Introduction à l'étude des Corps Finis

Robert Rolland

(Résumé)

1 Introduction

La structure de corps fini intervient dans divers domaines des mathématiques, en particulier dans la théorie de Galois sur la résolution des équations algébriques où ils sont introduits pour la première fois. Pour cette raison, en hommage au mathématicien français Evariste Galois (1811-1832), ces corps sont appelés les **corps de Galois**.

Avec le dévelopement de l'électronique, de l'informatique, de la transmission de l'information, de nouveaux champs d'applications de l'algèbre ont vu le jour. Ces domaines font un grand usage de la structure de corps fini.

Pour traiter et transmettre de l'information il est nécessaire de la numériser afin que l' **alphabet** utilisé ait une structure suffisamment riche permettant des opérations intéressantes. Compte tenu de la contrainte technologique binaire des circuits électroniques on pourrait penser que le corps à deux éléments $\mathbb{F}_2$ est suffisant. Mais ceci n'est pas vrai pour plusieurs raisons. D'une part, tout en restant en binaire, on peut parfois regrouper les bits pour en faire des nombres plus élaborés ; par exemple si on regroupe les bits huit par huit on travaille alors avec des objets qui peuvent être considérés comme des nombres du corps $\mathbb{F}_{256}$. On dispose alors d'opérations plus riches que celles qu'on aurait eues sur $\mathbb{F}_2$. D'autre part la structure même de l'information à transmettre où le type de traitement qu'on est amené à lui faire subir peuvent imposer une étape de calcul dans un corps fini adapté, quitte à éventuellement tout retranscrire en binaire à la fin.

Nous donnons ici une première introduction sur les corps finis pouvant servir de base à une étude des codes correcteurs d'erreurs, des codes compresseurs, de la cryptographie.

2 Premiers exemples

2.1 Les corps premiers

Parmis les anneaux $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ des classes résiduelles d'entiers modulo n nous savons caractériser les corps grâce au résultat bien connu suivant

Théorème 2.1 *L'anneau $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

2.2 Le corps $\mathbb{F}_8$

Soit $P(X) = X^3 + X + 1$. Ce polynôme est irréductible sur le corps à deux éléments $\mathbb{F}_2$ (en effet si ce polynôme se factorisait, étant de degré 3 il aurait en facteur un polynôme de degré 1, ce qui est impossible puique $P(1) = P(0) = 1$). Le quotient de l'anneau $\mathbb{Z}_2[X]$ des polynômes à coefficients dans $\mathbb{Z}_2$ par l'idéal engendré par P est un corps que nous noterons $\mathbb{F}_8$.

Ce corps peut être considéré comme constitué par les polynômes de degré inférieur ou égal à 2, à coefficients dans $\mathbb{Z}_2$. La multiplication se fait en réduisant la multiplication ordinaire modulo P. Chaque polynôme de ce type ayant trois coefficients valant soit 0 soit 1, on conclut qu'il y a 8 éléments dans $\mathbb{F}_8$. Nous venons de voir aussi qu'une première façon de représenter les éléments de ce corps est de donner les trois composantes de l'élément dans la base $1, X, X^2$.

Notons α la classe résiduelle du polynôme X modulo P. Ainsi il est clair que dans le corps $\mathbb{F}_8$ on a $P(\alpha) = 0$.

Calculons aussi les puissances de α dans la base $1, X, X^2$.

$$\begin{array}{rcccc} \alpha^0 & = & 1 & 0 & 0 \\ \alpha^1 & = & 0 & 1 & 0 \\ \alpha^2 & = & 0 & 0 & 1 \\ \alpha^3 & = & 1 & 1 & 0 \\ \alpha^4 & = & 0 & 1 & 1 \\ \alpha^5 & = & 1 & 1 & 1 \\ \alpha^6 & = & 1 & 0 & 1 \\ \alpha^7 & = & 1 & 0 & 0 \end{array}$$

Ainsi $\alpha^7 = \alpha_0 = 1$ et les puissances de α décrivent tous les éléments non nuls du corps. Autrement dit le groupe multiplicatif des éléments non nuls

du corps est cyclique et α en est un générateur. Les éléments non nuls de $\mathbb{F}_8$ peuvent donc être représentés par leur **logarithme à base** α.

