Master CSI, Arithmétique 1 : corps finis et applications

Gilles Zémor

11 décembre 2006

Première partie

Corps finis

1 Anneaux quotients de $\mathbb{Z}$ et de $K[X]$

1.1 Généralités, anneaux, idéaux, anneaux quotients, caractéristique

Un *anneau* $(A, +, \times)$ est un ensemble A muni de deux opérations (lois), $+$ et $\times$, telles que $(A, +)$ est un groupe commutatif d'élément neutre noté 0, et telles que $\times$ est associative, distributive par rapport à $+$, et munie d'un élément neutre noté 1. On note A^* le *groupe multiplicatif* de A, constitué des éléments inversibles (ou unités) de A. Ne pas confondre A^* avec $A \setminus \{0\}$: l'anneau A est un *corps* lorsque $A^* = A \setminus \{0\}$. On ne considérera que des anneaux commutatifs (i.e. dont la multiplication est commutative), de même lorsque nous parlerons de corps nous sous-entendrons qu'il s'agit d'un corps commutatif.

Un *idéal* I de A est un sous-groupe additif de A avec la propriété supplémentaire :

$$a \in A, x \in I \Rightarrow ax \in I.$$

L'anneau quotient A/I est l'ensemble des parties de A de la forme $x + I$. On vérifie que l'addition et la multiplication des parties $(x + I)$ et $(y + I)$ fait de A/I un anneau, et que l'application $x \mapsto x + I$ (la projection) est un morphisme de A sur A/I. L'ensemble aA des multiples de $a \in A$ est appelé *l'idéal principal* engendré par a, et est parfois noté (a).

On emploie également les notations :

$$a \equiv b \bmod I \qquad a \equiv b \mod c$$

pour signifier que les éléments a et b de A se projettent sur le même élément de l'anneau quotient A/I (resp. $A/(c)$), i.e. $a - b \in I$ (resp. $a - b \in (c)$). On écrit aussi $a = b \bmod I$, $a = b \bmod c$. On a tendance à utiliser la même notation a pour signifier l'élément de A et son projeté dans A/I s'il n'y a pas d'ambiguïté : s'il y a ambiguïté on utilise parfois la phrase «a modulo I» pour signifier le projeté de a.

Exemples d'anneaux : $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}, K[X], K[X,Y], K[[X]], K(X), \mathbb{Z}[i]$.

Dans la suite on s'intéresse plus particulièrement aux cas de $\mathbb{Z}$ et de $K[X]$, l'anneau des polynômes à coefficients dans le corps commutatif K, ainsi qu'à leurs quotients.

Soit ϕ l'application

$$\begin{array}{rcl} \phi : \mathbb{N} & \longrightarrow & A \\ n & \mapsto & \underbrace{1+1+\cdots+1}_{n \text{ fois}} \end{array}$$

qui se prolonge en un morphisme d'anneaux de $\mathbb{Z}$ dans A. On appelle *caractéristique* de A, et l'on la note $car(A)$, le plus petit entier strictement positif n, s'il existe, tel que $\phi(n) = 0$ dans A : si cet entier n'existe pas on définit la caractéristique de A comme étant égale à zéro.

– Exercice 1. *Montrer que si $n = car(A)$, $\ker \phi = n\mathbb{Z}$ et qu'il existe un isomorphisme d'anneaux entre $\mathbb{Z}/n\mathbb{Z}$ et un sous-anneau de A.*

1.2 Reconnaître un inversible et calculer l'inverse dans $A = \mathbb{Z}/n\mathbb{Z}$, $A = K[X]/(P)$

On note également par $\mathbb{F}_2$ l'anneau (et le corps) $\mathbb{Z}/2\mathbb{Z}$.

– Exercice 2. *Soit A l'anneau $A = \mathbb{F}_2[X]/(X^3+1)$. Décrire A, combien A a-t-il d'éléments ? Quel est A^* ?*

– **Solution.** $A^* = \{1, X, X^2\}$. `On a la factorisation` $X^3+1 = (X+1)(X^2+X+1)$. `Après avoir exclu les multiples de` $(X+1)$ `et` (X^2+X+1) `il reste` X `et` X^2. `On constate qu'ils sont inverses l'un de l'autre.`

L'exercice précédent se généralise de la manière suivante :

Théorème 1 *On a les caractérisations suivantes de l'inversibilité :*

— *l 'entier k est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si* $\text{pgcd}(k, n) = 1$.
— *le polynôme $Q(X)$ est inversible dans l'anneau $K[X]/(P)$ si et seulement si* $\text{pgcd}(P, Q) = 1$.

