Corps finis

Olivier RIOUL
ENST/COMELEC
olivier.rioul@enst.fr

Version 2.0 (1996-2006)

Cadre privé } sans modifications

Avant-Propos

Ce fascicule décrit les principales propriétés des corps finis, avec toutes les preuves mathématiques. Ce sujet déroute souvent parce que très abstrait : j'espère que cette petite présentation clarifira les esprits.

Comprendre ces propriétés est essentiel pour l'étude des codes linéaires et cycliques, et ce document a été conçu comme annexe de cours sur le codage correcteur. Il est cependant loin d'être exhaustif ; les sujets suivants ne sont pas abordés :

- Sous-corps d'un corps fini : Tout ce qui est ici dans la cadre «$F_q = F_{p^m}$ extension de F_p» peut être refait à l'identique dans le cadre plus général «F_{q^m} extension de F_q».
- Ordre d'un élément quelconque, polynômes cyclotomiques.
- Fonction arithmétiques d'Euler $\varphi(n)$, de Möbius $\mu(n)$; Transformée de Möbius, nombre de polynômes irréductibles sur F_p, d'éléments d'ordre donné.
- Propriétés d'espaces vectoriels des champs, bases. Norme, trace, bases duales.
- Algorithme de Berlekamp de factorisation polynômiale, utilisant le théorème des restes chinois, l'algorithme d'Euclide pour le calcul du pgcd, et la résolution de systèmes linéaires.
- Algorithmes rapides de transformée de Fourier : Algorithme de Hörner, transformations de Rader, de Good-Thomas, de Cooley-Tukey, etc.

Le lecteur intéressé pourra avec profit se référer aux références de la bibliographie donnée en fin de document pour ces sujets plus avancés.

Paris, septembre 2006

Table des matières

Chapitre 1

Domaines et champs

Le titre de ce chapitre pourrait s'intituler aussi « Anneaux et Corps ». Je rappelle ici quelques propriétés de base des structures algébriques indispensables à l'étude des corps finis. La présentation axiomatique des anneaux et des corps a été développé par l'école mathématique allemande à la fin du XIX^{e}siècle et au début du XX^{e}siècle. Le terme « Corps » (*Körper*) est dû à Kummer et Dedekind (en même temps de le terme « idéal ») en liaison avec une tentative de résolution du grand théorème de Fermat. Il a été traduit par *Field* (Champ) en anglais. Le terme « Anneau » (*Ring*) a été inventé par Hilbert un peu plus tard[1], au départ pour des entiers (*Zahlring*). On utilise aussi le mot « domaine » pour un anneau intègre.

1.1 Définitions

En bref, un *domaine*[2] est un endroit où l'on peut *additionner, soustraire et multiplier* comme on a l'habitude de le faire pour les entiers. Cela signifie qu'on peut définir une addition $a+b$ et une multiplication ab à l'intérieur du domaine avec un certain nombre de propriétés :

- Ces opérations sont commutatives ($a+b=b+a$, $ab=ba$) et associatives ($(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$), de sorte que l'on peut manipuler des sommes $\sum_i a_i$ et des produits $\prod_i a_i$ finis sans tenir compte de l'ordre des termes.
- Ajouter 0 ou multiplier par 1 ne change rien. Multiplier par 0 donne 0.

[1] Je me suis longtemps demandé (peut-être est-ce aussi votre cas) quel est le rapport avec l'*anneau* qu'on se passe au doigt. Une explication possible est que cela n'a aucun rapport : ce serait une (mauvaise) traduction de *Ring*, qui, en anglais, signifie aussi un *cercle* (au sens d'un cercle d'amis). En effet, les noms de structures mathématiques font souvent penser à des regroupements de personnes : groupe (groupe de jeunes, groupe professionnel), corps (corps de l'Etat, corps d'Armée).

[2] Le terme consacré en France est : « anneau commutatif unifère intègre », mais j'espère que « domaine » vous convient mieux.

- Addition et multiplication sont reliés par la propriété de distributivité $a(b+c) = ab + ac$ ce qui permet de développer des produits de sommes (par exemple, la formule du binôme : $(a+b)^n = \sum_i C_n^i a^i b^{n-i}$).
- On peut soustraire ($a+x = b$ donne $x = b-a$) mais pas diviser : par exemple, il n'y a pas d'entier x tel que $2x = 1$. Par contre, on peut toujours simplifier ($a+c = b+c$ ou $ac = bc$ donne $a = b$). Pour la multiplication cette propriété provient de : $ab = 0$ implique $a = 0$ ou $b = 0$.

Deux modèles de domaines sont constamment utilisés : les *nombres entiers* et les *polynômes*. Ils sont particulièrement agréables en ce qu'ils permettent de faire de l'arithmétique (voir ci-dessous).

Pour passer d'un domaine à un *champ*[3], il faut de plus être capable de *diviser* (par tout élément non nul). La division de a par $b \neq 0$ donne l'élément x solution de $bx = a$. Il est noté $x = \frac{a}{b}$. En particulier l'inverse de a est $a^{-1} = \frac{1}{a}$. Noter que l'écriture $x = \frac{a}{b}$ est *a priori* ambiguë puisqu'elle peut signifier ab^{-1} ou $b^{-1}a$. Mais ici, comme la multiplication est commutative, cette ambiguïté disparait.

1.2 Un peu d'artihmétique

Pour nous, l'arithmétique concerne uniquement les propriétés multiplicatives des nombres entiers (domaine $\mathbb{Z}$) ou des polynômes $P(x) = \sum_n a_n x^n$ à coefficients dans un champ F (domaine $F[x]$). Tout ce qui suit est valable aussi bien pour les entiers que pour les polynômes. L'une ou l'autre des propriétés suivantes sera utilisé tôt ou tard dans la suite.

Divisibilité et décomposition en facteurs irréductibles On dit que $a|b$ («a divise b») si b est multiple de a, i.e., on peut trouver c tel que $b = ca$. Les diviseurs triviaux (aussi appelés *unités*) divisent tout élément. Ce sont ± 1 dans $\mathbb{Z}$ et les polynômes constants $c \in F$ dans $F[x]$. L'élément p est *irréductible* ou *premier* s'il n'admet aucun diviseur non trivial (et n'est pas une unité). Tout élément se factorise en produit de facteurs irréductibles uniques (à une multiplication par une unité près). On retrouve facilement les propriétés de divisibilité et du pgcd (cf ci-dessous) en ayant en tête cette décomposition : par exemple, si p est irréductible, $p|ab$ implique $p|a$ ou $p|b$.

Pgcd et Bezout Le pgcd de a et b est noté $a \wedge b$: il est égal au produit des facteurs irréductibles communs à a et b, et est donc unique à une multiplication par une unité près. Tout autre diviseur commun le divise (d'où le terme «pgcd» : plus grand commun diviseur). a et b sont *premiers entre eux* si $a \wedge b = 1$, i.e., ils n'ont aucun facteur irréductible commun. On voit facilement que p est irréductible si et seulement si il est premier avec tout élément qu'il ne divise pas. Le pgcd $a \wedge b$ peut toujours s'écrire sous la forme

[3] Un champ est aussi appelé «corps commutatif». «Champ» traduit l'anglais «*field*». Un corps (*skew field*) peut être non commutatif, mais nous n'en rencontrerons pas ici.

$a \wedge b = \alpha a + \beta b$, où α et β sont deux entiers (ou polynômes). En particulier si a et b sont premiers entre eux, on obtient l'identité de Bezout (due à Bachet) :

$$\alpha a + \beta b = 1.$$

Réciproquement cette écriture implique que a et b sont premiers entre eux.

Division avec reste et arithmétique modulaire Même si a ne divise pas b, on peut faire une division avec reste (ou : division euclidienne) de b par a :

$$b = aq + r$$

où q est le quotient et r est le reste. Pour des entiers $|r| < |a|$. Pour des polynômes :

$$B(x) = A(x)Q(x) + R(x)$$

on a $d^\circ R(x) < d^\circ A(x)$. On peut toujours faire des calculs (addition, multiplication) *modulo* un certain élément m, avec la règle : $a = b \bmod m$ si $m|(a-b)$, i.e., s'ils ont même reste dans leur division par m. Ainsi le reste de la division de b par a peut s'écrire $r = b \bmod a$.

Pendant qu'on y est, rappelons quelques règles de vie polynomiale :

Degré Un polynôme (formel) de degré d s'écrit

$$P(x) = \sum_{n=0}^{d} a_n x^n \in F[x].$$

Le nombre de coefficients $a_n \in F$ est $d+1$. Le polynôme est *normalisé* si $a_d = 1$. Les degrés s'ajoutent quand on multiplie des polynômes.

Racines x_0 est une racine de $P(x)$ si $P(x_0) = 0$. Elle peut appartenir au champ F ou à un champ plus grand (contenant F). Un polynôme de degré d a $\leqslant d$ racines dans F. Si $x_0 \in F$ est une racine de $P(x)$, on peut factoriser $P(x) = (x - x_0)Q(x)$ dans $F[x]$. Si $P(x) = a_d x^d + \cdots + a_1 x + a_0$ a pour racines $x_1, \cdots, x_d \neq 0$, le polynôme *réciproque* $\tilde{P}(x) = a_0 x^d + \cdots + a_{d-1} x + a_d$ (écrit en renversant l'ordre des coefficients) a pour racines $1/x_1, \cdots, 1/x_d$.

Racines multiples et dérivée Une racine x_0 est multiple (de multiplicité $k > 1$) si $(x - x_0)^k | P(x)$. Dire que toute racine de $P(x)$ est simple (de multiplicité $= 1$) revient à dire que les racines de $P(x)$ sont distinctes. x_0 est une racine multiple (non simple) si et seulement si $P(x_0) = P'(x_0) = 0$, où $P'(x) = \sum_n n a_n x^{n-1}$ est la dérivée (formelle) de $P(x)$.

1.3 Construire un champ

Dans la suite on ne considérera que des champs particuliers : les *corps finis*[4](bien qu'un certain nombre de résultats s'établissent à l'identique pour des champs infinis).

> Un corps fini F_q est un champ qui ne contient qu'un nombre fini q d'éléments.

Un exemple de corps fini est l'ensemble[5] $F_2 = \{0,1\}$, avec la règle $1+1=0$. Bien qu'il soit simplissime, il est très important en pratique pour représenter des «bits» (chiffres binaires).

Deux constructions de champs (finis ou infinis) à partir d'un domaine sont couramment utilisés : La première consiste à définir «formellement» les *fractions* $\frac{a}{b}$. C'est ainsi qu'on définit le champ $\mathbb{Q}$ des rationnels à partir de $\mathbb{Z}$, ou les fractions rationnelles à partir des polynômes : mais ces champs sont infinis (et donc inintéressants ici). La deuxième utilise l'arithmétique modulaire (cf. ci-dessus) et sera employée dans la suite pour construire des corps finis, à partir du domaine des entiers $\mathbb{Z}$ ou d'une domaine de polynômes $F[x]$. Voici le détail :

0n ne peut pas toujours simplifier des produits ni *a fortiori* diviser modulo m en général. Par exemple $3.2 = 0 \bmod 6$: 2 et 3 n'ont pas d'inverse modulo 6. De même $(x-1)(x+1) = 0 \bmod x^2-1$. En fait, l'inverse de a modulo m existe si et seulement si a et m sont premiers entre eux. En effet, cette dernière assertion équivaut à Bezout : on peut trouver α et μ tels que $\alpha a + \mu m = 1$, i.e. $\alpha a = 1 \bmod m$ ce qui revient à dire que a admet un inverse α modulo m.

> a est inversible modulo $m \iff a \wedge m = 1$

Ainsi, on peut toujours diviser modulo m (i.e. on est dans un champ) si et seulement si m est premier avec tout a non nul (modulo m). Cela revient à dire que m est premier avec tout élément qu'il ne divise pas, i.e. $m = p$ est irréductible. Conclusion :

[4]Il est d'usage en France de parler de «corps fini» plutôt que de «champ fini» («*finite field*» en anglais). En fait, ceci est justifié parce que tout corps fini est commutatif (donc est un champ fini) ; c'est le théorème de Wedderburn (hors sujet !).

[5]La notation F_q (F comme «*field*») est universellement adoptée. On trouve aussi $GF(q)$ («Galois field»). Évariste Galois, le «Rimbaud» des mathématiques, fut tué alors qu'il avait 20 ans : il eût néanmoins le temps de fonder une bonne partie de l'Algèbre moderne (et entre autres les corps finis) à partir de l'âge de 17 ans .