Il est clair que dans la première représentation (sous forme polynômiale) il est facile de faire des additions, tandis que dans la deuxième (sous forme logarithmique) il est facile de faire des multiplications.

2.3 Construction à partir des anneaux de polynômes

Soit P un polynôme de degré n à coefficients dans le corps $\mathbb{Z}_p$ ireductible sur ce corps. On sait alors que l'idéal engendré par P est maximal. Donc le quotient $\mathbb{Z}_p[X]/(P)$ est un corps. Nous verrons par la suite que tous les corps finis peuvent être construits de cette façon.

3 Description des corps finis

Le premier résultat est le théorème de Wedderburn

Théorème 3.1 *Tout corps fini est commutatif.*

Théorème 3.2 *Soit F un corps fini. Il existe un plus petit entier p tel que la somme constituée de p termes égaux à 1 soit nulle. De plus p est un nombre premier et $\mathbb{Z}_p$ est un sous corps de F.*

Preuve : F étant fini, les nombres 1, $1+1$, $1+1+1$, etc.. ne peuvent être tous distincts. Deux de ces nombres sont donc égaux, et par simplification il existe une somme constituée de 1 qui est nulle. Nous noterons p le plus petit entier > 0 tel que la sommes de p termes égaux à 1 soit nulle.
Il est facile de voir que les éléments de F qui sont des sommes de 1 forment un sous anneau de F isomorphe à $\mathbb{Z}_p$. Ce sous anneau est intègre puisque F est un corps, ce qui prouve que p est premier et donc que cet anneau isomorphe à $\mathbb{Z}_p$ est un sous corps de F.

Définition 3.1 *Le nombre p intervenant dans le théorème précédent est appelé la caractéristique du corps F.*

Remarque En fait si on appelle ψ l'homomorphisme d'anneau de $\mathbb{Z}$ dans F qui à l'entier 1 fait correspondre l'unité également notée 1 de F, on voit que le noyau de ψ est $p\mathbb{Z}$ et donc que $\mathbb{Z}/p\mathbb{Z}$ est isomorphe au sous corps de F engendré par 1.

Théorème 3.3 *Soit F un corps fini de caractéristique p. Le nombre d'éléments de F est de la forme*

$$\sharp F = p^n.$$

Preuve : F contient le corps à p éléments $\mathbb{Z}_p$. C'est donc un espace vectoriel sur $\mathbb{Z}_p$. Sa dimension est nécessairement finie puisque F est fini. Si on note n la dimension de F sur $\mathbb{Z}_p$, on voit que $\sharp F = p^n$.

Remarque La démonstration du théorème précédent nous montre que F ne peut contenir un autre corps $\mathbb{Z}_r$ où r est un nombre premier distinct de p.

Nous allons maintenant regarder plus en détail la structure multiplicative d'un corps fini F ayant p^n éléments. Notons F^* l'ensemble des éléments non nuls de F.

Théorème 3.4 *Pour tout élément a de F^* il existe un plus petit entier e tel que a^e=1. De plus e divise $p^n - 1$.*

Preuve : F^* étant fini, les puissances de a ne peuvent être toutes distinctes. Donc deux de ces puissances sont égales et par simplification il existe une puissance de a qui vaut 1. Soit e le plus petit entier tel que $a^e = 1$. Les nombres $1, a, \ldots, a^{e-1}$ forment un sous groupe multiplicatif à e éléments du groupe F^* à $p^n - 1$ éléments. Donc e divise $p^n - 1$.

Définition 3.2 *Le nombre e du théorème précédent est appelé l'ordre de a.*

Soit a un élément d'ordre e dans F^*. a est donc solution de l'équation $X^e - 1 = 0$. Il est facile de voir qu'il en est de même de toutes les puissances de a. Par suite on a la factorisation suivante

$$X^e - 1 = (X - 1)(X - a)(X - a^2) \ldots (X - a^{e-1})$$

qui prouve qu'il n'y a pas d'autre élément que des puissances de a qui soit d'ordre e. Parmis les puissances de a, il peut y en avoir qui ont un ordre strictement inférieur à e. On peut voir que a^i (avec $1 < i < e$) est d'ordre $< e$ si et seulement si i n'est pas premier avec e ; en fait on a le résultat suivant

Théorème 3.5 *Si e est l'ordre de a, alors pour tout entier $1 \leq i \leq e$ l'ordre de a^i est égal à $ppcm(i, e)/i$.*

Preuve : Remarquons tout d'abord que $a^u = 1$ si et seulement si u est multiple de e (faire la division euclidienne de u par e). Donc k est l'ordre de a^i si et seulement si ki est le plus petit commun multiple de i et de e ce qui prouve le théorème.

