Corps finis

1 Morphisme de Frobenius

Dans cette section, p est un nombre premier.

Proposition 1.1. *Soit A un anneau de caractéristique p. Alors pour tout $a, b \in A$ qui commutent, $(a+b)^p = a^p + b^p$.*

Démonstration. Il suffit de développer le binôme de Newton pour $(a+b)^p$ (puisque a et b commutent) et de montrer que $\binom{p}{k} = 0$ dans A, pour $1 \leq k \leq p-1$. Cette dernière égalité vient du fait que $k\binom{p}{k} = p\binom{p-1}{k-1}$ est divisible par p et d'une application du lemme de Gauss. □

Corollaire 1.2. *Soit A un anneau de caractéristique p et $n \in \mathbb{N}$. Alors pour tout $a, b \in A$ qui commutent, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.*

Définition 1.3. *Soit K un corps de caractéristique p. L'application $x \mapsto x^p$ est un endomorphisme d'anneau de K, appelé le* ***morphisme de Frobenius*** *de K.*

Remarque 1.4. Comme tout morphisme de corps, le Frobenius est injectif, mais il n'est pas surjectif en général. Attention à ne pas immédiatement l'appeler « l'automorphisme de Frobenius » en caractéristique p. C'est bien un automorphisme dans le cas d'un corps fini.

Corollaire 1.5. *Soit K un corps de caractéristique p dans lequel le Frobenius est surjectif et $P \in K[X]$. Alors $P' = 0$ si et seulement s'il existe $Q \in K[X]$ tel que $P = Q^p$.*

Démonstration. On a déjà vu que $P' = 0$ équivaut à ce que $P = \tilde{Q}(X^p)$ pour un certain $\tilde{Q} \in K[X]$. En écrivant $\tilde{Q} = \sum_{k=0}^{n} a_k X^k$ puis $a_k = b_k^p$ on a $P = \sum_{k=0}^{n} b_k^p X^{kp} = \left(\sum_{k=0}^{n} b_k X^k\right)^p$. La réciproque est claire puisque $(Q^p)' = pQ'Q^{p-1}$. □

2 Les corps finis $\mathbb{Z}/p\mathbb{Z}$

Lemme 2.1. *Soit $n \in \mathbb{N}, n \geq 2$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. Les propriétés suivantes sont équivalentes.*

1. *$\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.*
2. *$\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.*
3. *k est premier avec n.*

Démonstration. $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\overline{1} \in \langle \overline{k} \rangle$, si et seulement si $\overline{k}$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$. Ensuite, la congruence $ku \equiv 1 \bmod n$ équivaut à l'existence d'un $v \in \mathbb{Z}$ tel que $ku + nv = 1$, c'est-à-dire à une relation de Bézout entre k et n, et donc leur coprimalité. □

Corollaire 2.2. *Soit $n \in \mathbb{N}, n \geq 2$. Les propriétés suivantes sont équivalentes :*

1. *n est premier.*
2. *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*
3. *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.*

Démonstration. Si n est premier alors tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est la classe d'un entier non divisible par n, donc premier avec n. D'après le Lemme précédent, ces classes sont toutes inversibles, donc 1. $\Rightarrow$ 2. 2. $\Rightarrow$ 3. est clair. Si n n'est pas premier, on a $n = ab$ avec $1 < a, b < n$ et donc $\overline{a}, \overline{b} \neq \overline{0}$, mais $\overline{a}\overline{b} = \overline{0}$ et donc, par contraposée, 3. $\Rightarrow$ 1. □

Définition 2.3. *Soit p un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.*

Conséquences de la structure de corps de $\mathbb{Z}/p\mathbb{Z}$: Petit théorème de Fermat, critère d'irréductibilité par réduction dans $\mathbb{Z}[X]$ facile à vérifier (application à l'irréductibilité des polynômes cyclotomiques), structure particulière des carrés (critère d'Euler, loi de réciprocité quadratique), application aux équations diophantiennes (voir feuille suivante)...