> Les éléments d'un domaine, modulo p, forment un champ si et seulement si p est irréductible. Le champ qui en résulte est noté
>
> $$\mathbb{Z} \bmod p$$
>
> pour les entiers modulo un nombre premier p, et
>
> $$F[x] \bmod P(x)$$
>
> pour les polynômes modulo le polynôme irréductible $P(x)$.

On dispose donc, par réduction modulo[6] un élément irréductible, d'une méthode puissante de construction de champs qui se révèlera très utile dans la suite, pour construire des corps finis. D'ailleurs, grâce à elle, nous disposons d'ores et déjà d'un exemple important de corps fini :

> Les entiers modulo p (premier) forment un corps fini à p éléments $F_p = \mathbb{Z} \bmod p$.

En effet, c'est un champ contenant exactement p éléments $\{0, 1, \cdots, p-1\}$. On retrouve l'exemple $F_2 = \{0, 1\}$ (un bit).

[6] Une autre notation couramment utilisée est $\mathbb{Z}/p$ et $F[x]/P(x)$ («domaines quotients»).

Chapitre 2

Propriétés des Corps Finis

On a déjà vu l'exemple d'un corps fini $F_p = \mathbb{Z}$ mod p à p éléments (où p est un nombre premier). Le problème est maintenant de construire tous les autres corps finis. Pour cela, on va se placer dans un corps fini F_q quelconque, et on va faire un certain nombre d'expériences qui vont nous permettre de le caractériser (et de justifier *a posteriori* son existence !).

2.1 Entiers et Caractéristique

La première expérience que nous allons faire dans F_q consiste à regarder ce qui se passe lorsqu'on considère successivement 1 (élément neutre pour la multiplication), $1+1$, $1+1+1$, etc. On peut les noter comme des entiers : $2 = 1+1$, $3 = 1+1+1$, etc. Plus généralement on note

$$n = 1+1+1+\cdots+1$$

(n termes). On peut également définir $-n$ (opposé de n). On obtient ainsi les *entiers du corps fini* F_q. A chaque entier $n \in \mathbb{Z}$ correspond un entier du corps $n \in F_q$.

Il est clair qu'on peut, à l'intérieur de F_q, additionner et multiplier des entiers comme on le fait dans $\mathbb{Z}$. On peut aussi simplifier des produits puisqu'on est dans le champ F_q. Les entiers de F_q forment donc un *domaine*.

Mais il y a quand même une grande différence avec les entiers de $\mathbb{Z}$: puisque F_q est fini, il apparait forcément dans la liste infinie des entiers de F_q des répétitions. On peut donc trouver deux indices $i < j$ (dans $\mathbb{Z}$) tels que $i = j$ dans F_q. En posant $n = j - i > 0$ (dans $\mathbb{Z}$), on a donc $n = 0$ dans F_q !

> Appelons p le plus petit entier > 0 (dans $\mathbb{Z}$) qui vérifie $p = 0$ dans F_q. On l'appelle la «caractéristique» de F_q.

La liste des entiers $n \in F_q$ prend alors la forme :

$$\cdots, p-1 = -1, 0, 1, 2, \cdots, p-1, 0, 1, 2, \cdots, p-1, 0, 1, \cdots$$

Les entiers $1, 2, \cdots, p-1$ sont tous non nuls par définition de la caractéristique p. Ils sont aussi distincts, sinon par différence on obtiendrait un entier $0 < k < p$ valant zéro dans F_q, ce qui contredit la définition de p. Ainsi, on voit qu'on manipule les entiers de F_q exactement comme des entiers modulo p. On peut donc identifier les entiers de F_q à $\mathbb{Z}$ mod p.

De plus, la caractéristique p est nécessairement un nombre *premier*. Sinon, on aurait $p = ab$ dans $\mathbb{Z}$, avec $0 < a, b < p$. Mais alors, dans F_q, on a $ab = 0$ et donc $a = 0$ ou $b = 0$, ce qui est impossible puisque $0 < a, b < p$. D'après ci-dessus, $\mathbb{Z}$ mod p est un corps fini puisque p est premier. Conclusion :

> Les entiers de F_q forment le corps fini
>
> $$F_p = \mathbb{Z} \text{ mod } p,$$
>
> où p (premier) est la caractéristique de F_q. Ainsi tout corps fini est automatiquement un «champ d'extension» de $F_p = \mathbb{Z}$ mod p, c'est à dire un corps fini contenant F_p.

2.2 Application : relations de Fröbenius

Avant de passer à d'autres «expériences» sur les corps finis, on va continuer à exploiter la notion de caractéristique p dans F_q, qui va nous permettre de simplifier beaucoup de calculs dans F_q. Toutes les relations qu'on va obtenir ci-dessous s'appelent les *relations de Fröbenius*.

Tout d'abord, comment calculer $(a+b)^p$ dans F_q ? On peut toujours développer avec la formule du binôme : $(a+b)^p = \sum_i \mathrm{C}_p^i a^i b^{p-i}$, mais cette formule se simplifie à l'extrême. En effet, dans l'expression de

$$C_p^i = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1},$$

il apparait, lorsque $1 < i < p$, le nombre p au numérateur et des entiers $< p$ au dénominateur. Aucun de ces entiers $< p$ (sauf 1) ne divise le p du numérateur ; les coefficients binomiaux C_p^i sont donc multiples de p pour tout $1 < i < p$ et valent zéro dans F_q. La formule du binôme se réduit donc ici à

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

Il est facile de généraliser par récurrence :

$$(\sum_i a_i)^p = \sum_i (a_i)^p$$

Généralisant encore en mettant plusieurs fois l'expression à la puissance p, on obtient la relation la plus générale :

Dans un corps fini F_q de caractéristique p, toute puissance de p se «distribue» sur les termes d'une somme :

$$(\sum_i a_i)^{p^k} = \sum_i (a_i)^{p^k}$$

On peut trouver d'autres variantes des relations de Fröbenius :

– On a
$$(a-b)^p = a^p - b^p.$$
Cela provient par exemple de $a^p = (a-b+b)^p = (a-b)^p + b^p$. En généralisant : $(a-b)^{p^k} = a^{p^k} - b^{p^k}$.

– En se placant dans $F_p = \mathbb{Z} \bmod p$ et en prenant tous les a_i ci-dessus égaux à 1, on obtient, pour tout entier $n \in F_p$: $n^p = (1+1+\cdots+1)^p = 1^p + 1^p + \cdots + 1^p = 1+1+\cdots+1 = n$. C'est le (petit) *théorème de Fermat* : pour $n \in \mathbb{Z}$ et p premier :
$$n^p = n \bmod p$$
Les éléments de F_p, s'identifient donc, dans un corps fini de caractéristique p, aux racines du polynôme $x^p - x$ (on généralisera ceci à F_q plus tard).

– On peut également simplifier des puissances $p$ièmes de polynômes à coefficients dans F_q : $P(x)^p = (\sum_n a_n x^n)^p = \sum_n (a_n)^p x^{np}$. Puisque d'après le point précédent $(a_n)^p = a_n$ si et seulement si $a_n \in F_p$, on obtient un *critère de Fröbenius* :
$$\boxed{P(x)^p = P(x^p) \iff P(x) \in F_p[x].}$$
Ce critère nous sera très utile pour l'étude des polynômes minimaux.

2.3 Ordre

Entamons maintenant une deuxième expérience dans notre corps fini F_q de caractéristique p. Cette expérience est similaire à la précédente. Au lieu de considérer des multiples de 1 : $n = 1+1+\cdots+1$, on s'intéresse ici aux puissances d'un élément $\alpha \in F_q$ (pas forcément entier).

On va donc regarder ce qui se passe lorsqu'on considère successivement, pour $\alpha \neq 0$, les puissances $\alpha^0 = 1$, $\alpha^1 = \alpha$, α^2, α^3, etc :

$$\alpha^n = \alpha \cdot \alpha \cdots \alpha \qquad (n \text{ facteurs})$$

On peut également définir $\alpha^{-n} = (1/\alpha)^n$. A chaque entier $n \in \mathbb{Z}$ correspond une puissance α^n qui appartient au corps fini F_q.

Ces puissances de α se «manipulent» comme d'habitude : On a par exemple $\alpha^n \alpha^m = \alpha^{n+m}$ et $(\alpha^n)^m = \alpha^{nm}$ pour n, m entiers quelconques. Il y a quand même une grande différence avec ce qu'on a l'habitude de faire dans $\mathbb{Z}$, par exemple : Puisque F_q est fini, il apparait forcément dans la liste infinie des puissances de

α des répétitions. On peut donc trouver deux indices $i < j$ tels que $\alpha^i = \alpha^j$ dans F_q. En posant $n = j - i > 0$ (dans $\mathbb{Z}$), on a donc $\alpha^n = 1$ dans F_q. Autrement dit, tous les éléments α d'un corps fini sont des *racines de l'unité*, c'est à dire des racines d'une équation $x^n = 1$.

> Appelons $\omega = \omega(\alpha)$ le plus petit entier > 0 (dans $\mathbb{Z}$) qui vérifie $\alpha^\omega = 1$ dans F_q. On l'appelle l'«ordre» de α.

La liste des puissances $\alpha^n \in F_q$ prend alors la forme :

$$\cdots, \alpha^{\omega-1} = 1/\alpha, 1, \alpha, \alpha^2, \cdots, \alpha^{\omega-1}, 1, \alpha, \alpha^2, \cdots, \alpha^{\omega-1}, 1, \cdots$$

Les puissances $\alpha^1, \alpha^2, \cdots, \alpha^{\omega-1}$ sont tous $\neq 1$ par définition de l'ordre ω. Ils sont aussi distincts, sinon par division on obtiendrait un entier $0 < k < \omega$ tel que $\alpha^k = 1$ dans F_q, ce qui contredit la définition de ω. Conclusion :

> On manipule les puissances n dans α^n exactement comme des entiers n modulo $\omega = \omega(\alpha)$. En particulier,
>
> $$\alpha^n = 1 \iff \omega | n.$$

Noter l'analogie avec les entiers de F_q : la caractéristique p n'est rien d'autre que l'«ordre» de 1 pour l'addition. Ici, l'ordre est défini pour la multiplication (puissances).

L'ordre peut également se définir dans des cadres plus généraux. Ainsi, dans tout champ, 1 est le seul élément d'ordre 1 et -1 est le seul élément d'ordre 2. Dans $\mathbb{C}$, $e^{2i\pi/n}$ est d'ordre n.

On peut aussi, avec exactement le même raisonnement que ci-dessus, définir l'ordre d'un élément a inversible modulo m ($a \wedge m = 1$). On aura l'occasion d'utiliser ceci plus tard :

> L'ordre de a modulo m (où $a \wedge m = 1$) est le plus petit entier positif ω pour lequel $a^\omega = 1 \bmod m$. Les puissances de a : $a^0, a^1, \cdots, a^{\omega-1} \bmod m$ sont toutes distinctes modulo m et $a^n = 1 \bmod m \iff \omega | n$.

2.4 Description primitive de F_q

On va continuer ici à exploiter la notion d'«ordre» d'un élément dans F_q. Tout d'abord, l'ordre ω de $\alpha \neq 0$ est, d'après ce qu'on a vu, le nombre de puissances de α distinctes. Clairement, ces ω puissances α^k, $k = 0, \cdots, \omega - 1$ sont racines du polynôme $x^\omega - 1$ de degré ω. Par conséquent[1] :

[1] Pour cette raison, on dit que α d'ordre n est une «racine primitive $n$ième de l'unité».

Si $\alpha \in F_q$ est d'ordre ω, les racines de $x^\omega - 1$ sont exactement les puissances α^k pour $k = 0, \cdots, \omega - 1$.

Il y a, dans F_q, au plus $q-1$ éléments non nuls. Puisqu'il y a ω puissances distinctes de α, on doit donc avoir $\omega \leqslant q-1$: l'ordre d'un élément ne peut pas être aussi grand qu'on veut. On va maintenant déterminer la valeur *maximale* possible pour ω.