En conclusion pour chaque e qui divise $p^n - 1$, si on suppose que e est l'ordre d'un élément, il y a exactement $\phi(e)$ éléments qui ont pour ordre e (Où ϕ est la fonction indicatice d'Euler). Mais on sait qu'il y a en tout $p^n - 1$ éléments dans F^* et que $\sum_{e|p^n-1} \phi(e) = p^n - 1$, donc tout e qui divise $p^n - 1$ est l'ordre d'un élément. En particulier il existe un élément d'ordre $p^n - 1$; cet élément engendre donc le groupe F^*.
On obtient donc le théorème

Théorème 3.6 *Le groupe multiplicatif F^* est cyclique.*

Définition 3.3 *Un générateur du groupe multiplicatif F^* est appelé un élément primitif.*

Corollaire 3.1 *Tout élément β du corps F vérifie*

$$\beta^q = \beta$$

Preuve : Si $\beta = 0$ le résultat est clair. Si $\beta \in F^*$ alors on sait que $q - 1$ est un multiple de l'ordre de β, si bien que $\beta^{q-1} = 1$.

Ce résultat implique que le polynôme $X^q - X$ se décompose entièrement dans F et que ses q racines dans F sont exactement les q éléments de F. En particulier toutes les racines de ce polynôme sont distinctes. En appliquant ce résultat au sous coprs premier on obtient

Corollaire 3.2 *Les éléments du corps F tels que*

$$x^p = x$$

sont exactement les éléments de $\mathbb{Z}_p$.

Une autre façon d'exprimer que le groupe multiplicatif d'un corps fini est cyclique est de dire que :

Corollaire 3.3 *Dans tout corps fini il existe un élément primitif.*

Théorème 3.7 *Dans tout corps fini ayant $q = p^n$ éléments (p premier)*

$$(x + y)^p = x^p + y^p.$$

Preuve : Il suffit d'appliquer la formule du binôme en remarquant que dans le corps $p = 0$.

Comme conséquences de ce résultat nous avons

Corollaire 3.4 *Dans tout corps fini ayant $q = p^n$ éléments*

$$(x + y)^{p^t} = x^{p^t} + y^{p^t}$$

Corollaire 3.5 *Si P est un polynôme à coefficients dans $\mathbb{Z}_p$ et si F un corps fini à $q = p^n$ éléments alors pour tout x de ce corps*

$$\Big(P(x)\Big)^{p^t} = P(x^{p^t})$$

Corollaire 3.6 *Avec les notations du corollaire précédent, si u est une racine du polynôme P (à coefficients dans $\mathbb{Z}_p$) alors les nombres*

$$u^p, u^{p^2}, \ldots, u^{p^{n-1}}$$

sont aussi des racines de P.

Un élément non nul β étant donné dans le corps fini F à $q = p^n$ éléments, nous savons que β est racine du polynôme $X^q - X$ à coefficients dans $\mathbb{Z}_p$. La question est de savoir si β peut être racine d'un polynôme à coefficients dans $\mathbb{Z}_p$ de degré plus petit.

Définition 3.4 *On appelle polynôme minimal de β sur $\mathbb{Z}_p$, le polynôme normalisé (i.e. dont le coefficient du terme de plus haut degré est 1) à coefficients dans $\mathbb{Z}_p$, de plus petit degré ayant β comme racine.*

Remarquons que ceci a un sens car il est facile de voir grâce à la remarque précédente qu'un tel polynôme existe, et l'utilisation de la division euclidienne nous montre qu'il est unique.

Cette notion est liée à la notion bien connue en algèbre linéaire de polynôme minimal d'un opérateur. En effet appelons T_α l'opérateur linéaire de l'espace

vectoriel F dans lui même qui à un élément x fait correspondre αx. Il est clair que si P est un polynôme à coefficients dans le corps de base $\mathbb{Z}_p$ alors

$$P(T_\alpha)(x) = P(\alpha).x$$

ce qui montre que le polynôme minimal de α est aussi le polynôme minimal de T_α.

