbf{F}$ *est de cardinal* p^n*.*

Démonstration. Si $\mathbf{F}$ était de caractéristique nulle, son sous-corps premier serait $\mathbf{Q}$ et $\mathbf{F}$ serait alors infini. Soit p la caractéristique de p, le plongement $\mathbf{F}_p \hookrightarrow \mathbf{F}$ donne que $\mathbf{F}$ est un $\mathbf{F}_p$-espace vectoriel de dimension finie donc de cardinal p^N avec N la dimension de $\mathbf{F}$ sur $\mathbf{F}_p$. □

Proposition 1.2. *Soit* $\mathbf{F}$ *un corps de caractéristique* $p > 0$*, alors pour tout* $N > 0$*, l'application* $\sigma_n : x \in \mathbf{F} \mapsto x^{p^n}$ *est un morphisme de corps. De plus si* $\mathbf{F}$ *est fini, c'est un automorphisme.*

On appelle σ_1 *le* morphisme de Frobenius *et* σ_n *le morphisme de Frobenius d'ordre* n*.*

Démonstration. Il suffite de le montrer pour σ_1 car σ_n est simplement σ_1 composée n fois avec elle-même. L'application σ_1 est un morphisme de corps car pour tout $x, y \in \mathbf{F}, (x+y)^p = x^p + y^p$. Si $\mathbf{F}$ est un corps fini alors σ_1 est un automorphisme car σ_1 est injective. □

Lemme 1.3. *Soit* $\mathbf{F}$ *un corps et* $\sigma : \mathbf{F} \Rightarrow \mathbf{F}$ *un automorphisme de corps, alors l'ensemble* $\{x \in \mathbf{F} : \sigma(x) = x\}$ *est un sous-corps de* $\mathbf{F}$*.*

Théorème 1.4. *Soit* p *un nombre premier et* $N > 0$ *un entier. On pose* $q = p^N$*, il existe un corps* $\mathbf{F}$ *de cardinal* q*. Deux tels corps sont isomorphes car* $\mathbf{F}$ *s'obtient comme un corps de décomposition du polynôme* $X^q - X$ *sur* $\mathbf{F}_p$*. On note* $\mathbf{F}_q$ *le corps de cardinal* q*.*

Plus généralement, le corps $\mathbf{F}_{q^m}$ *s'obtient comme un corps de décomposition de* $X^{q^m} - X$ *sur* $\mathbf{F}_q$*.*

Démonstration. Soit $\mathbf{F}$ un corps de décomposition de $P = X^q - X$, $\mathbf{F}$ est nécessairement scindé à racines simples dans $\mathbf{F}$ car $P' = -1 \neq 0$. Donc $\mathbf{F}$ est au moins de cardinal q car P a exactement q racines dans $\mathbf{F}$. Maintenant, posons $\mathcal{L} = \{x \in \mathbf{F} : x^q = x\}$. Par ce que l'on vient de dire, L est de cardinal q et c'est un sous corps de $\mathbf{F}$ par la proposition 1.2 et le lemme 1.3. Maintenant comme $\mathbf{F}$ est engendré par les racines de P, on a en fait $\mathbf{F} = \mathcal{L}$ et tout a été prouvé. □

Exemple 1.5. Le corps $\mathbf{F}_4$ s'obtient comme un corps de rupture du polynôme $X^2 + X + 1$ car $X^4 - X = X(X-1)(X^2+X+1)$. On note α une racine de $X^2 + X + 1$ dans $\mathbf{F}_4$. Voici la table d'addition et de multiplication de $\mathbf{F}_4 = \{0, 1, \alpha, 1+\alpha\}$.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

;

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

.

Proposition 1.6. *Soit* $\mathbf{F}_{p^n}$ *et* $\mathbf{F}_{p^m}$ *deux corps finis, alors* $\mathbf{F}_{p^n}$ *est isomorphe à un sous-corps de* $\mathbf{F}_{p^m}$ *si et seulement si* n *divise* m*.*

Démonstration. Si on a un plongement $\mathbf{F}_{p^n} \to \mathbf{F}_{p^m}$, alors par la multiplicativité des degrés des extensions on a que n divise m.