Appelons donc γ un élément d'*ordre maximal* $m = \omega(\gamma)$. On va montrer que pour tout α d'ordre $n = \omega(\alpha)$, n divise m. Soit $d = m \wedge n$ le pgcd des ordres m et n et $m' = \frac{n}{d}$. Par construction m et m' sont premiers entre eux. On veut montrer que $n|m$, c'est à dire que $m' = 1$ (*a priori* $m' \geqslant 1$). Tout d'abord, l'élément $\gamma' = \alpha^d = \alpha^{n/m'}$ est clairement d'ordre m'. En effet, puisque α est d'ordre n, les m' puissances $\gamma'^k = (\alpha^{n/m'})^k$, $k = 1, \cdots, m'-1$, sont $\neq 1$ et $\gamma'^{m'} = \alpha^n = 1$. On dispose donc de deux éléments γ et γ', d'ordres respectifs m et m', premiers entre eux. Considérons alors le produit $\gamma\gamma'$ d'ordre ω. Puisque $(\gamma\gamma')^{\omega m'} = \gamma^{\omega m'}$, l'ordre de γ doit diviser $\omega m'$, i.e. $m|\omega m'$. Mais comme $m \wedge m' = 1$, il vient $m|\omega$. De même en échangeant les rôles de γ et γ' on obtient $m'|\omega$. Ainsi, toujours parce que $m \wedge m' = 1$, $mm'|\omega$. Mais m est l'ordre maximal, donc $\omega = m$ et nécessairement $m' = 1$. On a bien montré que $n|m$.

Ainsi, l'ordre de tout élément $\alpha \neq 0$ divise $m = \omega(\gamma)$, et par conséquent $\alpha^m = 1$: tous les éléments non nuls de F_q sont racines de la même équation $x^m - 1 = 0$. On peut même facilement préciser quelles sont ces racines : d'après ci-dessus, ce sont les m puissances (distinctes) de γ : $1, \gamma, \gamma^2, \cdots, \gamma^{m-1}$. On en conclut que chacun des $q-1$ éléments non nuls de F_q est une des m puissances (distinctes) de γ. Par conséquent l'ordre maximal est $m = q-1$, et les éléments non nuls de F_q sont exactement les racines de $x^{q-1} - 1$. Conclusion :

Tout corps fini F_q admet un «élément primitif» γ, i.e. d'ordre maximal $= q-1$. Tout élément non nul de F_q est une puissance de γ :

$$\begin{aligned} F_q &= \{0, 1, \gamma, \gamma^2, \cdots, \gamma^{q-2}\} \\ &= \text{ensemble des racines de } x^q - x \end{aligned}$$

On a ainsi complètement décrit la multiplication et la division dans F_q : par exemple, multiplier γ^i et γ^j donne $\gamma^{i+j \bmod q-1}$. Par contre on ne sait rien encore de la structure d'addition – cela découlera du paragraphe suivant.

Il est maintenant facile de caractériser les valeurs que peut prendre l'ordre $\omega(\alpha)$ dans F_q. On sait déjà qu'il doit diviser l'odre maximal $q-1$. Inversement, si $n|q-1$, un élément d'ordre n est par exemple $\alpha = \gamma^{(q-1)/n}$. En effet on a bien $\alpha^k \neq 1$ pour $k = 1, \cdots, n-1$ et $\alpha^n = \gamma^{q-1} = 1$.

F_q admet un élément d'ordre $n \iff n|(q-1)$.

2.5 Adjoindre un élément : Polynôme minimal

Continuons gaiement avec une troisième expérience sur F_q, similaire aux deux précédentes. On considère toujours un élément $\alpha \in F_q$, mais cette fois-ci, on s'intéresse non seulement aux puissances de α mais aussi à toutes les combinaisons à coefficients entiers ($\in F_p$) de puissances de α. Autrement dit, on s'intéresse à toutes les expressions polynômiales :

$$P(\alpha) = \sum_n a_n \alpha^n$$

(où $P(x) \in F_p[x]$) qui vivent toutes dans F_q.

> L'ensemble de ces polynômes en α est noté $F_p[\alpha]$. On dit qu'on a obtenu une extension de F_p en adjoignant α à F_p.

Il est clair qu'on peut, à l'intérieur de F_q, additionner et multiplier des polynômes de $F_p[\alpha]$ comme on le fait dans $F_p[x]$ (on peut également simplifier des produits puisqu'on est dans le champ F_q). $F_p[\alpha]$ est donc un *domaine*.

Mais il y a quand même une grande différence avec les polynômes $\in F_p[x]$: Le corps F_q est fini, alors qu'il y a un infinité d'expressions polynômiales $P(\alpha)$ possibles (on peut toujours considérer un polynôme de degré aussi grand qu'on veut). On peut donc forcément trouver deux expressions polynômiales distinctes ($Q(x) \neq R(x)$ dans $F_p[x]$) pour lesquelles $Q(\alpha) = R(\alpha)$ dans F_q. En posant $P(x) = Q(x) - R(x)$ on obtient que α est toujours racine d'un polynôme[2] : $P(\alpha) = 0$.

Appelons $M_\alpha(x)$ le «plus petit» polynôme (i.e., de degré minimal $d > 0$) s'annulant en α. *A priori* $M_\alpha(x)$ est défini à une constante multiplicative près, mais on peut toujours choisir $M_\alpha(x)$ *normalisé*. $M_\alpha(x)$ est alors bien *unique*. En effet, si deux polynômes normalisés distincts de degré d s'annulent en α, leur différence s'annulerait également en α et serait de degré $< d$, ce qui contredit la définition du polynôme minimal.

> Le «polynôme minimal» de $\alpha \in F_q$ est l'unique polynôme $\in F_p[x]$ normalisé de degré minimal s'annulant en α. Son degré d est le «degré de α» (ou de l'extension $F_p[\alpha]$).

Revenons sur des expressions polynômiales quelconques : $P(\alpha) \in F_p[\alpha]$. On voit facilement qu'on peut toujours considérer $P(x) \bmod M_\alpha(x)$ à la place de $P(x)$, puisque tout multiple de $M_\alpha(x)$ s'annule en α. Le polynôme $P(x)$ est de degré $< d$ après réduction modulo $M_\alpha(x)$ et on peut donc toujours écrire :

$$P(\alpha) = \sum_{n=0}^{d-1} a_n \alpha^n$$

[2] On dit que α est «algébrique» ; $F_p[\alpha]$ est une «extension algébrique simple»

Cette écriture est unique : tous les éléments $\in F_p[\alpha]$ de cette forme sont en effet distincts, sinon par différence on obtiendrait un polynôme de degré $< d$ qui s'annule en α, ce qui contredit la définition du polynôme minimal. Noter que puisqu'il y a p valeurs possibles pour chacun des d coefficients $a_n \in F_p$, on obtient au total p^d éléments distincts dans $F_p[\alpha]$.

On voit donc qu'on manipule les expressions polynômiales de $F_p[\alpha]$ exactement comme des polynômes modulo $M_\alpha(x)$. On peut donc identifier :

$$F_p[\alpha] = F_p[x] \bmod M_\alpha(x).$$

En particulier, tout polynôme s'annulant en α doit être multiple du polynôme minimal de α.

De plus, $M_\alpha(x)$ est nécessairement un polynôme *irréductible*. Sinon, on aurait $M_\alpha(x) = P(x)Q(x)$ dans $F_p[x]$, où $P(x)$ et $Q(x)$ sont de degré $< d$. Mais alors, dans F_q, on a $P(\alpha)Q(\alpha) = 0$ et donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$, ce qui est impossible puisque $P(x)$ et $Q(x)$ sont de degré $< d$.

D'après la construction générale des champs expliquée ci-dessus, $F_p[\alpha] = F_p[x] \bmod M_\alpha(x)$ est un champ puisque $M_\alpha(x)$ est irréductible. Nous avons déja vu qu'il possède exactement p^d éléments. Conclusion :

> Les polynômes en α forment un corps fini à p^d éléments (inclus dans F_q) :
>
> $$F_p[\alpha] = F_p[x] \bmod M_\alpha(x),$$
>
> où $M_\alpha(x)$ (irréductible) est le polynôme minimal de α de degré d. En particulier,
>
> $$P(\alpha) = 0 \iff M_\alpha(x) | P(x)$$

Noter que la démarche faite dans ce paragraphe est exactement la même que celle faite pour les entiers de F_q. On avait obtenu que F_p est «le plus petit sous-corps» de F_q, puisque tout corps fini contient nécessairement F_p. Ici, on obtient que $F_p[\alpha]$, construit par adjonction de $\alpha \in F_q$, est *le plus petit sous-corps de F_q contenant α* (puisque si F_q contient α, il contient nécessairemnt $F_p[\alpha]$). De plus, on sait décrire $F_p[\alpha]$ complètement comme le champ des polynômes modulo $M_\alpha(x)$. Les deux situations se rejoignent en prenant α entier de F_q : On alors $M_\alpha(x) = x - \alpha$, $d = 1$, et $F_p[\alpha] = F_p$.

Un exemple

Si vous commencez à avoir un mal de tête, ne paniquez pas ! Un exemple (dégagé du contexte des corps finis) permettra peut être de clarifier : Le champ des nombres complexes $\mathbb{C}$ de nos grands-pères est obtenu à partir des nombres réels $\mathbb{R}$ en adjoignant i. Le polynôme minimal de i est $x^2 + 1$, $\mathbb{C} = \mathbb{R}[i]$ est donc une extension de $\mathbb{R}$ de degré 2. D'après ci-dessus, on peut aussi définir $\mathbb{C}$ par

$\mathbb{C} = \mathbb{R}[x] \bmod x^2+1$. Vérifier que le produit complexe $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$ correspond bien au produit de polynômes modulo x^2+1 : $(a+bx)(c+dx) \bmod x^2+1$. Vérifier par ailleurs que l'on a bien $P(i) = 0 \iff x^2+1 | P(x)$ pour $P(x) \in \mathbb{R}[x]$.

2.6 Description primitive de F_q (suite) et unicité

On va maintenant exploiter les résultats obtenus sur le polynôme minimal lorsqu'on prend $\alpha = \gamma$ un élément primitif de F_q. Nous savons que F_q contient le corps $F_p[\gamma]$, décrit ci-dessus comme $F_p[\gamma] = F_p[x] \bmod M_\gamma(x)$ où $M_\gamma(x)$ est le polynôme minimal de γ. Ce corps possède exactement p^m éléments, où m est le degré de γ. Mais puisque tout élément de F_q est soit nul, soit une puissance de γ, F_q est inclus dans $F_p[\gamma]$. Il y a donc égalité $F_q = F_p[\gamma]$. Ainsi :

> Un corps fini à q éléments de caractéristique p peut toujours s'écrire sous la forme :
>
> $$F_q = F_p[\gamma] = F_p[x] \bmod M_\gamma(x).$$
>
> où γ est primitif. En particulier q doit être une puissance de p :
>
> $$q = p^m$$
>
> où m est le degré de γ. Le polynôme minimal $M_\gamma(x)$ de γ primitif, est appelé «polynôme primitif».

Cette description de F_q est très utile : elle va nous permettre de construire effectivement F_q en pratique. Noter qu'une conséquence est qu'il ne peut pas exister de corps à q éléments si q n'est pas une puissance d'un nombre premier p. Par exemple, il n'existe pas de corps à 6 éléments.

La caractérisation ci-dessus va nous permettre de montrer facilement que F_q est « essentiellement unique » : Cela signifie qu'il ne peut y avoir, à un changement de notation près éventuellement[3], qu'un seul corps à $q = p^m$ éléments. D'après ce qu'on vient de voir, F_q peut s'écrire $F_q = F_p[x] \bmod M_\gamma(x)$, où $F_p = \mathbb{Z} \bmod p$. Il est donc nécessairement de caractéristique p.

Notons au passage qu'il n'y a qu'un seul corps à p éléments F_p. Il est en effet nécessairement de caractéristique p et donc doit contenir le champ des entiers $\mathbb{Z} \bmod p$, d'où $F_p = \mathbb{Z} \bmod p$: F_p est bien déterminé de manière unique.

