Corps finis

1. Définitions et notations

On suppose connues les définitions des mots ou expressions *corps*, *morphisme de corps*, *extension de corps*.

1.1. **Corps de rupture.** Si k est un corps, $k[X]$ l'anneau des polynômes à coefficients dans k, et $P(X)$ un polynôme *irréductible* de degré d dans $k[X]$, alors le quotient $K := k[X]/(P(X))$ par l'idéal engendré par $P(X)$ est un corps contenant un sous-corps isomorphe à k (les classes des constantes). On l'appelle le corps de rupture de $P(X)$. En effet, si on désigne par α la classe de X dans le quotient K, on a $P(\alpha) = 0$ dans K : α est une racine de P dans K. Le corps K est un k-espace vectoriel : 1, α, α^2,..., α^{d-1} forment une base de K comme k-espace vectoriel (savoir faire la démonstration qui repose sur la *division euclidienne* des polynômes).

1.2. **Caractéristique, morphisme de Frobenius.** Si k est un corps, on construit le morphisme d'anneaux

$$\begin{array}{rcl} \varphi : \mathbf{Z} & \longrightarrow & k \\ n & \longmapsto & n.1 \end{array}$$

dont le noyau est un idéal de $\mathbf{Z}$. S'il est réduit à $\{0\}$, on dit que k est de caractéristique zéro. Sinon - et c'est toujours le cas si k est fini -, c'est un idéal premier, puisque k n'a pas de diviseurs de zéro. Soit p le générateur positif de l'idéal. On appelle p la *caractéristique* de k.
Si $p > 0$ le morphisme ϕ induit un morphisme de corps injectif de $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ dans k. Tout corps de caractéristique p est une extension de $\mathbf{F}_p$. En particulier, tout corps fini de caractéristique p est un espace vectoriel de dimension finie sur $\mathbf{F}_p$. Son nombre d'éléments est donc une puissance de p.
Dans $\mathbf{Z}$, le coefficient du binôme $\binom{p}{k}$ est divisible par p pour $0 < k < p$. Si a et b sont deux éléments d'un corps K de caractéristique p, on a donc

$$(a+b)^p = a^p + b^p.$$

On a, bien sûr, $(ab)^p = a^p b^p$.

Proposition 1.3. *Soit K un corps fini de caractéristique p. L'application*

$$\begin{array}{rcl} F : K & \longrightarrow & K \\ x & \longmapsto & x^p \end{array}$$

est un automorphisme de K appelé automorphisme de Frobenius. Les éléments fixés par F sont les éléments du corps premier.

Démonstration. F est un morphisme de corps, dont le noyau est réduit à $\{0\}$, donc injectif. Puisque K est fini, il est aussi surjectif. On remarque de plus que le polynôme $X^p - X$ a au plus p racines dans K. Or on en connait p qui sont les éléments du corps premier $\mathbf{F}_p$. On les connait donc toutes. □

Corollaire 1.4. *Soit P un polynôme à coefficients dans $\mathbf{F}_p[X]$. On a $(P(X))^p = P(X^p)$ et l'application*

$$\begin{array}{rcl} \mathbf{F}_p[X] & \longrightarrow & \mathbf{F}_p[X] \\ P(X) & \longmapsto & (P(X))^p \end{array}$$

est $\mathbf{F}_p$-linéaire.

Attention : il faut ici que le corps soit $\mathbf{F}_p$. Que se passe-t-il si on prend un corps fini de caractéristique p différent de $\mathbf{F}_p$?

Théorème 1.5. *Soit p un nombre premier et n un entier positif. Soit K un corps fini de caractéristique p et de cardinal p^n.*

1. *K est un espace vectoriel de dimension n sur $\mathbf{F}_p$.*
2. *Le groupe multiplicatif K^* est cyclique d'ordre $p^n - 1$. Le polynôme $X^{p^n} - X$ est scindé dans $K[X]$ et a pour racines les p^n éléments de K.*

Exercice 1. On suppose $p = 2$. Quels sont les éléments de K qui sont des carrés ?
On suppose maintenant que p est impair. Vérifier que les carrés non nuls de K sont les racines du polynôme $X^{\frac{p^n-1}{2}} - 1$.