Réciproquement, si n divise m on écrit $m = n\ell$. Soit $\mathbf{F}$ un corps de décomposition de $P = X^{p^n} - X$ sur $\mathbf{F}_{p^m}$, soit x une racine de P dans $\mathbf{F}$, alors on a $x^{p^n} = x$. Si on élève les deux cotés de cette équation à la puissance p^n ℓ fois, on a que $x^{p^{n\ell}} = x^{p^m} = x$, ce qui donne que x appartient à $\mathbf{F}_{p^m}$. On en déduit que $\mathbf{F}_{p^m}$ contient déjà toutes les racines de P donc $\mathbf{F}_{p^m}$ contient un sous corps isomorphe à $\mathbf{F}_{p^n}$. □

Corollaire 1.7. *Soient n, m deux entiers tels que n divise m et q une puissance d'un nombre premier. Il y a exactement n plongement $\mathbf{F}_{q^n} \hookrightarrow \mathbf{F}_{q^m}$.*

Exercice 1 :
S oit $\mathbf{F}$ un corps fini, montrer que $\mathbf{F}$ n'est pas algébriquement clos.

Corollaire 1.8. *Soit q une puissance d'un nombre premier. On choisit $\mathbf{F}_{q^{n!}}$ avec un plongement $\mathbf{F}_{q^{n!}} \hookrightarrow \mathbf{F}_{q^{(n+1)!}}$. Montrer que*

$$\mathbf{F} := \bigcup_{n \geq 1} \mathbf{F}_{q^{n!}}$$

est une clôture algébrique de $\mathbf{F}_q$.

2 Polynômes irréductibles sur les corps finis

Proposition 2.1 (Corollaire de la proposition 1.6)**.** *Soient q, m deux entiers avec $q = p^n$ pour un certain entier n. Soit Q un polynôme irréductible sur $\mathbf{F}_q$ de degré d divisant m, alors Q divise $X^{q^m} - X$.*

Démonstration. Soit $P := X^{q^m} - X$ et x une racine de Q dans une clôture algébrique de $\mathbf{F}_q$, on a que Q est le polynôme minimal de x sur $\mathbf{F}_q$ donc le degré de l'extension $\mathbf{F}_q(x)$ est égal à d. Par la proposition 1.6, on a que $\mathbf{F}_q(x)$ est isomorphe à un sous corps de $\mathbf{F}_{q^m}$. Donc par le théorème 1.4, on a $x^{q^m} - x = 0$. Ceci peut être fait pour toutes les racines de Q dans la clôture algébrique. On a donc que Q divise $X^{q^m} - X$ dans $\overline{\mathbf{F}_q}$. Si Q ne divise pas P dans $\mathbf{F}_q$, alors ils sont premiers entre eux car Q est irréductible sur $\mathbf{F}_q$. Mais par Bézout, il serait aussi premiers entre eux dans $\overline{\mathbf{F}_q}$, c'est absurde. □

Corollaire 2.2. *Soit $\mathrm{Irr}(q, d)$ l'ensemble des polynômes irréductibles unitaires sur $\mathbf{F}_q$ de degré d. on a*

$$X^{q^m} - X = \prod_{d|m} \prod_{Q \in \mathrm{Irr}(q,d)} Q$$

Démonstration. Soit $L = \prod_{d|m} \prod_{Q \in \mathrm{Irr}(q,d)} Q$ et $P = X^{q^m} - X$, on a déjà que L divise P par la proposition 2.1 et le lemme de Gauss. Maintenant écrivons $P = LR$ et supposons que $R \neq 1$. Soit R_1 un facteur irréductible de R de degré d. Par l'égalité $P = LR$ on a que $\mathbf{F}_{q^m}$ contient un corps de rupture de R_1. Donc on a que d divise m et donc $R_1 \in \mathrm{Irr}(q, d)$ c'est absurde car P possèderait alors un facteur carré mais $P' = 1$. □

Exercice 1 :
O n définit la fonction de Mobius $\mu : \mathbf{N}^* \to \{0, -1, 1\}$ par $\mu(1) = 1, \mu(n) = 0$ si n contient un facteur carré

et $\mu(p_1 \cdots p_r) = (-1)^r$ si les p_i sont des nombres premiers distincts.