Si maintenant F'_q est un autre corps fini à $q = p^m$ éléments, on sait que les éléments non nuls de F'_q sont les racines de $x^{q-1}-1$. Mais puisque $\gamma^{q-1}-1 = 0$, le polynôme minimal $M_\gamma(x)$ doit diviser $x^{q-1}-1$. Par conséquent on peut trouver $\alpha \in F'_q$ tel que $M_\gamma(\alpha) = 0$. On voit alors que $M_\gamma(x)$ est aussi le polynôme minimal

[3] Ce «changement de notation» est ce qu'on appelle un «isomorphisme de corps».

de α. En effet puisque $M_\gamma(\alpha) = 0$, on doit avoir $M_\alpha(x)|M_\gamma(x)$ irréductible d'où $M_\alpha(x) = M_\gamma(x)$. Par conséquent $F_p[\alpha] = F_p[x] \bmod M_\alpha(x)$ est un sous-corps fini de F'_q à $p^m = q$ éléments, donc $= F'_q$. Par ailleurs, comme $M_\alpha(x) = M_\gamma(x)$ ce corps est $= F_p[x] \bmod M_\gamma(x) = F_q$. On peut donc identifier $F_q = F'_q$: l'unicité de F_q est démontrée :

> Un corps fini à q éléments est *unique* (à un isomorphisme de corps près).

Chapitre 3

Construction des Corps Finis

On a vu au chapitre précédent qu'un corps fini F_q à q éléments est nécessairement tel que q est une puissance d'un nombre premier p, et que ce corps est unique à un isomorphisme près. Il reste, pour conclure, à montrer que ce corps *existe* : autrement dit, on cherche maintenant à construire F_q. On donne dans ce chapitre plusieurs constructions, ainsi que des tables qui permettent en pratique de calculer dans F_q.

3.1 Il existe un corps fini à q éléments

On va maintenant prouver l'existence d'un corps à $q = p^m$ éléments. Cette fois-ci on ne fait donc aucune supposition du genre : «plaçons-mous dans un corps fini F_q...» Nous allons d'abord montrer qu'on peut construire facilement $F_q = F_{p^m}$ à la condition que l'on puisse trouver un polynôme irréductible $P(x) \in F_p[x]$ de degré m.

En effet, d'après la fameuse construction de champs par réduction modulo un polynôme irréductible, $F_p[x] \bmod P(x)$ est un champ. Ses éléments α sont des polynômes $\bmod P(x)$, qui peuvent s'écrire comme des polynômes de degré $< m$ après réduction $\bmod P(x)$:

$$\sum_{n=0}^{m-1} a_n x^n \bmod P(x)$$

Il y a p valeurs possibles pour chacun des d coefficients $a_n \in F_p$, donc au total $q = p^m$ éléments. Ces éléments sont bien distincts (i.e., l'écriture ci-dessus est unique), sinon on obtiendrait par différence un polynôme non nul de degré $< m$ égal à 0 $\bmod P(x)$, ce qui est impossible. On a donc bien obtenu un corps à $q = p^m$ éléments.

Cette construction explicite de F_q pose quand même problème, car il se base sur l'existence d'un polynôme irréductible $P(x) \in F_p[x]$ de degré m. Or rien ne nous dit, pour l'instant, qu'un tel polynôme existe toujours pour toute valeur de

p premier et de m ! On ne peut donc pas en déduire, pour l'instant, qu'un corps à p^m éléments existe toujours.

Pour faire le lien avec les paragraphes du chapitre précédent, considérons

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

C'est un élément du corps fini $F_p[x] \bmod P(x)$. Tout élément du corps peut s'écrire :

$$\sum_n a_n x^n \bmod P(x) = \sum_n a_n \alpha^n$$

i.e. comme un polynôme en α. En particulier $P(\alpha) = P(x) \bmod P(x) = 0$: α est donc une racine de $P(x)$. On retrouve donc l'identification

$$F_p[x] \bmod P(x) = F_p[\alpha]$$

mais cette fois ci en construisant α explicitement à partir de $P(x)$. On a ici adjoint «symboliquement» une racine α de $P(x)$ à F_p. Noter que $P(x)$ apparait, *a posteriori*, comme le polynôme minimal de α : en effet $P(\alpha) = 0$ donc $M_\alpha(x)|P(x)$ irréductible, d'où $P(x) = M_\alpha(x)$. La morale de cette histoire est la suivante :

> Etant donné $P(x) \in F_p[x]$ irréductible de degré d, on peut toujours construire un champ d'extension de F_p (de degré d) :
>
> $$F_p[x] \bmod P(x)$$
>
> dans lequel $P(x)$ n'est plus irréductible (puisqu'il admet $\alpha = x \bmod P(x)$ comme racine).

Noter que cette construction marche aussi bien à partir de F_p que de tout corps fini F_q (il suffit de reprendre mot pour mot ce qui précède en remplacant F_p par F_q). On peut donc «casser» tout polynôme irréductible de $F_q[x]$ en se placant dans un corps plus grand.

A partir de là, on peut par récurrence casser complètement tout polynôme $P(x)$ (irréductible ou non) de $F_p[x]$. En effet, en décomposant $P(x)$ en facteurs irréductibles, il suffit d'adjoindre (symboliquement) une racine de l'un de ces facteurs de degré > 1. On obtient un corps fini plus grand (contenant F_p) avec une décomposition plus fine pour $P(x)$, et on recommence tant qu'il reste dans $P(x)$ des facteurs à casser (irréductibles de degré > 1). A la fin on obtient un (énorme) corps fini – contenant tous les autres – dans lequel $P(x)$ se «casse» complètement.

> Tout polynôme $P(x) \in F_p[x]$ admet un «champ de décomposition», c'est à dire un champ d'extension de F_p dans lequel $P(x)$ se décompose complètement (en facteurs du premier degré).

Un exemple

Pour cet exemple on se place à nouveau dans $\mathbb{R}$. Prenons un polynôme irréductible de $\mathbb{R}[x]$ de degré 2 : $P(x) = ax^2+bx+c$, de discriminant $\Delta = b^2-4ac < 0$. Alors $\mathbb{R}[x]$ mod $P(x)$ est en fait une version déquisée de $\mathbb{C}$ dans lequel $P(x)$ admet pour racines complexes $(-b \pm i\sqrt{|\Delta|})/2a$. D'ailleurs on sait bien que $\mathbb{C}$ est un corps de décomposition pour *tout* polynôme $\in \mathbb{R}[x]$, puisqu'un tel polynôme se décompose toujours complètement dans $\mathbb{C}$.

On en déduit d'ailleurs que tout polynôme $\in \mathbb{R}[x]$ se décompose en facteurs de degrés 1 et 2 dans $\mathbb{R}$; il n'y a donc pas, sur $\mathbb{R}$, de polynôme irréductible de degré > 2. Ceci correspond au fait qu'il n'existe pas[1], contrairement à ce qui se passe pour les corps finis, de champ d'extension de $\mathbb{R}$ de degré > 2 : on ne peut pas «généraliser» les nombres complexes.

Une construction de F_q

On va maintenant construire, à partir de rien, un corps fini à $q = p^m$ éléments F_q. On construit tout d'abord un champ F de décomposition du polynôme $x^q - x \in F_p[x]$ (comme expliqué ci-dessus). Ce champ est une extension de F_p, et est donc de caractéristique p. Dans F on définit F_q comme l'ensemble des racines de $x^q - x$. Les q racines de $x^q - x$ sont bien distinctes (simples), car le polynôme dérivé $qx^{q-1} - 1 = p^m x^{q-1} - 1 = -1$ ne s'annule jamais. Par conséquent F_q a bien q éléments. Il reste à montrer que F_q est champ (contenu dans F). La division/différence de deux éléments a et b de F_q est dans F_q, car

$$(a/b)^q = a^q/b^q = a/b \text{ pour } b \neq 0$$

$$(a-b)^q = a^q - b^q = a - b$$

par Fröbenius dans F (q est une puissance de p). Par conséquent F_q est bien stable par inverse/opposé (prendre $a = 1$ ou $0 \in F_q$) et par produit/somme (changer b en $1/b$ ou $-b \in F_q$), donc est un champ. Conclusion :

> Pour tout p premier et $m > 0$, il existe un seul corps fini à $q = p^m$ éléments. Il peut être défini par l'une ou l'autre des caractérisations ci-dessus.

3.2 Construction pratique de F_q

On a donc a notre disposition des corps finis à $2, 3, 4, 5, 7, 8, 9, 11, 13, 16$,... éléments. Le tout est maintenant de pouvoir les construire en pratique. La construction donnée ci-dessus est lourde : on lui préfère $F_q = F_p[x]$ mod $M_\gamma(x)$ où γ est

[1] Il n'existe qu'un seul corps (non commutatif) d'extension de $\mathbb{R}$ de degré > 2 : le corps de quaternions (de degré 4).

primitif. Maintenant qu'on sait que F_q existe, on sait aussi qu'un polynôme primitif $M_\gamma(x)$ existe et qu'on peut donc toujours construire F_q de cette manière.

Comme $\gamma^{q-1} = 1$, on peut trouver $M_\gamma(x)$ parmi les facteurs irréductibles de degré m de $x^{q-1} - 1 = x^{p^m-1} - 1$. Ceci suggère la construction de F_q ($q = p^m$) suivante : Décomposer tout d'abord $x^{q-1} - 1$ dans $F_p[x]$. Cette étape est la plus délicate, mais il existe des algorithmes efficaces (dont celui de Berlekamp, 1967) . Sélectionner ensuite, dans la décomposition $x^{q-1} - 1$, un facteur irréductible $P(x)$ de degré m jusqu'à temps que $\gamma = x \bmod P(x)$ soit d'ordre $q-1$, i.e., primitif. $P(x) = M_\gamma(x)$ est alors un polynôme primitif (nous savons qu'il doit exister).

Voici une liste de quelques polynômes primitifs sur F_2 de degré $1 < m \leqslant 16$ qui permettent de construire les corps finis F_{2^m} :

$x^2 + x + 1$	$x^7 + x^3 + 1$	$x^{12} + x^6 + x^4 + x + 1$
$x^3 + x + 1$	$x^8 + x^4 + x^3 + x^2 + 1$	$x^{13} + x^4 + x^3 + x + 1$
$x^4 + x + 1$	$x^9 + x^4 + 1$	$x^{14} + x^{10} + x^6 + x + 1$
$x^5 + x^2 + 1$	$x^{10} + x^3 + 1$	$x^{15} + x + 1$
$x^6 + x + 1$	$x^{11} + x^2 + 1$	$x^{16} + x^{12} + x^3 + x + 1$

F_q est alors donné par

$$F_q = F_p[\gamma] = F_p[x] \bmod M_\gamma(x) = \{0, 1, \gamma, \cdots, \gamma^{q-2}\}.$$

Ainsi chaque élément correspond à un polynôme en γ de degré $< m$ (modulo $M_\gamma(x)$) et à une puissance de γ. F_q est en fait complètement caractérisé par la table de correspondance donnant les $\gamma^i = P_i(\gamma)$ où $P_i(x) = \sum_n a_n x^n$ est degré $< m$. Pour écrire cette table, il suffit de calculer successivement les γ^i pour $i = 0, 1, \cdots, q-2$, en multipliant par γ et en réduisant modulo $P(x) = M_\gamma(x)$ à chaque fois.

Prenons comme exemple la construction de F_{32}. Le polynôme primitif de la table ci-dessus est $x^5 + x^2 + 1$, et γ d'ordre $32 - 1 = 31$. Le calcul des puissances de γ fournit la table suivante :

$0 = [00000]$	$\gamma^7 = [10100]$	$\gamma^{15} = [11111]$	$\gamma^{23} = [01111]$
$1 = [00001]$	$\gamma^8 = [01101]$	$\gamma^{16} = [11011]$	$\gamma^{24} = [11110]$
$\gamma = [00010]$	$\gamma^9 = [11010]$	$\gamma^{17} = [10011]$	$\gamma^{25} = [11001]$
$\gamma^2 = [00100]$	$\gamma^{10} = [10001]$	$\gamma^{18} = [00011]$	$\gamma^{26} = [10111]$
$\gamma^3 = [01000]$	$\gamma^{11} = [00111]$	$\gamma^{19} = [00110]$	$\gamma^{27} = [01011]$
$\gamma^4 = [10000]$	$\gamma^{12} = [01110]$	$\gamma^{20} = [01100]$	$\gamma^{28} = [10110]$
$\gamma^5 = [00101]$	$\gamma^{13} = [11100]$	$\gamma^{21} = [11000]$	$\gamma^{29} = [01001]$
$\gamma^6 = [01010]$	$\gamma^{14} = [11101]$	$\gamma^{22} = [10101]$	$\gamma^{30} = [10010]$

On prend souvent l'habitude, comme ici, d'écrire les $P_i(\gamma) = \sum_n a_n \gamma^n$ sous forme du vecteur $[a_{m-1} \cdots a_1 a_0]$. Par exemple, $[11101] = \gamma^4 + \gamma^3 + \gamma^2 + 1$.