Théorème 1.6 (de l'élément primitif)**.** *Soit p un nombre premier et n un entier positif. Soit K un corps fini de caractéristique p et de cardinal p^n. Il existe un élément α dans K tel que $K = \mathbf{F}_p[\alpha]$. Il existe un polynôme irréductible $P(X)$ de $\mathbf{F}_p[X]$ tel que l'application*

$$\begin{array}{rcl} \phi : \mathbf{F}_p[X]/(P(X)) & \longrightarrow & K \\ \dot{X} & \longmapsto & \alpha \end{array}$$

soit un isomorphisme de corps.
De plus, le polynôme $P(X)$ est scindé dans K, l'ensemble de ses racines est $\{\alpha, \alpha^p, \ldots, \alpha^{p^{(n-1)}}\}$ et il divise $X^{p^n} - X$ dans $\mathbf{F}_p[X]$.

Démonstration. Prenons pour α un générateur du groupe multiplicatif K^*. On voit que $K = \mathbf{F}_p[\alpha]$. Soit ℓ le plus grand entier tel que le système $1, \alpha, \ldots, \alpha^{\ell-1}$ est libre sur $\mathbf{F}_p$. On a donc une relation de dépendance linéaire sur $\mathbf{F}_p$

$$\alpha^\ell + a_{\ell-1}\alpha^{\ell-1} + \ldots + a_0 = 0.$$

On en déduit que toutes les puissances de α sont dans $\mathrm{Vect}(1, \alpha, \ldots, \alpha^{\ell-1})$, donc que $K = \mathrm{Vect}(1, \alpha, \ldots, \alpha^{\ell-1})$ et que $\ell = n$. Posons $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$. Ce polynôme de $\mathbf{F}_p[X]$ a α pour racine dans K. Il est irréductible dans $\mathbf{F}_p[X]$: sinon α serait racine d'un de ses facteurs et le système $1, \alpha, \ldots, \alpha^{n-1}$ ne serait pas libre.
Vérifier que l'application ϕ est bien un isomorphisme.
L'ensemble des racines de P dans K est stable par l'automorphisme de Frobenius, à cause de la relation $P(X^p) = (P(X))^p$. L'ensemble des racines de $P(X)$ est donc composé de α, α^p,..., $\alpha^{p^{(n-1)}}$, tous différents et tous générateurs de K^*, puisque l'ordre de α est $p^n - 1$. Il s'ensuit que $P(X)$ est scindé dans $K[X]$ et qu'il divise donc $X^{p^n} - X$ dans $\mathbf{F}_p[X]$. □

On vient de montrer que tout corps fini à p^n éléments est (à isomorphisme près) le quotient de $\mathbf{F}_p[X]$ par l'idéal engendré par un polynôme irréductible de degré n. D'où les questions :

(1) Y a-t-il des polynômes irréductibles de degré n dans $\mathbf{F}_p[X]$? La réponse est oui (voir exercice 2, feuille 2).

(2) P et Q étant deux polynômes de degré n irréductibles dans $\mathbf{F}_p[X]$, les quotients $\mathbf{F}_p[X]/(P(X))$ et $\mathbf{F}_p[X]/(Q(X))$ sont-ils isomorphes ?

Théorème 1.7. *Soit p un nombre premier et n un entier positif. Soit K un corps fini de caractéristique p et de cardinal p^n. Les automorphismes de K sont les puissances de l'automorphisme de Frobenius. Ils forment un groupe cyclique d'ordre n. Soit r un entier naturel. L'ensemble des éléments fixés par F^r est un sous-corps de K.*

Démonstration. On a déjà vu que F est un automorphisme et $F^n = \mathrm{Id}_K$. Les éléments fixés par F^r sont les solutions de l'équation $x^{p^r} = x$ qui forment un sous-corps de K.
Un automorphisme σ de K induit un automorphisme du groupe K^*. Il est entièrement déterminé par l'image d'un générateur α. D'après le théorème de l'élément primitif, K est égal à $\mathbf{F}_p[\alpha]$, et le polynôme minimal de α est irréductible de degré d dans $\mathbf{F}_p[X]$. Soit σ un automorphisme de K. Comme $P(\alpha) = 0$, $\sigma(\alpha)$ est aussi racine de P. En effet,

$$0 = \sigma(P(\alpha)) = P(\sigma(\alpha)).$$

On en déduit que les seules possibilités pour $\sigma(\alpha)$ sont les images de α par une puissance du Frobenius. □

Exercice 2. Calculer, suivant les valeurs de r, le nombre d'éléments du sous-corps fixé par F^r.