3 Construction des corps finis

Proposition 3.1. *Soit K un corps fini. Il existe un nombre premier p et $n \in \mathbb{N}^*$ tels que $|K| = p^n$.*

Démonstration. K étant intègre, sa caractéristique est 0 ou un nombre premier. Mais si sa caractéristique était 0, K contiendrait un sous-anneau isomorphe à $\mathbb{Z}$, ce qui est impossible puisque K est fini. Soit donc p la caractéristique de K. Le sous-anneau de K engendré par 1 est alors isomorphe à $\mathbb{F}_p$. K étant fini, il est un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \geq 1$. Si $(e_1, \ldots, e_n)$ est une base de K, l'application

$$(x_1, \ldots, x_n) \mapsto \sum_{k=1}^{n} x_k e_k$$

est une bijection de $(\mathbb{F}_p)^n$ dans K et donc $|K| = p^n$. □

Nous allons maintenant montrer la réciproque de la proposition précédente.

Proposition 3.2. *Soit p un nombre premier et $n \in \mathbb{N}^*$. Si un corps fini K a pour cardinal p^n, alors K est un corps de décomposition de $X^{p^n} - X \in \mathbb{F}_p[X]$.*

Démonstration. Il est clair que 0 est racine de $X^{p^n} - X$. De plus, $K^\times$ est d'ordre $p^n - 1$ et donc, d'après le théorème de Lagrange, pour tout $x \in K^\times, x^{p^n-1} = 1$ et donc $x^{p^n} = x$. Ainsi, $X^{p^n} - X$ est scindé dans K et ses racines sont exactement les éléments de K. En particulier, $K = \mathbb{F}_p(K)$ et donc K est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. □

Théorème 3.3. *Soit p un nombre premier et $n \in \mathbb{N}^*$. Alors il existe un corps fini de cardinal p^n. De plus, celui-ci est unique à isomorphisme près.*

Démonstration. Considérons le corps de décomposition K de $X^{p^n} - X$ sur $\mathbb{F}_p$. Alors les p^n éléments de K qui sont les racines de $X^{p^n} - X$ forment un sous-corps F de K, ce que l'on voit en utilisant l'automorphisme de Frobenius. Comme K est engendré par F, on a donc $K = F$ et $|K| = p^n$. L'unicité vient de la Proposition 3.2 et du fait qu'un corps de décomposition est unique à isomorphisme près. □

Définition 3.4. *Soit q une puissance de nombre premier. On note $\mathbb{F}_q$ le corps fini à q éléments.*

Remarque 3.5. ⚠ Quand $q = p^n$ est une puissance d'un nombre premier, avec $n \geq 2$, le corps $\mathbb{F}_{p^n}$ n'a pas grand-chose à voir avec $\mathbb{Z}/p^n\mathbb{Z}$ ou $(\mathbb{F}_p)^n$! Ces derniers ne sont même pas intègres.

Exemple 3.6. Le polynôme $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$ car il est de degré 2 et sans racine, et donc on peut construire $\mathbb{F}_4$ comme étant $\mathbb{F}_2[X]/(X^2 + X + 1)$.

4 Propriétés des corps finis

Proposition 4.1. *Soit q une puissance de nombre premier. Alors $(\mathbb{F}_q^\times, \times)$ est un groupe cyclique.*

Démonstration. C'est un résultat vu en théorie des groupes : tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. $\square$

Proposition 4.2. *Soit q une puissance de nombre premier et K un corps contenant $\mathbb{F}_q$. Alors pour tout $x \in K$, $x \in \mathbb{F}_q$ si et seulement si $x^q = x$.*

Démonstration. Par construction des corps finis comme corps de décomposition. $\square$

Exercice 1. *Montrer que si $d \mid n$ alors $X^{q^d} - X \mid X^{q^n} - X$ dans $\mathbb{Z}[X]$.*

Proposition 4.3. *Soit q une puissance de nombre premier et $d, n \in \mathbb{N}$. Alors $\mathbb{F}_{q^n}$ est une extension de corps de $\mathbb{F}_{q^d}$ si et seulement si $d \mid n$.*

Démonstration. Si $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ est une extension de corps, alors la multiplicativité des degrés donne que $[\mathbb{F}_{q^d} : \mathbb{F}_q] \mid [\mathbb{F}_{q^n} : \mathbb{F}_q]$, c'est-à-dire $d \mid n$.