Une fois cette table de correspondance écrite, il est très facile d'effectuer n'importe qu'elle opération dans F_q. Ainsi, sommer $a = [a_{m-1} \cdots a_1 a_0]$ et $b =$

$[b_{m-1}\cdots b_1 b_0]$ revient à sommer modulo p composante par composante. Par exemple dans F_{32} :

$$\gamma^{13}+\gamma^{22}=[11100]+[10101]=[01001]=\gamma^{29}.$$

Multiplier $a=\gamma^i$ et $b=\gamma^j$ revient à additionner les puissances i et j : c'est une addition modulo $q-1$ puisque γ est d'ordre $q-1$. Par exemple dans F_{32} :

$$[10100]\times[10110]=\gamma^7\gamma^{28}=\gamma^{35}=\gamma^4=[10000].$$

De même, on peut facilement diviser, d'élever à une certaine puissance ou d'extraire une racine carrée, etc.

3.3 Tables des corps finis F_{2^m}

En général, un élément de F_{2^m} peut être représenté soit comme une puissance d'un élément primitif γ, soit comme un polynôme en γ de degré $< m$ (i.e., un vecteur de m bits). Plutôt que de tabuler systématiquement les correspondances entre puissances de γ et vecteurs de m bits (comme dans l'exemple de F_{32} ci-dessus), on va donner les *tables de correspondance de Zech* : elles sont plus simples et permettent de faire tous les calculs désirés plus facilement dans F_{2^m}.

Correspondances de Zech

L'idée est la suivante : pour chaque indice i, on détermine l'indice j tel que

$$1+\gamma^i=\gamma^j.$$

On peut alors effectuer les calculs «à la main» dans F_{2^m} de la façon suivante.

- Tous les éléments non nuls de F_{2^m} sont décrits comme des puissances[2] de γ. Rappelons que lorsqu'on écrit γ^i, i doit être pris modulo 2^m-1.
- Pour la multiplication ou la division, pas de problème : $\gamma^i\gamma^j=\gamma^{i+j}$, $\gamma^i/\gamma^j=\gamma^{i-j}$ (addition ou soustraction $i\pm j$ modulo 2^m-1).
- Pour additionner $\gamma^i+\gamma^j$ (où par exemple $i<j$), on écrit $\gamma^i+\gamma^j=\gamma^i(1+\gamma^{j-i})$ et on trouve l'indice k tel que $\gamma^k=1+\gamma^{j-i}$ à l'aide de la table de Zech. D'où le résultat : $\gamma^i+\gamma^j=\gamma^{i+k}$. Ce genre de calcul est très simple en pratique car il transforme en quelque sorte addition en multiplication. Noter aussi que soustraction = addition dans F_{2^m}.

Remarquer que i et j dans la formule $1+\gamma^i=\gamma^j$ jouent en fait des rôles symmétriques car $1+\gamma^j=\gamma^i$ ($-1=1$ dans un corps de caractéristique 2). Il suffit donc de tabuler les correspondances $i\longleftrightarrow j$. Evidemment, on a toujours $1+1=0$ et $1+0=1$ (inutile de tabuler ces correspondances-ci). Au total il y a donc $2^{m-1}-1$ correspondances à tabuler.

[2] On peut aussi adopter la convention $\gamma^\infty=0$.

Tables de F_4, F_8, F_{16}, F_{32}, F_{64} et F_{128}

Description de F_4 : polynôme primitif x^2+x+1, γ d'ordre 3. Avec la description classique, on obtient :

$0=[00]$	$\gamma=[10]$
$1=[01]$	$\gamma^2=[11]=1+\gamma$

Mais puisque $[10]+1=[11]$, la seule correspondance de Zech à retenir ici est

$1 \longleftrightarrow 2$

Elle suffit à elle seule à décrire F_4 !

Description de F_8 : polynôme primitif x^3+x+1, γ d'ordre 7. Description classique :

$0=[000]$	$\gamma=[010]$	$\gamma^3=[011]$	$\gamma^5=[111]$
$1=[001]$	$\gamma^2=[100]$	$\gamma^4=[110]$	$\gamma^6=[101]$

Table de Zech :

$1 \longleftrightarrow 3$
$2 \longleftrightarrow 6$
$4 \longleftrightarrow 5$

Description de F_{16} : polynôme primitif x^4+x+1, γ d'ordre 15. Description classique :

$0=[0000]$	$\gamma^3=[1000]$	$\gamma^7=[1011]$	$\gamma^{11}=[1110]$
$1=[0001]$	$\gamma^4=[0011]$	$\gamma^8=[0101]$	$\gamma^{12}=[1111]$
$\gamma=[0010]$	$\gamma^5=[0110]$	$\gamma^9=[1010]$	$\gamma^{13}=[1101]$
$\gamma^2=[0100]$	$\gamma^6=[1100]$	$\gamma^{10}=[0111]$	$\gamma^{14}=[1001]$

Table de Zech :

$1 \longleftrightarrow 4$	$6 \longleftrightarrow 13$
$2 \longleftrightarrow 8$	$7 \longleftrightarrow 9$
$3 \longleftrightarrow 14$	$11 \longleftrightarrow 12$
$5 \longleftrightarrow 10$	

Description de F_{32} : polynôme primitif x^5+x^2+1, γ d'ordre 31. La description classique est donnée dans le paragraphe précédent. Table de Zech :

$1 \longleftrightarrow 18$	$7 \longleftrightarrow 22$	$13 \longleftrightarrow 14$
$2 \longleftrightarrow 5$	$8 \longleftrightarrow 20$	$15 \longleftrightarrow 24$
$3 \longleftrightarrow 29$	$9 \longleftrightarrow 16$	$17 \longleftrightarrow 30$
$4 \longleftrightarrow 10$	$11 \longleftrightarrow 19$	$21 \longleftrightarrow 25$
$6 \longleftrightarrow 27$	$12 \longleftrightarrow 23$	$26 \longleftrightarrow 28$

Description de F_{64} : polynôme primitif x^6+x+1, γ d'ordre 63.

$1 \longleftrightarrow 6$	$9 \longleftrightarrow 45$	$17 \longleftrightarrow 47$	$29 \longleftrightarrow 60$	$40 \longleftrightarrow 55$
$2 \longleftrightarrow 12$	$10 \longleftrightarrow 61$	$18 \longleftrightarrow 27$	$30 \longleftrightarrow 46$	$51 \longleftrightarrow 53$
$3 \longleftrightarrow 32$	$11 \longleftrightarrow 25$	$19 \longleftrightarrow 56$	$31 \longleftrightarrow 34$	$57 \longleftrightarrow 58$
$4 \longleftrightarrow 24$	$13 \longleftrightarrow 35$	$20 \longleftrightarrow 59$	$36 \longleftrightarrow 54$	
$5 \longleftrightarrow 62$	$14 \longleftrightarrow 52$	$21 \longleftrightarrow 42$	$37 \longleftrightarrow 44$	
$7 \longleftrightarrow 26$	$15 \longleftrightarrow 23$	$22 \longleftrightarrow 50$	$38 \longleftrightarrow 49$	
$8 \longleftrightarrow 48$	$16 \longleftrightarrow 33$	$28 \longleftrightarrow 41$	$39 \longleftrightarrow 43$	

Description de F_{128} : polynôme primitif $x^7 + x^3 + 1$, γ d'ordre 127.

$1 \leftrightarrow 31$	$13 \leftrightarrow 91$	$25 \leftrightarrow 86$	$41 \leftrightarrow 66$	$58 \leftrightarrow 75$	$83 \leftrightarrow 92$
$2 \leftrightarrow 62$	$15 \leftrightarrow 63$	$26 \leftrightarrow 55$	$42 \leftrightarrow 80$	$59 \leftrightarrow 81$	$87 \leftrightarrow 108$
$3 \leftrightarrow 7$	$16 \leftrightarrow 115$	$27 \leftrightarrow 117$	$43 \leftrightarrow 76$	$60 \leftrightarrow 125$	$90 \leftrightarrow 100$
$4 \leftrightarrow 124$	$17 \leftrightarrow 69$	$29 \leftrightarrow 101$	$45 \leftrightarrow 50$	$61 \leftrightarrow 102$	$93 \leftrightarrow 104$
$5 \leftrightarrow 82$	$18 \leftrightarrow 88$	$30 \leftrightarrow 126$	$46 \leftrightarrow 105$	$64 \leftrightarrow 79$	$96 \leftrightarrow 97$
$6 \leftrightarrow 14$	$19 \leftrightarrow 106$	$32 \leftrightarrow 103$	$47 \leftrightarrow 89$	$65 \leftrightarrow 67$	$99 \leftrightarrow 111$
$8 \leftrightarrow 121$	$20 \leftrightarrow 74$	$33 \leftrightarrow 84$	$48 \leftrightarrow 112$	$70 \leftrightarrow 109$	$113 \leftrightarrow 119$
$9 \leftrightarrow 44$	$21 \leftrightarrow 40$	$35 \leftrightarrow 118$	$51 \leftrightarrow 94$	$71 \leftrightarrow 95$	$120 \leftrightarrow 123$
$10 \leftrightarrow 37$	$22 \leftrightarrow 68$	$36 \leftrightarrow 49$	$52 \leftrightarrow 110$	$72 \leftrightarrow 98$	
$11 \leftrightarrow 34$	$23 \leftrightarrow 116$	$38 \leftrightarrow 85$	$53 \leftrightarrow 73$	$77 \leftrightarrow 122$	
$12 \leftrightarrow 28$	$24 \leftrightarrow 56$	$39 \leftrightarrow 57$	$54 \leftrightarrow 107$	$78 \leftrightarrow 114$	

3.4 Eléments conjugués

Nous savons que le polynôme minimal $M_\alpha(x)$ d'un élément $\alpha \in F_q$ divise $x^q - x$, puisque $\alpha^q = \alpha$. Comme les éléments de F_q sont exactement les racines de $x^q - x$, $M_\alpha(x)$ se décompose complètement dans F_q. Nous allons maintenant expliciter toutes les racines de $M_\alpha(x)$.

Tout d'abord α est bien sûr racine de $M_\alpha(x)$ (par définition du polynôme minimal). D'après Fröbenius, on a $M_\alpha(\alpha^{p^k}) = M_\alpha(\alpha)^{p^k} = 0$, donc les éléments α^{p^k}, $k \geqslant 0$, sont également des racines de $M_\alpha(x)$.

Combien y a-t-il de racines distinctes α^{p^k} ? Nous savons que les puissances p^k interviennent ici modulo ω, où ω est l'ordre de α. Il y a donc autant de racines distinctes que des puissances de p distinctes modulo ω. Mais nous avons également vu que ce nombre est l'ordre m de p modulo ω : les puissances de p distinctes en question sont $1, p, p^2, \cdots, p^{m-1} \bmod \omega$, avec $p^m = 1 \bmod \omega$. Par conséquent les racines distinctes de $M_\alpha(x)$ de la forme α^{p^k} sont $\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{m-1}}$, alors que $\alpha^{p^m} = \alpha$.

A-t-on dénombré toutes les racines possibles de $M_\alpha(x)$? Pour le savoir, formons le polynôme $P(x) = \prod_{i=0}^{m-1}(x - \alpha^{p^i})$. Clairement $P(x)$ divise $M_\alpha(x)$, mais *a priori* $P(x) \in F_q[x]$. Si on peut montrer que $P(x)$ est en fait à coefficients dans F_p, on en déduira $P(x) = M_\alpha(x)$ puisque $M_\alpha(x)$ est irréductible dans $F_p[x]$. Il reste donc à montrer que $P(x) \in F_p[x]$, ce qu'on peut prouver aisément grâce au

critère de Fröbenius :

$$\begin{aligned} P(x)^p &= (x-\alpha)^p (x-\alpha^p)^p \cdots (x-\alpha^{p^{m-1}})^p \\ &= (x^p-\alpha^p)(x^p-\alpha^{p^2})\cdots(x^p-\alpha^{p^m}) = P(x^p) \end{aligned}$$

(on a utilisé $\alpha^{p^m} = \alpha$ pour obtenir la dernière égalité). On a donc bien $P(x) = M_\alpha(x)$. En particulier m apparaît comme le degré de α. Conclusion :

> Les «conjugués» de α : $\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{m-1}}$ sont les racines du polynôme minimal :
>
> $$M_\alpha(x) = \prod_{i=0}^{m-1} (x-\alpha^{p^i})$$
>
> Le degré m de α est le plus petit entier >0 tel que $\alpha^{p^m} = \alpha$ (c'est l'ordre de p modulo l'ordre de α).