1. Montrer que μ est multiplicative, i.e si $m \wedge n = 1$, alors $\mu(mn) = \mu(m) \cdot \mu(n)$.
2. Montrer que pour tout $n \in \mathbf{N}^*, n \neq 1, \sum_{d|n} \mu(d) = 0$.
3. Soit $f : \mathbf{N}^* \Rightarrow A$ où A est un groupe abélien. On pose $g(n) = \sum_{d|n} f(d)$. Montrer la formule d'inversion de Mobius : $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.
4. En déduire la formule $\sum_{d|n} \mu\left(\frac{n}{d}\right) d$.

Proposition 2.3. *Soit $I(q,d) := \operatorname{Card} \operatorname{Irr}(q,d)$, alors on a*

$$q^m = \sum_{d|m} dI(q,d).$$

et par la formule d'inversion de Mobius on a

$$I(q,d) = \frac{1}{d} \sum_{d'|d} \mu\left(\frac{d'}{d}\right) q^{d'}.$$

En particulier, pour tout $d \geq 1$, il existe un polynôme irréductible de degré d et on a l'équivalent

$$I(q,d) \sim_{d\to\infty} \frac{q^d}{d}.$$

Démonstration. On déduit la formule avec le corollaire 2.2. On obtient la formule de $I(q,d)$ avec la formule d'inversion de Môbius appliquée à la fonction $d \mapsto dI(q,d)$. □

Corollaire 2.4 (Théorème de l'élément primitif)**.** *Soit q une puissance d'un nombre premier et n un entier, le corps $\mathbf{F}_q^n$ s'obtient comme un corps de rupture d'un polynôme irréductible sur $\mathbf{F}_q$ de degré n. En particulier l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est monogène.*

3 Résultats sur les corps finis

3.1 Le groupe des inversibles

Proposition 3.1. *Le groupe des inversibles d'un corps fini est cyclique.*

Démonstration. Soit $\mathbf{F}$ un corps fini de cardinal q et $M = q-1$ le cardinal de $\mathbf{F}^\times$.

Soit d un entier divisant M et x un élément d'ordre d. On va montrer que tout élément d'ordre d s'obtient comme une puissance de x. Le groupe engendré par x est de taille d et tous les éléments dedans sont racines du polynôme $X^d - 1$. Comme ce polynôme a au plus d racines dans $\mathbf{F}$ on les a toutes. Donc si y est d'ordre d, on a que y est une puissance de x. Ainsi, $\mathbf{F}^\times$ contient au plus $\varphi(d)$ éléments d'ordre d.

Soit $N(d)$ le nombre d'éléments d'ordre d, on a $N(d) \leq \varphi(d)$ et $M = \sum_{d|M} N(d) \leq \sum_{d|M} \varphi(d) = M$. Donc il n'y a que des égalités et en particulier $N(M) = \varphi(M) \neq 0$ donc $\mathbf{F}^\times$ est cyclique. □

Corollaire 3.2 (Théorème de l'élément primitif)**.** *Soit q une puissance d'un nombre premier et n un entier. Le corps $\mathbf{F}_{q^n}$ s'obtient comme un corps de rupture d'un polynôme irréductible sur $\mathbf{F}_q$ de degré n. En particulier, il existe des polynômes irréductibles de tout degré sur $\mathbf{F}_q$. En particulier, l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est monogène.*