Réciproquement, si $d \mid n$, alors $X^{q^d} - X \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$ et donc $X^{q^d} - X$ est scindé dans $\mathbb{F}_{q^n}$, d'où $\mathbb{F}_{q^n}$ contient son corps de décomposition $\mathbb{F}_{q^d}$. $\square$

Exercice 2. *Montrer que le polynôme $X^4 + 1$ est réductible dans tous les $\mathbb{F}_p[X]$, bien qu'il soit irréductible dans $\mathbb{Z}[X]$. (Indication : On pourra montrer qu'il admet une racine dans $\mathbb{F}_{p^2}$.)*

Proposition 4.4. *Soit q une puissance de nombre premier et $P \in \mathbb{F}_q[X]$. Si P est irréductible alors P n'a pas de facteur carré dans $\overline{\mathbb{F}_q}[X]$.*

Démonstration. Si P a un facteur carré dans $\overline{\mathbb{F}_q}[X]$, on a $P = Q^2R$ avec $Q, R \in \overline{\mathbb{F}_q}[X]$. Alors Q divise P et $P' = 2Q'QR + Q^2R'$ dans $\overline{\mathbb{F}_q}[X]$. Ainsi, P et P' ne sont pas premiers entre eux dans $\overline{\mathbb{F}_q}[X]$, donc dans $\mathbb{F}_q[X]$ par invariance du PGCD par extension de corps. Puisque P est irréductible, le seul facteur commun possible à P et P' est alors P, ce qui implique que $P' = 0$ pour des raisons de degré. Mais alors d'après le Corollaire 1.5, $P = Q^p$ pour un certain $Q \in \mathbb{F}_q[X]$, ce qui est absurde par irréductibilité de P. $\square$

Remarque 4.5. La propriété de n'avoir pas de facteur carré dans la clôture algébrique est la **séparabilité**. Ainsi, tout polynôme irréductible est séparable dans $\mathbb{F}_q[X]$. On dit que $\mathbb{F}_q$ est un **corps parfait**. En général, un corps est parfait si et seulement s'il est de caractéristique 0 ou de caractéristique p avec Frobenius surjectif. C'est cette dernière propriété qu'on a utilisé ci-dessus.

5 Carrés dans $\mathbb{F}_q$

Dans cette section, on s'intéresse aux carrés dans les corps finis. Commençons par remarquer que tout élément de $\mathbb{F}_{2^n}$ est un carré, de manière unique, puisque la fonction carré est l'automorphisme de Frobenius.

Exercice 3. *Prouver directement que tout élément de $\mathbb{F}_{2^n}$ est un carré de manière unique.*

Dans la suite de cette section, on supposera donc q impair.

Proposition 5.1 (Critère d'Euler)**.** *Soit q une puissance de nombre premier impair et $x \in \mathbb{F}_q^\times$. Alors x est un carré dans $\mathbb{F}_q$ si et seulement si $x^{\frac{q-1}{2}} = 1$.*

Démonstration. L'application $f : x \mapsto x^2$ est un endomorphisme du groupe $\mathbb{F}_q^\times$. Son noyau est égal à $\{-1, 1\}$, car ces deux éléments sont de carré 1 et le polynôme $X^2 - 1$ ne peut avoir qu'au plus deux racines dans le corps $\mathbb{F}_q$. Ainsi, par le premier théorème d'isomorphisme et le théorème de Lagrange, l'image de f est d'ordre $\frac{q-1}{2}$. Maintenant, si x est un carré, $x = y^2$, alors $x^{\frac{q-1}{2}} = y^{q-1} = 1$ par le théorème de Lagrange et réciproquement, puisque le polynôme $X^{\frac{q-1}{2}} - 1$ ne peut avoir qu'au plus $\frac{q-1}{2}$ racines dans le corps $\mathbb{F}_q$, ses racines sont exactement les carrés de $\mathbb{F}_q^\times$. □

Au passage, on a montré le fait suivant.