Noter qu'en regroupant les éléments de F_q (racines de $x^q - x$) par conjugués, on obtient :

> $x^q - x$ est le produit des différents polynômes minimaux d'éléments de F_q

Connaissant les conjugués de α, $M_\alpha(x) \in F_p[x]$ peut alors se calculer par la formule ci-dessus (qui nécessite de calculer dans F_q). Souvent un simple petit raisonnement permet d'éviter ce calcul (voir ci-dessous). Noter que dans tous les cas, les éléments $\alpha \in F_p$ ont pour polynôme minimal $x-\alpha$, et donc n'ont pas de conjugués autres qu'eux-mêmes. Etant donné un corps fini décrit à l'aide d'un élément primitif γ, il est également facile de déterminer le polynôme minimal de γ : c'est celui qui a servi à construire le corps !

Conjugués et polynômes minimaux pour F_4, F_8 et F_{16}

Pour les exemples ci-dessous, se référer à la description des corps F_{2^m}.

Conjugués et polynômes minimaux pour F_4 : γ et γ^2 sont conjugués. Polynômes minimaux : $M_0(x) = x, M_1(x) = x-1 = x+1$, et $M_\gamma(x) = x^2+x+1$. D'où la décomposition $x^4 + x = x(x+1)(x^2+x+1)$.

Conjugués et polynômes minimaux pour F_8 : Eléments conjugués : $\{\gamma, \gamma^2, \gamma^4\}$, $\{\gamma^3, \gamma^6, \gamma^5\}$. C'est $M_\gamma(x) = x^3+x+1$ qui a servi à construire le corps. Ici, puisque $\{\gamma^6, \gamma^5, \gamma^3\}$ se trouvent être les inverses de $\gamma, \gamma^2, \gamma^4$, le polynôme minimal correspondant est le polynôme réciproque $\tilde{M}_\gamma(x) = x^3+x^2+1$. D'où la décomposition $x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

Conjugués	Polynôme minimal
$\{1\}$	$x+1$
$\{\gamma, \gamma^2, \gamma^4\}$	x^3+x+1
$\{\gamma^3, \gamma^6, \gamma^5\}$	x^3+x^2+1

Conjugués et polynômes minimaux pour F_{16} : Les puissances de γ des éléments conjugués sont : $\{1,2,4,8\}$, $\{3,6,12,9\}$, $\{5,10\}$, $\{7,14,13,11\}$. Ici $M_\gamma(x) = x^4 + x + 1$ et par le même raisonnement que ci dessus, $M_{\gamma^7}(x) = \tilde{M}_\gamma(x) = x^4 + x^3 + 1$. Pour γ^3, on note que les 4 conjugués sont racines de $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. Puisque leur polynôme minimal doit être un facteur de degré 4, c'est forcément $x^4 + x^3 + x^2 + x + 1$. De même, pour γ^5, les deux conjugués sont racines de $x^3 - 1 = (x-1)(x^2 + x + 1)$, d'où $M_{\gamma^5}(x) = x^2 + x + 1$.

Conjugués	Polynôme minimal
$\{1\}$	$x+1$
$\{\gamma, \gamma^2, \gamma^4, \gamma^8\}$	$x^4 + x + 1$
$\{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}$	$x^4 + x^3 + x^2 + x + 1$
$\{\gamma^5, \gamma^{10}\}$	$x^2 + x + 1$
$\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$	$x^4 + x^3 + 1$

Analogie avec les complexes conjugués dans $\mathbb{C}$: Si $\alpha \in \mathbb{R}$, son polynôme minimal $\in \mathbb{R}[x]$ est bien sûr $x - \alpha$. Si par contre $\alpha \in \mathbb{C}$, il est facile de voir que son polynôme minimal $\in \mathbb{R}[x]$ est $x^2 - 2\mathscr{R}e(\alpha)x + |\alpha|^2 = (x-\alpha)(x-\alpha^*)$, où α^* est le conjugué (au sens usuel) de α. Dans $\mathbb{C}$ il ne peut pas y avoir plus que deux conjugués α et α^* (alors que dans un corps fini il peut y en avoir plus).

Chapitre 4

Transformée de Fourier

Je donne dans ce chapitre une présentation algébrique de la transformée de Fourier discrète (TFD). La TFD est un outil de base indispensable dans de nombreux domaines comme le traitement de signal et le codage correcteur d'erreurs. L'accent est mis ici sur les transformées de Fourier définies dans des corps finis.

4.1 Séquences et convolution

Dans de nombreuses situations on est amené à manipuler des séquences finies du type $u_0, u_1, \cdots, u_{n-1}$, où les u_i sont des éléments d'un certain champ F. En codage algébrique une telle séquence représente par exemple un mot de code, dont les symboles u_i appartiennent à un corps fini F_q. En traitement du signal les u_i sont par exemple des échantillons d'un signal à valeurs réelles ou complexes ($u_i \in \mathbb{R}$ ou $\mathbb{C}$) pris à des instants consécutifs. D'où une habitude bien ancrée en traitement du signal : on considère que l'indice i représente le *temps*. On parlera donc, lorsqu'on a affaire aux u_i, de «description temporelle».

Afin de manipuler mathématiquement de telles séquences, on les représente souvent à l'aide d'une «structure algébrique». On peut par exemple voir la séquence $u_0, u_1, \cdots, u_{n-1}$ comme un vecteur colonne ($\in F^n$) :

$$\underline{u} = \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix}$$

et utiliser des outils d'algèbre linéaire (matrices, vecteurs, ...). On peut évidemment la représenter aussi comme un vecteur ligne $\underline{u}^t$ (transposé de $\underline{u}$) – une convention habituelle en codage algébrique. Dans la suite, on va surtout représenter $\underline{u}$ comme un polynôme

$$u(x) = u_0 + u_1 x + \cdots u_{n-1} x^{n-1}$$

de degré $n-1$, et utiliser des outils d'algèbre polynômiale.

On a souvent intérêt à convenir que u_i est définie en fait pour tout $i \in \mathbb{Z}$, en adoptant la convention que $u_i = 0$ pour $i < 0$ et $i \geqslant n$. On peut ainsi, par exemple, définir facilement une translation de j échantillons vers la droite : $v_i = u_{i-j}$ qui correspond en notation polynômiale à $v(x) = x^j u(x)$.

Une opération fondamentale est produit de deux polynômes :

$$v(x) = u(x)h(x)$$

où $u(x)$ est de degré $n-1$ et où $h(x)$ est de degré $l-1$. Le résultat $v(x)$ est de degré $n+l-2$ (et possède donc $n+l-1$ coefficients). En développant $v(x) = \sum_j h_j [x^j u(x)]$ on obtient l'expression du coefficient v_j, $j = 0, \cdots, n+l-2$ comme une somme finie de translatés :

$$v_i = \sum_j h_j u_{i-j}$$

C'est une *convolution discrète* de taille $n \times l$. Elle est couramment utilisée, par exemple pour décrire une opération de filtrage en traitement du signal numérique. La translation en est un cas particulier ($h(x) = x^j$). Noter que la convolution est commutative (puisque $u(x)h(x) = h(x)u(x)$) :

$$v_i = \sum_j u_j h_{i-j}$$

Pour illustrer, une convolution de taille 3×3 s'écrit en clair :

$$\begin{aligned} v_0 &= u_0 h_0 \\ v_1 &= u_0 h_1 + u_1 h_0 \\ v_2 &= u_0 h_2 + u_1 h_1 + u_2 h_0 \\ v_3 &= u_1 h_2 + u_2 h_1 \\ v_4 &= u_2 h_2 \end{aligned}$$

4.2 Séquences et convolution cycliques

Dans toute la suite on s'intéresse à des séquences «cycliques» u_0, u_1, $\cdots$, u_{n-1}. On peut les voir comme des suites infinies, périodiques de période n :

$$\cdots, u_0, u_1, \cdots, u_{n-1}, u_0, u_1, \cdots, u_{n-1}, u_0, u_1, \cdots, u_{n-1}, \cdots$$

Une autre façon de les voir est de considérer que *les indices interviennent modulo n*. Ainsi, $u_{-1} = u_{n-1}$, $u_n = u_0$, etc. On adoptera toujours cette convention dans la suite. Par exemple, une translation cyclique de j échantillons est définie par $v_i = u_{i-j \pmod n}$ Comme on sous-entend désormais que les indices sont pris modulo n, on écrira simplement $v_i = u_{i-j}$.

Les séquences périodiques sont très souvent utilisés en traitement du signal ; en codage algébrique elles représentent des mots de code d'un code cyclique (où $u_i \in F_q$). C'est pourquoi tout ce qu'on va dire dans la suite de ce chapitre est fondamental pour l'étude des codes cycliques.

Quelle est la représentation polynômiale adéquate d'une séquence cyclique ? Elle doit tenir compte du fait que les indices interviennent modulo n. Par exemple, une translation de n échantillons n'a aucun effet. Or nous savons que cette translation correspond à une multiplication par x^n. On doit donc avoir $x^n = x^0 = 1$. Pour cela, il faut adopter une notation polynômiale modulo $x^n - 1$. Ainsi, une séquence cyclique de taille n s'écrit $u(x) \bmod x^n - 1$ en notation polynômiale. La façon correcte d'écrire la translation cyclique $v_i = u_{i-j}$ en notation polynômiale est clairement :

$$v(x) = x^j u(x) \bmod x^n - 1.$$

On peut facilement en déduire l'expression d'un produit polynômial modulo $x^n - 1$:

$$v(x) = h(x)u(x) \bmod x^n - 1 = \sum_{i=0}^{n-1} h_i [x^i u(x)] \bmod x^n - 1$$

Dans cette expression on peut prendre $h(x)$ de degré $n-1$ (puisqu'il n'intervient que par l'intermédiaire de $h(x) \bmod x^n - 1$). On obtient par linéarité $v_i = \sum_j h_j v_{i-j}$, dont l'expression ressemble trait pour trait à la convolution[1] discrète décrite ci-dessus, si ce n'est que les indices sont pris modulo n. Noter que puisque $u(x)h(x) = h(x)u(x)$, on a aussi $v_i = \sum_j u_j h_{i-j}$.

> Une convolution cyclique de taille n :
>
> $$v_i = \sum_j h_j u_{i-j} = \sum_j u_j h_{i-j}$$
>
> (indices modulo n) correspond au produit polynômial :
>
> $$v(x) = h(x)u(x) \bmod x^n - 1$$
>
> La translation cyclique $v_i = u_{i-j}$ en est un cas particulier (pour $h(x) = x^j$).

Pour illustrer, une convolution cyclique de taille 3 est donnée par

$$\begin{aligned} v_0 &= u_0h_0 + u_1h_2 + u_2h_1 \\ v_1 &= u_0h_1 + u_1h_0 + u_2h_2 \\ v_2 &= u_0h_2 + u_1h_1 + u_2h_0 \end{aligned}$$

[1] Ce type de convolution avec les indices modulo n s'appelle indifféremment : convolution cyclique, circulaire, ou périodique. Par opposition la convolution discrète défini ci-dessus se nomme également convolution acyclique, apériodique ou «linéaire» (bien qu'elle ne soit pas plus linéaire que la convolution cyclique).