Corollaire 3.3. *Soit q une puissance d'un nombre premier, $\mathbf{F}_q$ admet une racine primitive n-ième de l'unité si et seulement si n divise $q-1$.*

Démonstration. Comme le groupe $\mathbf{F}_{q^n}^\times$ est cyclique, l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est monogène et finie. □

3.2 Les carrés dans $\mathbf{F}_q$

Proposition 3.4. *Soit $\mathbf{F}_q$ un corps fini, alors*

1. *Si q est pair, tout élément de $\mathbf{F}_q$ est un carré.*
2. *Sinon $\mathbf{F}_q^\times$ contient exactement $\frac{q-1}{2}$ carrés, soit Γ le sous-groupe des carrés dans $\mathbf{F}_q^\times$ et $a \in \mathbf{F}_q^\times \setminus \Gamma$, on a*

$$\mathbf{F}_q^\times = \Gamma \sqcup a \cdot \Gamma.$$

Démonstration. Si q est pair alors par la proposition 1.2, l'application $F : x \in \mathbf{F}_q \mapsto x^2$ est un morphisme de corps. Il est donc injectif et donc bijectif car $\mathbf{F}_q$ est fini.

Sinon, Soit $\varphi : x \in \mathbf{F}_q^\times \mapsto x^2 \in \mathbf{F}_q^\times$. C'est un morphisme de groupe son noyau est de cardinal 2 car les racines carrés de 1 sont 1 et -1 (on est en caractéristique impaire). Soit $\Gamma = \operatorname{Im}\varphi$, on a donc $\operatorname{Card}\Gamma = \frac{\operatorname{Card}\mathbf{F}_q^\times}{2} = \frac{q-1}{2}$. Maintenant soit $a \in \Gamma^c$, on a une application injective $x \in \Gamma \mapsto a \cdot x \in \Gamma^c$. Comme Γ et son complémentaire ont même cardinal, c'est une bijection. □

Corollaire 3.5. *Soient $a, b, c \in \mathbf{Z}$ tels que a, b, c ne sont pas des carrés dans $\mathbf{Z}$ mais le produit abc l'est, le polynôme*

$$(X^2 - a)(X^2 - b)(X^2 - c)$$

n'a pas de racines dans $\mathbf{Q}$ mais a des racines dans $\mathbf{F}_p$ pour tout p premier.

Démonstration. Soit P le polynôme $(X^2 - a)(X^2 - b)(X^2 - c)$. Comme P est unitaire à coefficients entiers, toutes ses racines rationnelles sont entières. Par les hypothèses sur a, b, c, P n'a pas de racines dans $\mathbf{Z}$.

Soit p un nombre premier. Si $p = 2$, alors P a des racines dans $\mathbf{F}_2$. Sinon, supposons que P n'a pas de racines dans $\mathbf{F}_p$ pour un certain p premier impair. Cela veut dire que a, b, c ne sont pas des carrés dans $\mathbf{F}_p$ et par la proposition précédente le produit abc non plus. Mais c'est absurde car abc est un carré dans $\mathbf{Z}$. □

Proposition 3.6. *Soit q une puissance d'un nombre premier impair, alors $x \in \mathbf{F}_q^\times$ est un carré si et seulement si $x^{\frac{q-1}{2}} = 1$.*

Démonstration. Si x est un carré dans $\mathbf{F}_q^\times$, alors $x = y^2$ avec $y \in \mathbf{F}_q^\times$ et alors

$$x^{\frac{q-1}{2}} = y^{q-1} = 1$$

par le théorème de Fermat. Maintenant, on sait qu'il y a exactement $\frac{q-1}{2}$ carrés dans $\mathbf{F}_q^\times$ et qu'ils sont tous racines du polynôme $Q = X^{\frac{q-1}{2}} - 1$ qui est aussi de degré $\frac{q-1}{2}$. On a donc trouvé toutes les racines de Q et l'équivalence est prouvée. □

Corollaire 3.7. *Soit q une puissance d'un nombre premier impair, -1 est un carré dans $\mathbf{F}_q$ si et seulement si q est congru à 1 modulo 4.*

Loi de réciprocité quadratique.– Soit p un nombre premier impair et $n \in \mathbf{F}_p$, on definit le symbole de Legendre

$$\left(\frac{n}{p}\right) = \begin{cases} 1 \text{ si } n \text{ est un carré dans } \mathbf{F}_p \\ 0 \text{ si } n = 0 \\ -1 \text{ sinon.} \end{cases}$$

On étend cette notation à $n \in \mathbf{Z}$ en prenant son image modulo p.