Corollaire 5.2. *Soit q une puissance de nombre premier impair. Alors $\mathbb{F}_q$ possède $\frac{q+1}{2}$ carrés.*

Exercice 4. *Donner une autre démonstration de ce résultat en utilisant le fait que $\mathbb{F}_q^\times$ est cyclique.*

Proposition 5.3. *Soit q une puissance de nombre premier. Alors -1 est un carré dans $\mathbb{F}_q$ si et seulement si q est pair ou $q \equiv 1 \bmod 4$. En particulier, -1 est toujours un carré dans $\mathbb{F}_{q^2}$.*

Démonstration. Si q est pair, il est clair que $-1 = 1^2$. Sinon, on calcule

$$(-1)^{\frac{q-1}{2}} = \begin{cases} 1 \text{ si } q \equiv 1 \bmod 4 \\ -1 \text{ si } q \equiv 3 \bmod 4. \end{cases}$$

□

6 Exercices

Exercice 5. *Soit p un nombre premier et $n \geq 2$. Montrer que $(\mathbb{F}_{p^n}, +) \simeq ((\mathbb{F}_p)^n, +) \not\simeq (\mathbb{Z}/p^n\mathbb{Z}, +)$.*

Exercice 6. *Donner un isomorphisme entre $\mathbb{F}_3[X]/(X^2+1)$ et $\mathbb{F}_3[X]/(X^2+X-1)$.*

Exercice 7. *Chercher les polynômes irréductibles de degré $2, 3, 4, 5$ dans $\mathbb{F}_2[X]$.*

Exercice 8. *Écrire les tables d'addition et de multiplication de $\mathbb{F}_4$. Donner un générateur de $\mathbb{F}_4^\times$.*

Exercice 9. *Donner deux constructions de $\mathbb{F}_{16}$, comme extension de degré 4 de $\mathbb{F}_2$ et comme extension de degré 2 de $\mathbb{F}_4$, et un isomorphisme entre les deux.*

Exercice 10. *Donner un générateur de $\mathbb{F}_{11}^\times$.*

Exercice 11. *Soit $x \in \mathbb{F}_q$. Montrer que x est un carré dans $\mathbb{F}_{q^2}$.*

Exercice 12. *Montrer qu'un corps fini ne peut être algébriquement clos.*

Exercice 13. *Soit q une puissance de nombre premier. Montrer que*

$$\bigcup_{n\in\mathbb{N}} \mathbb{F}_{q^{n!}}$$

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

Exercice 14. *Soit q une puissance de nombre premier et $P \in \mathbb{F}_q[X]$ irréductible de degré n. Montrer que si $\alpha \in \mathbb{F}_{q^n}[x]$ est une racine de P dans $\mathbb{F}_{q^n}$, alors α^q également. En déduire que P est scindé dans $\mathbb{F}_{q^n}$.*

Exercice 15. *Soit q une puissance de nombre premier. Montrer que toute extension finie de $\mathbb{F}_q$ est un corps de rupture sur $\mathbb{F}_q$ et est donc monogène. (On peut procéder par maximalité du degré d'un élément de l'extension ou par cyclicité du groupe multiplicatif d'un corps fini.)*

Exercice 16. *D'après l'exercice précédent, pour toute puissance de nombre premier q et tout $n \in \mathbb{N}^*$, il existe un élément primitif $\theta \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$. En particulier, $\mathbb{F}_q$ admet des polynômes irréductibles de tout degré. On va maintenant les dénombrer.*

1. *Soit $n \in \mathbb{N}^*$. On note $I_q(n) = \{P \in \mathbb{F}_q[X] \mid P \text{ irréductible, unitaire}, \deg P = n\}$ et $\pi_q(n) = \#I_q(n)$. Montrer que pour tout diviseur d de n et tout $P \in I_q(d)$, $P \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$.*
2. *Réciproquement, montrer qu'un facteur irréductible unitaire de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ est dans $I_q(d)$ avec d un diviseur de n.*
3. *En déduire que $q^n = \sum_{d\mid n} \pi_q(d)$.*
4. *En admettant la **formule d'inversion de Möbius**[1] donner une formule pour $\pi_q(n)$ en fonction de q et de n.*
5. *Montrer que $\pi_q(n) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$ et que $\pi_q(n) \underset{q\to+\infty}{\sim} \frac{q^n}{n}$*
6. *Si l'on choisit uniformément un polynôme unitaire dans $\mathbb{F}_q[X]$ de degré n, avec n ou q grand, estimer la probabilité que le polynôme choisi soit irréductible.*