à comparer avec la convolution acyclique correspondante (cf. ci-dessus). En général, on peut écrire la convolution cyclique matriciellement :

$$\underline{v} = \mathbf{H}\underline{u}$$

où **H** est une «matrice cyclique» :

$$\mathbf{H} = \begin{pmatrix} h_0 & h_{n-1} & \cdots & h_1 \\ h_1 & h_0 & h_{n-1} & h_2 \\ \vdots & & \ddots & \vdots \\ h_{n-1} & h_{n-2} & \cdots & h_0 \end{pmatrix}$$

4.3 Transformée de Fourier discrète

En analyse harmonique ou en traitement du signal, la transformée de Fourier d'une fonction (signal) $u(t) \in \mathbb{R}$ ou $\mathbb{C}$ est d'un usage courant. Elle est donnée par une formule du type

$$U(f) = \int u(t) e^{-2j\pi f t} dt$$

où $j^2 = -1$. Ici t représente le temps et f est la fréquence. Lorsque le signal est échantillonné (u_i pour $i \in \mathbb{Z}$ au lieu de $u(t)$) la formule devient

$$U(f) = \sum_i u_i e^{-2j\pi f i}.$$

C'est une «série de Fourier» pour $U(f)$, qui est périodique de période 1. Enfin, en évaluant la transformée de Fourier pour les n fréquences : $U_k = U(f = k/n)$, $k = 0$ à $n-1$, on obtient la définition d'une *transformée de Fourier discrète (TFD)* de la séquence $u_0, u_1, \cdots, u_{n-1}$:

$$U_k = \sum_{i=0}^{n-1} u_i e^{-2j\pi i k/n} \qquad k = 0, \cdots, n-1$$

C'est cette définition que nous allons exploiter dans la suite.

Ici, la TFD est définie traditionnellement dans $\mathbb{R}$ ou $\mathbb{C}$, mais on peut aisément généraliser. En effet, si on note $W = e^{-2j\pi/n}$, on s'aperçoit que W est *un élément d'ordre n* : les puissances W^k, $k = 1$ à $n-1$, sont toutes $\neq 1$, et $W^n = 1$. On voit alors facilement (cf. chapitres précédents) que les racines du polynôme $x^n - 1$ sont exactement les puissances distinctes de W, à savoir W^k pour $k = 0$ à $n-1$. On va s'apercevoir dans la suite que c'est cette propriété (W d'ordre n) qui est importante dans la TFD ; c'est notamment elle qui va permettre de faire le lien avec la convolution cyclique (pour laquelle on a vu que $x^n - 1$ joue un rôle important). On est donc amené à la définition générale de la TFD suivante :

Dans un champ F admettant un élément W d'ordre n (de sorte que $x^n - 1 = \prod_{k=0}^{n-1}(x - W^k)$ admette n racines distinctes dans F), la transformée de Fourier discrète (TFD) de la séquence $u_0, u_1, \cdots, u_{n-1}$ est la séquence $U_0, U_1, \cdots, U_{n-1}$ définie par :

$$U_k = \sum_{i=0}^{n-1} u_i W^{ik}.$$

Par analogie avec le traitement du signal, on dit que (U_k) est le «spectre» de (u_i), les indices k sont des «fréquences».

On peut également écrire la TFD matriciellement :

$$\underline{U} = \mathbf{W}\underline{u}$$

où $\mathbf{W} = (W^{ik})_{i,k}$ est la «matrice de Fourier» :

$$\mathbf{W} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W & W^2 & \cdots & W^{n-1} \\ \vdots & \vdots & & & \vdots \\ 1 & W^{n-1} & W^{2(n-1)} & \cdots & W^{(n-1)(n-1)} \end{pmatrix}$$

La TFD est donc une *transformation linéaire*. Donnons quelques exemples de définition de la TFD dans $\mathbb{R}$, $\mathbb{C}$ et dans un corps fini F_q.

Transformée de Fourier dans $\mathbb{R}$ et $\mathbb{C}$: $x^n - 1$ ne se décompose complètement sur $\mathbb{R}$ que pour $n = 1$ (racine 1) et $n = 2$ (racines ± 1). Ainsi on ne peut définir une TFD dans $\mathbb{R}$ que pour les longueurs triviales $n = 1$ et 2. Pour $n > 2$ on est obligé de se plonger dans le champ d'extension $\mathbb{C}$ où $x^n - 1$ se décompose toujours complètement. En posant $W = e^{-2j\pi/n}$, on retrouve la définition initiale de la TFD dans $\mathbb{C}$. Mais ce choix pour W d'ordre n n'est pas le seul : $W = e^{2j\pi/n}$ convient aussi, ainsi que par exemple $W = e^{6j\pi/n}$ lorsque n est pair.

Transformée de Fourier dans un corps fini : Pour qu'on puisse définir une TFD dans $F_q = F_{p^m}$ de caractéristique p, il faut que F_q admette un élément d'ordre n. Mais on a vu que cela est possible si et seulement si n divise $q - 1$. Autrement dit, il faut que $p^m = 1 \bmod n$. Cette relation est impossible si n est multiple de p, puisque p est premier[2]. Par conséquent, dans F_q, on ne peut pas définir une TFD de longueur n dès lors que $p|n$. Si maintenant p ne divise pas n (i.e. p est inversible modulo n) on peut toujours trouver m tel que $p^m = 1 \bmod n$. D'ailleurs, on sait que la plus petite valeur de p pour laquelle cela arrive est l'*ordre* de p modulo n.

Une TFD de longueur n ne peut être définie dans un corps fini de caractéristique p que si p ne divise pas n.

[2] D'ailleurs, si $p|n$ – disons $n = pq$ – la relation de Frôbenius $x^n - 1 = x^{pq} - 1 = (x^q - 1)^p$ montre que $x^n - 1$ ne peut pas posséder que de racines distinctes.

Donnons un exemple : On dispose au départ d'éléments de F_2, et on veut définir un TFD de longueur 23. Cela est possible en se placant dans un sur-corps fini F_{2^m} puisque 23 est impair. Les premières puissances de 2 modulo 23 sont

$$1,2,4,8,16,32=9,18,36=13,26=3,6,12,24=1 \pmod{23},$$

par conséquent $m=11$ est la plus petite valeur de m pour laquelle $2^m=1 \bmod 23$. Ainsi, le corps fini $F_{2^{11}}=F_{2048}$ admet bien un élément W d'ordre 23 (que l'on peut trouver grâce à une table de description de ce corps) et on peut définir la TFD de longueur $n=23$ par la formule donnée ci-dessus.

Ainsi, si on dispose au départ d'élements $u_i \in F_p$, il faut en général se plonger dans un sur-corps *localisateur*[3] F_{p^m} pour pouvoir définir une transformée de Fourier : on aura alors $U_k \in F_{p^m}$. Cette situation est analogue à celle déjà observée pour le passage $\mathbb{R} \to \mathbb{C}$.

> Le plus petit corps fini $F_q = F_{p^m}$ admettant un élément W d'ordre n (i.e., dans lequel on peut définir une TFD de longueur n) est appelé «corps localisateur». C'est $F_q = F_{p^m}$ où m est l'ordre de p modulo n (i.e., le plus petit indice m tel que $n|p^m-1$).

Dans le cas particulier où n est de la forme $n=p^m-1$, le corps localisateur est clairement $F_q=F_{p^m}=F_{n+1}$. On peut alors facilement trouver W d'ordre $n=q-1$ puisque c'est un *élément primitif* de F_q. Pour cette raison on dit que $n=p^m-1$ est une *longueur primitive*. Noter que l'on retrouve ici la décomposition $x^{q-1}-1=\prod_{k=0}^{q-2}(x-W^k)$ où les W^k sont exactement les éléments non nuls de F_q.

4.4 Inversion

Nous avons déjà mentionné que la TFD est une transformation linéaire $\underline{U}=\mathbf{W}\underline{u}$. On va maintenant voir comment inverser la TFD, i.e., calculer $\mathbf{W}^{-1}$. Pour ce faire, la méthode la plus simple consiste à calculer la somme géométrique $\sum_{k=0}^{n-1} W^{ik}$. Si $i=0$, on obtient le nombre de termes : n. Sinon, comme W est d'ordre n, $W^i \neq 0$ et $\sum_{k=0}^{n-1} W^{ik}=\frac{W^{in}-1}{W^i-1}=0$ (puisque $W^n=1$). Ainsi, on obtient, en changeant i en $i-j$:

$$\sum_{k=0}^{n-1} W^{ik}W^{-kj}=\begin{cases} n & \text{si } i=j, \\ 0 & \text{sinon.}\end{cases}$$

Le membre de gauche n'est rien d'autre que le terme général d'un produit matriciel égal à l'identité : $\mathbf{W}\mathbf{W}^{-1}=n\mathbf{I}$. Par conséquent l'inverse de $\mathbf{W}$ est $\mathbf{W}^{-1}=$

[3] Le terme «localisateur» vient du codage algébrique : F_{p^m} sert, dans un algorithme de décodage, à localiser (trouver les positions) des erreurs.

$(\frac{1}{n}W^{-ki})_{k,i}$. Elle s'obtient à partir de $\mathbf{W}$ en changeant W en W^{-1} et en divisant par n.

La transformée de Fourier inverse est donnée par

$$U_k = \frac{1}{n}\sum_{i=0}^{n-1} u_i W^{-ki}$$

Ainsi la transformée de Fourier inverse est, au facteur $1/n$ près, une transformée de Fourier avec W^{-1} à la place[4] de W. Noter que dans un corps fini F_{p^m}, $1/n$ doit être interprêté comme l'inverse de l'entier n dans ce corps, i.e., l'inverse de n modulo p. Ceci est bien compatible avec la condition «p ne divise pas n», équivalente à «n inversible modulo p», sans laquelle on ne peut pas définir la TFD de longueur n. Dans le cas particulier d'un corps de caractéristique 2, il n'y a qu'un entier non nul : 1. Dans ce cas on a donc $1/n = 1$, et la formule de la TFD inverse se simplifie.

Noter une relation triviale, mais importante en TFD et polynômes :

Si on représente la séquence u_i et son spectre par des polynômes :

$$u(x) = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$$

$$U(x) = U_0 + U_1 x + \cdots + U_{n-1}x^{n-1}$$

la TFD directe et inverse s'écrivent :

$$U_k = u(W^k)$$

$$u_i = \frac{1}{n}U(W^{-i})$$

4.5 TFD et Convolution cyclique

On va maintenant faire le lien entre convolution cyclique et TFD. Il est tout d'abord facile de voir que la TFD transforme convolution cyclique en produit : la convolution cyclique s'écrit $v(x) = h(x)u(x) \bmod x^n - 1$, d'où en faisant $x = W^k$:

$$V_k = H_k U_k$$

On obtient un produit terme à terme des spectres de u et h. Puisque la TFD est inversible, la transformée de Fourier inverse de ce produit doit redonner une convolution cyclique $v_i = \sum_j h_j u_{i-j}$. Ainsi :

[4] Dans $\mathbb{C}$, W^{-1} et W sont complexes conjugués ; la formule d'inversion implique donc que la TFD est un opérateur *orthogonal* : la matrice $\frac{1}{\sqrt{n}}\mathbf{W}$ est unitaire, i.e. son inverse est égale à sa transposée conjuguée $\frac{1}{\sqrt{n}}\mathbf{W}^\dagger$.

La TFD transforme convolution cyclique en produit :

$$v_i = \sum_j h_j u_{i-j} \iff V_k = H_k U_k$$

En particulier pour $h(x) = x^m$, on voit que la TFD transforme une translation cyclique $v_i = u_{i-m}$ en «modulation» (multiplication par des puissances de W^m) : $V_k = W^{km} U_k$. Grâce à la similarité entre TFD et TFD inverse, on voit que la TFD inverse transforme également translation cyclique $V_k = U_{k-m}$ en modulation $v_i = W^{-im} u_i$ (avec W^{-1} au lieu de W) – ceci revient à dire que la TFD transforme modulation en translation cyclique.

La TFD transforme translation cyclique en modulation et vice versa :

$$u_{i-m} \overset{\text{TFD}}{\longleftrightarrow} W^{km} U_k$$

$$W^{-im} u_i \overset{\text{TFD}}{\longleftrightarrow} U_{k-m}$$

Un peu de sport

On va maintenant montrer que la TFD est la *seule* transformée linéaire qui a cette propriété de transformer convolution cyclique en produit ; cela va justifier *a posteriori* la définition de la TFD – qui peut sembler déroutante au premier abord – en liaison avec la convolution cyclique.

On va en fait montrer le résultat suivant. Ecrivons la convolution cyclique par $\underline{h}$ sous forme matricielle : $\underline{v} = \mathbf{H}\underline{u}$. Si pour tout $\underline{h}$, $\underline{u} \to \underline{U} = \mathbf{W}\underline{u}$ est une transformation linéaire inversible telle que $V_k = H_k U_k$, où $\underline{U} = \mathbf{W}\underline{u}$, $\underline{V} = \mathbf{W}\underline{v}$, et H_k sont n constantes dépendantes de $\underline{h}$, alors la seule possibilité (sauf variante triviale) est que $\underline{U} = \mathbf{W}\underline{u}$ corresponde à une transformée de Fourier discrète. Noter que l'on fait ici des hypothèses très faibles : on ne suppose rien sur la façon dont H_k dépend de $\underline{h}$: les H_k sont en fait simplement définies comme les valeurs propres[5] de $\mathbf{H}$.