Lemme 1.8. *Soit p un nombre premier et n un entier positif. Un polynôme $P(X)$ irréductible de degré d dans $\mathbf{F}_p[X]$ divise $X^{p^n} - X$ si et seulement si d divise n.*

Démonstration. On remarque d'abord que $p^d - 1$ divise $p^n - 1$ si et seulement si d divise n (division euclidienne).
Soit P irréductible de degré d. On vient de voir (1.6) que P divise $X^{p^d} - X$ dans $\mathbf{F}_p[X]$. Lorsque d divise n, $p^d - 1$ divise $p^n - 1$ et $X^{p^d-1} - 1$ divise $X^{p^n-1} - 1$. Donc P divise $X^{p^n} - X$.
Supposons maintenant que $P(X)$, irréductible de degré d dans $\mathbf{F}_p[X]$, divise $X^{p^n} - X$. Dans le quotient $K := \mathbf{F}_p[X]/(P(X))$ notons α un générateur du groupe multiplicatif K^*. L'ordre de α dans K^* est $p^d - 1$. Considérons l'ensemble des éléments x de K tels que $x^{p^n} = x$. C'est un sous-anneau de K. Comme $P(X)$ divise $X^{p^n} - X$ ce sous-anneau contient α. Il est donc égal à K. Tous les éléments de $K^\times$ sont solutions de l'équation $x^{p^n-1} = 1$. Parmi eux il en est d'ordre $p^d - 1$ et par suite $p^d - 1$, divise $p^n - 1$. On en déduit que d divise n. □

Théorème 1.9. *Soit p un nombre premier et n un entier positif. Il existe un corps à p^n éléments, unique à isomorphisme près. On le note $\mathbf{F}_{p^n}$.*

Remarquons que, comme $\mathbf{F}_{p^n}$ a un groupe d'automorphismes non réduit à l'identité si $n > 1$, il y a en général plus d'un isomorphisme entre deux corps à p^n éléments : on peut toujours composer par un automorphisme de l'un des deux corps.

Démonstration. Il reste simplement à donner une réponse positive à la question (2) ci-dessus.
Soit $P(X)$ un polynôme de degré n, irréductible dans $\mathbf{F}_p[X]$. Désignons par K le quotient $\mathbf{F}_p[X]/(P(X))$.
Si $Q(X)$ est un autre polynôme irréductible de degré n, le lemme 1.8 montre qu'il divise $X^{p^n} - X$. L'ensemble de ses racines est stable par l'action du Frobenius.
Soit β l'une d'entre elles. Comme son ordre dans K^* divise $p^n - 1$, les éléments de l'ensemble $\beta, \beta^p, \ldots, \beta^{p^{(n-1)}}$ sont tous distincts : ce sont les racines de Q dans K.
Considérons alors l'application de $\mathbf{F}_p[X]/(Q(X))$ dans K qui envoie la classe de X sur β et la classe d'un polynôme $R(X)$ modulo $Q(X)$ sur $R(\beta)$. Vérifier qu'elle est bien définie, injective et que c'est un isomorphisme de corps. □

Exercice 3. Soit p un nombre premier et n un entier positif. On appelle *polynôme primitif* un polynôme irréductible de degré n dans $\mathbf{F}_p[X]$ dont une racine au moins est un générateur du groupe multiplicatif $\mathbf{F}^*_{p^n}$.
Montrer que toutes ses racines sont des générateurs de $\mathbf{F}^*_{p^n}$.
Montrer que tout générateur de $\mathbf{F}^*_{p^n}$ est racine d'un unique polynôme de $\mathbf{F}_p[X]$ irréductible, de degré n. En déduire le nombre de polynômes primitifs de degré n dans $\mathbf{F}_p[X]$ en fonction de p et de n. Exemple : $p = 2$, $n = 4$.