Exercice 17. *Soit q une puissance de nombre premier et $n \in \mathbb{N}^*$. Montrons que $A \in \mathcal{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^q = A$.*

Exercice 18. *Soit q une puissance de nombre premier impair. Montrer que tout élément de $\mathbb{F}_q$ est somme de deux carrés. En déduire qu'il n'existe que deux classes d'équivalence de formes quadratiques non dégénérée sur $\mathbb{F}_q^n$.*

1. Si pour tout $n \in \mathbb{N}^*$, $b_n = \sum_{d\mid n} a_d$ alors pour tout $n \in \mathbb{N}^*, a_n = \sum_{d\mid n} \mu(n/d) b_d$ où

$$\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n = p_1 \dots p_r \text{ avec les } p_i \text{ premiers deux à deux distincts} \\ 0 \text{ si } n \text{ a un facteur carré.} \end{cases}$$

Exercice 19 (Théorème de Chevalley-Warning)**.** *Soit q une puissance de nombre premier.*

1. *Soit $d \in \mathbb{N}$. Montrer que*
$$\sum_{x \in \mathbb{F}_q} x^d = \begin{cases} -1 \text{ si } m \geq 1 \text{ et } q-1 \mid d \\ 0 \text{ sinon.} \end{cases}$$
2. *Soit $P_1, \ldots, P_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ vérifiant $\sum_{i=1}^{r} \deg P_i < n$ et posons $P = \prod_{i=1}^{r}(1 - P_i^{q-1})$. Montrer que la fonction polynomiale associée à P est l'indicatrice de l'ensemble des racines communes des P_i.*
3. *Calculer $\sum_{\underline{x} \in \mathbb{F}_q^n} P(\underline{x})$ de deux manières différentes.*
4. *En déduire que le nombre de racines communes des P_i est divisible par la caractéristique p de $\mathbb{F}_q$.*
5. *Montrer que si $P_1, \ldots, P_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ sont homogènes et vérifient $\sum_{i=1}^{r} \deg P_i < n$, alors ils ont un zéro commun non nul dans $\mathbb{F}_q^n$.*

Remarque. Le dernier énoncé signifie géométriquement que les hypersurfaces projectives d'équations $P_i = 0$ dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$ ont une intersection non vide.

Exercice 20 (Théorème de Wedderburn)**.** *Soit K une algèbre à division finie. On va montrer que K est un corps, c'est-à-dire que K est commutative.*

1. *Soit $Z = \{x \in K \mid \forall y \in K, xy = yx\}$. Montrer que Z est un corps fini. En déduire qu'il existe une puissance de nombre premier q et un entier $n \in \mathbb{N}^*$ tels que $|Z| = q$ et $|K| = q^n$.*
2. *Faisons agir $K^\times$ sur lui-même par conjugaison. Pour tout $x \in K^\times$, montrer que* $\mathrm{Stab}(x) \cup \{0\}$ *est un sous-corps de K contenant Z.*
3. *En déduire que, pour tout $x \in K^\times$, il existe d divisant n tel que $|\mathrm{Stab}(x)| = q^d - 1$.*
4. *En utilisant l'équation aux classes, montrer que $\Phi_n(q) \mid q - 1$, où*
$$\Phi_n = \prod_{\zeta \text{ racine primitive } n-\text{ième de l'unité}} (X - \zeta).$$
(On pourra admettre que $\Phi_n(q)$ est bien un entier.)
5. *Établir une absurdité en supposant que $n > 1$.*

Remarque. Wedderburn était écossais, le *W* se prononce à l'anglaise !

Exercice 21. *Soit K un corps de caractéristique p. Déterminer les racines p-ièmes de l'unité dans K.*

Exercice 22. *Soit p un nombre premier, K un corps de caractéristique p et $a \in K$. Montrer que le polynôme $X^p - X + a$ est soit scindé dans $K[X]$, soit irréductible dans $K[X]$. (Indication : On pourra montrer que si une extension de K possède une racine de ce polynôme, alors elle les possède toutes.)*

Exercice 23. *Soit p un nombre premier et $K = \mathbb{F}_p(T)$. Montrer que le polynôme $X^p - T \in K[X]$ est irréductible mais pas séparable (i.e. il a un facteur multiple dans $\overline{K}$).*