Compte tenu de la définition d'un polynôme minimal il est facile de voir que :

Théorème 3.8 *Dans tout corps fini ayant $q = p^n$ éléments, le polynôme minimal d'un élément est irréductible (attention la réciproque est fausse) et divise $x^q - x$. Le polynôme minimal de α est générateur de l'idéal des polynômes à coefficients dans $\mathbb{Z}_p$ qui s'annulent en α.*

Théorème 3.9 *Dans tout corps fini F ayant $q = p^n$ éléments, le polynôme minimal d'un élément est de degré inférieur ou égal à n.*

Preuve : Soit $u \in F$. Les éléments $1, u, u^2, \cdots, u^n$ sont linéairement dépendants.

Théorème 3.10 *Dans tout corps fini F ayant $q = p^n$ éléments, le polynôme minimal d'un élément primitif est de degré n. (Attention la réciproque est fausse).*

Preuve : Soit α un élément primitif de F et $M(X)$ son polynôme minimal dont on note d le degré. Le corps $\mathbb{Z}_p[X]/\Big(M(X)\Big)$ est de dimension d sur $\mathbb{Z}_p$ et contient F. Donc $d \geq n$ et en vertu du théorème précédent $d = n$.

Théorème 3.11 *L'ensemble des polynômes minimaux des éléments du corps fini F est constitué de tous les facteurs irréductibles de $X^q - X$.*

Preuve : Rappelons que $X^q - X = \prod_{u \in \mathbb{F}_q}(X - u)$. Décomposons maintenant $X^q - X$ sur $\mathbb{Z}_p$ sous la forme

$$X^q - X = \prod_{i \in I} R_i(X),$$

où les polynômes $R_i(X)$ sont irréductibles, à coefficients dans $\mathbb{Z}_p$. Si $u \in F$, le polynôme minimal de u est l'un des polynômes $R_i(X)$: celui qui a u pour

racine. De plus tout polynôme $R_i(X)$ est le polynôme minimal de ses racines. Ainsi les $R_i(X)$ sont exactement les polynmes minimaux des éléments de F.

Nous sommes maintenant en mesure de montrer qu'il n'y a qu'une structure de corps à q éléments.

Théorème 3.12 *Tous les corps finis ayant $q = p^n$ éléments sont isomorphes.*

Preuve : Le polynôme $X^q - X$ se décompose de manière unique sur $\mathbb{Z}_p$ en un produit de facteurs irréductibles (ceci est bien entendu un résultat général concernant tous les polynômes). Soient F et G deux corps ayant $q = p^n$ éléments. Soit α un élément primitif de F et $M(X)$ son polynôme minimal. Alors $M(X)$ est un facteur irréductible de $X^q - X$, c'est donc le polynôme minimal d'un élément β de G. Il est clair que l'homomorphisme de corps qui à α fait correspondre β est un isomorphisme.

Il nous reste maintenant à montrer que :

Théorème 3.13 *Pour tout entier $q = p^n$ puissance d'un nombre premier p il existe un corps ayant q éléments.*

Preuve : Il y a plusieurs démonstrations de ce résultat. L'une d'elles consiste à dénombrer les polynômes de degré n à coefficients dans $\mathbb{Z}_p$ qui sont irréductibles sur $\mathbb{Z}_p$. La démonstration qui suit est différente et utilise le fait immédiat à vérifier que si F est une extension finie de $\mathbb{Z}_p$ qui contient les zéros de $X^q - X$ alors les zéros de $X^q - X$ forment un corps et que ces zéros sont tous distincts. Il est alors facile par extensions successives de construire un corps F qui contient tous les zéros de $X^q - X$ et par suite le corps formé par les zéros de $X^q - X$ répond à la question.

En conclusion nous avons montré que pour chaque entier q puissance d'un nombre premier il existe un corps unique à q éléments et qu'on décrit ainsi tous les corps finis. Le corps à $q = p^n$ éléments est noté $\mathbb{F}_q$ (en particulier $\mathbb{Z}_p$ est aussi noté $\mathbb{F}_p$).