Proposition 3.8. *Soit x un entier et p un nombre premier impair, on a en fait*

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

On en déduit que

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

Démonstration. Cela résulte de la proposition 3.6. □

Proposition 3.9. *On a*

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

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

Démonstration. La première formule se déduit du corollaire 3.7. La deuxième est bien définie car les seuls carrés modulo 8 sont 0,1 et 4. Comme p est premier on a bien $p^2 \equiv 1 \mod 8$. Pour la montrer on choisit α une racine primitive 8-ième de l'unité dans une clôture algébrique de $\mathbf{F}_p$ (elle existe par le corollaire 3.3). On pose alors $y = \alpha + \alpha^{-1}$.

1. Montrer que $y^2 = 2$ en utilisant le fait que α^2 et α^{-2} sont les deux racines carrés de -1.
2. Si $p \equiv \pm 1 \mod 8$, montrer que $y^p = y$ et en déduire que $\left(\frac{2}{p}\right) = 1$.
3. Si $p \equiv \pm 5 \mod 8$, montrer que $y^p = -y$ en utilisant le fait que $\alpha^4 = -1$. En déduire que $\left(\frac{2}{p}\right) = -1$.

□

Théorème 3.10 (Loi de réciprocité quadratique)**.** *Soient ℓ, p des nombres premiers impairs, on a*

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

Le reste de cette partie est dédiée à la preuve de la loi de réciprocité quadratique.

Soit w une racine primitive ℓ-ième dans une cloture algébrique de $\mathbf{F}_p$, (elle existe par le corollaire 3.3). On pose

$$y = \sum_{t \in \mathbf{F}_\ell} \left(\frac{t}{p}\right) w^t$$

Exercice 1 :
M ontrer que cette somme est bien définie (expliquer le sens de w^t).

Lemme 3.11. *On a $y^2 = (-1)^{\frac{\ell-1}{2}}\ \ell$. Où on identifie ℓ et son image dans $\mathbf{F}_p$.*

Démonstration.

$$\begin{aligned} y^2 &= \sum_{t,u \in \mathbf{F}_\ell} \left(\frac{ut}{\ell}\right) w^{u+t} \\ &= \sum_{u \in \mathbf{F}_\ell} w^u \left(\sum_{t \in \mathbf{F}_\ell} \left(\frac{t(u-t)}{\ell}\right)\right) \end{aligned}$$

Or

$$\left(\frac{t(u-t)}{\ell}\right) = \left(\frac{-t^2}{\ell}\right)\left(\frac{1-t^{-1}u}{\ell}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{1-t^{-1}u}{\ell}\right).$$

D'où

$$(-1)^{\frac{\ell-1}{2}}\ y^2 = \sum_{u \in \mathbf{F}_\ell} C_u w^u$$

avec $C_u = \sum_{t \in \mathbf{F}_\ell} \left(\frac{1-t^{-1}u}{\ell}\right)$.

Exercice 2 :
M ontrer que

1. Si $u = 0, C_u = \ell - 1$.
2. Sinon $C_u = -1$.

□

Lemme 3.12. *On a $y^{p-1} = \left(\frac{p}{\ell}\right)$.*

Démonstration. On a $y^p = \left(\frac{p}{\ell}\right) y$. □

On en déduit maintenant la loi de réciprocité quadratique, en effet par les lemmes 3.11 et 3.12, on a

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

Et par la proposition 3.8 on a

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