On va d'abord traiter le cas $h(x) = x$ d'une translation d'un échantillon $v_i = u_{i-1}$ dont les valeurs popres sont notées W_k. On doit donc avoir $v_i = u_{i-1}$ si et seulement si $V_k = W_k U_k$. Si on opère n fois cette translation, on obtient l'identité. Par conséquent on doit avoir $U_k = (W_k)^n U_k$, d'où $(W_k)^n = 1$: les valeurs propres W_k sont des racines du polynôme $x^n - 1$.

En remplacant, dans $V_k = W_k U_k$, les expressions $V_k = \sum_i W_{k,i} v_i = \sum_i W_{k,i} u_{i-1}$ et $U_k = \sum_i W_{k,i} u_i$, où $W_{k,i}$ est le terme général de la matrice $\mathbf{W}$, on obtient la relation $\sum_i u_i W_{k,i+1} = \sum_i u_i W_{k,i} W_k$. On doit donc avoir $W_{k,i+1} = W_k W_{k,i}$ d'où

[5] Le fait que la transformation $\underline{U} = \mathbf{W}\underline{u}$ transforme la convolution cyclique $\underline{v} = \mathbf{H}\underline{u}$ en produit correspond en fait à une *diagonalisation* de $\mathbf{H}$. En effet, elle équivaut à $\mathbf{W}\underline{v} = \Delta\mathbf{W}\underline{u}$, où Δ est une matrice diagonale dont les éléments sont les H_k. Autrement dit, on a bien la diagonalisation $\mathbf{H} = \mathbf{W}^{-1}\Delta\mathbf{W}$, et les n constantes H_k sont les valeurs propres de $\mathbf{H}$. Le vecteur propre correspondant à H_k est la $k$ième colonne de $\mathbf{W}^{-1}$.

en itérant : $W_{k,i} = (W_k)^i W_{k,0}$. Noter que $W_{k,0} \neq 0$ sinon $\mathbf{W}$ ne serait pas inversible. La matrice $\mathbf{W}$ apparaît donc, à des facteurs multiplicatifs non nuls près, comme une «matrice de Vandermonde». Si certains W_k étaient égaux, il y aurait des lignes proportionelles dans cette matrice, qui ne serait pas inversible. Il faut donc que les W_k soient tous distincts.

Résumons-nous : les W_k doivent être n racines distinctes de $x^n - 1$. Que l'on soit dans $\mathbb{C}$, ou dans un corps fini F_q, on a vu que cela signifiait qu'il existe un élément d'ordre n, noté W, de telle sorte que les racines de $x^n - 1$ soient exactement les puissances W^k, $k = 0$ à $n-1$ (cette propriété est en fait générale dans tout champ). On peut donc choisir, quitte à changer l'ordre des valeurs propres, $W_k = W^k$. La matrice $\mathbf{W}$ est alors bien (à la multiplication des lignes par des constantes non nulles près) de la forme d'un matrice de Fourier $\mathbf{W} = (W_{k,i}) = (W^{ki})$.

Finalement, pour obtenir la propriété pour une convolution cyclique quelconque, il suffit de considérer $v_i = \sum_j h_j u_{i-j}$ comme une combinaison linéaire de translations de j échantillons (dont les valeurs propres sont les $(W_k)^j$). On obtient donc l'équivalence avec $V_k = [\sum_j h_j (W_k)^j] U_k$ qui est bien de la forme voulue. Les valeurs propres correspondantes sont $H_k = \sum_j h_j W^{jk}$. Ainsi $\underline{H}$ s'obtient aussi par TFD : $\underline{H} = \mathbf{W}\underline{h}$.

> La TFD est la seule transformation linéaire inversible qui diagonalise la convolution cyclique (i.e., transforme convolution cyclique en produit).

4.6 Décimation cyclique

Opérer une *décimation cyclique* sur une séquence u_i (i mod n) consiste à calculer u_{ai} où $a > 0$ est le facteur de décimation. Par exemple, u_{2i}, $i = 0, \cdots, n-1$ est un décimé cyclique de u_i, où l'on a pris un échantillon sur deux.

Malgré les apparences, on ne perd pas d'information en décimant une séquence par une facteur a, pourvu que a et n soient *premiers entre eux* (ce qu'on suppose désormais). En effet, sous cette condition, a est inversible modulo n ; la transformation $i \to ai$ mod n est donc un simple «changement de variable» réversible. Autrement dit, les u_{ai}, $i = 0, \cdots, n-1$ sont exactement les échantillons u_i, pris dans un autre ordre.

Ce type de changement de variable est parfois utile. Illustrons-le en calculant le TFD du décimé cyclique. Par changement de variable $j = ai$,

$$\sum_{i=0}^{n-1} u_{ai} W^{ik} = \sum_{j=0}^{n-1} u_j W^{jk/a}$$

où $1/a$ est l'inverse de a modulo n. Ainsi :

Lorsque $a \wedge n = 1$,

$$u_{ai} \overset{\text{TFD}}{\longleftrightarrow} U_{k/a}$$

où $k/a = a^{-1}k$ doit être interprété modulo n.

La décimation par un facteur a correspond à une certaine permutation des échantillons u_i ; en transformée de Fourier elle correspond à la permutation inverse sur les U_k.

On va utiliser tout de suite cette propriété de décimation cyclique pour établir les contraintes de conjugaison de la TFD, qui sont particulièrement importantes.

4.7 Contraintes de conjugaison

Il arrive souvent que les échantillons (ou symboles) u_i d'une séquence appartiennent à un certain champ F, et que pour calculer la TFD on ait besoin de se placer dans un sur-corps localisateur F' plus grand. La TFD U_k doit alors vérifier une « *contrainte de conjugaison* », qui traduit que les symboles de départ appartiennent non pas à F', mais seulement à F.

Les contraintes de conjugaison de la TFD d'une séquence réelle sont bien connues. Un échantillon $u_i \in \mathbb{R}$ est réel s'il est égal à son conjugué : $u_i = u_i^*$. Comme la TFD est inversible, cela revient à dire, par TFD, que $U_k = \sum_i u_i^* W^{ik}$. Cette dernière somme se réduit à U_{-k}^* puisque $W^* = W^{-1}$. On obtient donc le résultat (bien connu) :

Dans $\mathbb{C}$, U_k est la TFD d'une séquence réelle si et seulement si elle est à symétrie hermitienne : $U_k = U_{-k}^*$.

On va maintenant établir les contraintes de conjugaison dans le cas des corps finis. On suppose ici que les symboles u_i appartiennent à $F = F_p$, et que le sur-corps localisateur (dans lequel on définit U_k) est $F_q = F_{p^m}$. Le raisonnement est tout à fait analogue à celui fait pour $F = \mathbb{R}$.

Nous savons que les conjugués de u_i sont les puissances $u_i^{p^k}$, $k > 0$. Mais puisque $u_i \in F_p$, son polynôme minimal n'a qu'une racine u_i. Ainsi on peut affirmer que $u_i \in F_p$ si et seulement si il est égal à ses conjugués, ce qui revient à dire que $u_i = u_i^p$. On obtient donc[6], par transformée de Fourier, que $u_i \in F_p$ si et seulement si :

$$U_k = \sum_{i=0}^{n-1} u_i^p W^{ik}$$

[6]Une autre façon d'obtenir cette caractérisation est de remarquer que, d'après la théorie des corps finis, les éléments de F_p sont exactement les racines de $x^p - x$. Ainsi $u_i \in F_p \iff u_i = u_i^p$.

Puisque p est premier avec n, on peut opérer le changement de variable $k \to kp$ (décimation cyclique). On obtient :

$$U_{kp} = \sum_{i=0}^{n-1} u_i^p (W^{ik})^p$$

et cette dernière somme se réduit

$$\left(\sum_{i=0}^{n-1} u_i W^{ik} \right)^p = (U_k)^p$$

par les relations de Fröbenius. Ainsi :

> $U_k \in F_{p^m}$ est la TFD d'une séquence d'éléments de F_p si et seulement si
>
> $$U_{kp} = (U_k)^p.$$

4.8 Accords de conjugaison

On vient de voir que la TFD d'une séquence réelle est à symétrie hermitienne. On peut donc ne spécifier les valeurs du spectre U_k que pour $0 \leqslant k \leqslant n/2$. En effet les autres sont alors automatiquement déterminées par la contrainte de conjugaison $U_{n-k} = U_{-k} = U_k^*$. En général $U_k \in \mathbb{C}$, mais il y a au moins une exception : U_0 doit être réel puisque $U_0 = U_{-0} = U_0^*$. De même, $U_{n/2} \in \mathbb{R}$ (lorsque n est pair). On a ainsi complètement spécifié le spectre d'une séquence réelle.

On va maintenant faire de même lorsque $u_i \in F_p$. Pour cela il est utile d'introduire la notion d'*accord de conjugaison*[7].

Lorsqu'on spécifie la valeur de U_k dans le corps localisateur, à cause des contraintes de conjugaison $U_{lp} = (U_l)^p$, on spécifie du même coup les valeurs de $U_{kp}, U_{kp^2}, \cdots$ par la formule $U_{kp^j} = (U_k)^{p^j}$. Autrement dit le spectre évalué à la fréquence k l'est automatiquement pour toutes les fréquences kp^j $(j \geqslant 0)$. Ces fréquences sont appelées *fréquences conjuguées* car elles correspondent aux conjugués de W^k : $W^k, W^{kp}, \cdots W^{kp^{d-1}}$ par la relation $U_{kp^j} = u(W^{kp^j})$. D'après la théorie des corps finis, il y a exactement d éléments conjugués de W^k, où d (le degré de W^k) est le plus petit entier tel que $(W^k)^{p^d} = W^k$, i.e., $kp^d = k \bmod n$. Tout ceci motive la définition suivante :

> L'accord de conjugaison de k est l'ensemble des fréquences conjuguées de k :
>
> $$A_k = \{k, pk, p^2k, \cdots, p^{d-1}k \bmod n\}$$
>
> où $d = d(k)$ est le plus petit entier tel que $p^d k = k \bmod n$.

[7] Pour nous un *accord* est un ensemble de fréquences. Les «accords de conjugaison» décrits ici sont aussi appelés les «classes cyclotomiques p-aires modulo n».

On peut ainsi partitionner (découper) les fréquences $\{0,1,\cdots,n-1\}$ en un ensemble d'accords de conjugaison. Par exemple, pour $n=23$ et $p=2$, $A_0=\{0\}$, $A_1=\{1,2,4,8,16,9,18,13,3,6,12\}$, et $A_5=\{5,10,20,17,11,22,21,19,\ 15,\ 7,14\}$; ici trois accords de conjugaison suffisent pour partitionner toutes les fréquences.

D'après ce qu'on vient de voir, spécifier une valeur du spectre U_k spécifie du même coup toutes les valeurs U_l, où $l \in A_k$. Mais ce n'est pas tout : si d est le nombre de fréquences conjuguées dans A_k, on doit également avoir, à cause des contraintes de conjugaison, $U_{kp^d} = (U_k)^{p^d} = U_k$. Autrement dit U_k doit être une racine de $x^{p^d} - x$, c'est à dire un élément du corps fini F_{p^d}, qui est intermédiaire entre F_p et le corps localisateur F_{p^m} ; U_k ne peut donc pas, en général, prendre une valeur quelconque dans F_{p^m}. En résumé, les contraintes de conjugaison déterminent la nature du spectre U_k :

> U_k est le spectre d'une séquence d'éléments de F_p si et seulement si :
> • U_k prend une valeur de F_{p^d}, où d est le nombre d'éléments de l'accord de conjugaison de k.
> • Les valeurs du spectre aux autres fréquences de l'accord de conjugaison s'en déduisent par $U_{kp^j} = (U_k)^{p^j}$

Bibliographie

[1] Robert Mc Eliece, *Finite fields for computer scientists and engineers*, Kluwer Academic, 1987. Livre admirable, pour une introduction aux corps finis.

[2] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997. Extrêmement complet !