4 Les extensions - Les sous corps

La description des sous corps d'un corps fini est donnée par le

Théorème 4.1 *Soit $\mathbb{F}_{p^n}$ un corps fini (p premier). Les sous corps de ce corps sont les corps $\mathbb{F}_{p^m}$ avec m diviseur de n.*

Preuve : Soit F un sous corps de $\mathbb{F}_{p^n}$. Puisque c'est un sous groupe $\sharp F$ divise p^n, donc est de la forme p^m avec $m \leq n$. F^* est sous groupe multiplicatif de $\mathbb{F}_{p^n}^*$ donc $p^m - 1$ divise $p^n - 1$. Si on note $n = km + r$ on voit que

$$\frac{p^n - 1}{p^m - 1} = p^r \frac{p^{km} - 1}{p^m - 1} + \frac{p^r - 1}{p^m - 1}$$

donc le premier membre est entier si et seulement si $r = 0$. On conclut donc que m divise n et réciproquement.

En particulier soit α un élément de $\mathbb{F}_{p^n}$ et $M_\alpha(X)$ son polynôme minimal. Soit d le degré de ce polynôme. Il est facile de voir que $(1, \alpha, \alpha^2, \cdots, \alpha^{d-1})$ est une base du sous corps engendré par α, et que ce sous corps est isomorphe à $\mathbb{F}_p[X]/(M_\alpha(X))$ ou encore à $\mathbb{F}_{p^d}$. Par suite d divise n. On a donc

Théorème 4.2 *Le degré du polynôme minimal d'un élément α du corps $\mathbb{F}_{p^n}$ divise n.*

De plus aucun sous corps d'ordre strictement inférieur à p^d ne contient α (puisqu'on a considéré le sous corps engendré par α, c'est á dire le plus petit sous corps contenant α). Par suite α ne peut pas être une racine de $X^{p^r} - X$ avec $r < d$.

On sait que les nombres $\alpha, \alpha^p, \cdots, \alpha^{p^{d-1}}$ sont racines du polynôme $M_\alpha(X)$. Si deux d'entre eux étaient égaux par exemple

$$\alpha^{p^i} \text{ et } \alpha^{p^j}$$

avec $0 \leq i < j \leq d - 1$, alors on aurait

$$\alpha^{p^j - p^i} = 1,$$

où encore

$$\alpha^{p^i(p^{j-i}-1)} = 1,$$

ce qui signifie puisque $0 < p^j - p^i < d$ que $p^i(p^{j-i} - 1)$ divise $p^d - 1$. Mais ceci implique que $i = 0$ et donc que α soit racine de $X^{p^j} - X$, ce qui est impossible.

Donc les nombres $\alpha, \alpha^p, \cdots, \alpha^{p^{d-1}}$ dont on sait qu'ils sont racines du polynôme minimal $M_\alpha(X)$ sont distincts. On a donc là toutes les racines de $M_\alpha(X)$ ce qui donne

Théorème 4.3 *Le polynôme minimal d'un élément α se décompose sous la forme*

$$M_\alpha(X) = (X-\alpha)(X-\alpha^p)\cdots(X-\alpha^{p^{d-1}})$$

Définition 4.1 *Les nombres*

$$\alpha^p, \cdots, \alpha^{p^{d-1}}$$

sont les conjugués de α.

Le polynôme caractéristique de α est par définition le polynôme ayant pour racines les nombres $\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$. C'est le polynôme $M_\alpha(X)^{n/d}$.

5 Les polynômes irreductibles et primitifs

Soit $M_\alpha(X)$ le polynôme minimal de $\alpha \in \mathbb{F}_q$ sur $\mathbb{F}_p$. Il se décompose sous la forme

$$M_\alpha(X) = (X-\alpha)(X-\alpha^p)\cdots(X-\alpha^{p^{d-1}})$$

dans $\mathbb{F}_q$, ce qui montre que les fonctions symétriques des racines, c'est-à-dire de α et de ses conjugués sont dans $\mathbb{F}_p$. En particulier on définit la trace de α sur $\mathbb{F}_p$ par

$$Tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}$$

c'est-à-dire la somme des racines du polynôme caractéristique. De même la norme de α sur $\mathbb{F}_p$ est

$$N(\alpha) = \alpha.\alpha^{p^2}.\cdots.\alpha^{p^{n-1}}$$

c'est-à-dire le produit des racines du polynôme caractéristique.