Si d est un diviseur non-trivial commun à k et à n, on a, en posant $a = n/d \neq 0$ dans $\mathbb{Z}/n\mathbb{Z}$, $ka = 0 \bmod n$. L'élément k de $\mathbb{Z}/n\mathbb{Z}$ n'est donc pas inversible, sinon l'associativité de la multiplication impliquerait les égalités suivantes dans $\mathbb{Z}/n\mathbb{Z}$

$$a = (k^{-1}k)a = k^{-1}(ka) = k^{-1}0 = 0$$

ce qui est absurde. On raisonne identiquement dans $K[X]/(P)$.

La réciproque, c'est-à-dire être premier avec n (ou avec P) implique l'inversibilité, vient de l'existence de la *division euclidienne* dans $\mathbb{Z}$ et dans $K[X]$.

On *reconnaît* donc le caractère inversible d'un élément d'un de ces anneaux quotients grâce à l'algorithme d'Euclide. On *calcule* l'inverse d'un élément par l'algorithme d'Euclide étendu qui nous donne une identité de Bézout. Soit à calculer, par exemple, l'inverse de $X^2 + 1$ dans $\mathbb{F}_2[X]/(X^4 + X + 1)$. L'identité de Bézout à trouver est de la forme :

$$U(X)(X^4 + X + 1) + V(X)(X^2 + 1) = 1.$$

L'algorithme d'Euclide appliqué à $(X^4 + X + 1)$ et $X^2 + 1$ nous donne la suite de divisions euclidiennes suivantes :

$$\begin{aligned} X^4 + X + 1 &= (X^2 + 1)(X^2 + 1) + X \quad (1) \\ X^2 + 1 &= X \cdot X + 1 \quad (2) \end{aligned}$$

Pour trouver l'identité de Bézout, on écrit la dernière égalité (2) sous la forme :

$$1 = (X^2 + 1) + X \cdot X \quad (3)$$

Puis on remonte progressivement la suite d'égalités, en remplaçant le reste de la division euclidienne par son expression : ici on transforme (1) en une expression pour le reste X

$$X = X^4 + X + 1 + (X^2 + 1)(X^2 + 1)$$

et l'on substitue dans (3) pour obtenir

$$\begin{aligned} 1 &= (X^2 + 1) + X(X^4 + X + 1 + (X^2 + 1)(X^2 + 1)) \\ 1 &= X(X^4 + X + 1) + (1 + X(X^2 + 1))(X^2 + 1) \\ 1 &= X(X^4 + X + 1) + (X^3 + X + 1)(X^2 + 1). \end{aligned}$$

C'est l'identité de Bézout avec $U(X) = X$ et $V(X) = X^3 + X + 1$. L'inverse de $X^2 + 1$ dans $\mathbb{F}_2[X]/(X^4 + X + 1)$ est $V(X) = X^3 + X + 1$.

1.3 Irréductibilité, polynômes irréductibles

On a la conséquence suivante du théorème 1 :

Proposition 2 *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. L'anneau $K[X]/(P)$ est un corps si et seulement si le polynôme $P(X)$ est irréductible.*

Notons qu'un polynôme $P(X) \in K[X]$ admet a comme racine dans K si et seulement s'il est divisible par le polynôme $(X-a)$. En particulier, si un polynôme est irréductible sur K, et s'il est de degré strictement supérieur à 2, il n'a pas de racine dans K. Attention, la réciproque n'est pas vraie, un produit de deux polynômes irréductibles sur K de degrés > 1, n'a toujours pas de racine dans K, mais n'est plus irréductible.

Il y a unicité de la décomposition en facteurs irréductibles dans les anneaux $\mathbb{Z}$ et $K[X]$ (c'est une conséquence de l'existence de la division euclidienne). En particulier, retenons :

Proposition 3 *le nombre de racines d'un polynôme de $K[X]$ est inférieur ou égal à son degré.*

– Exercice 3. *Quels sont tous les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 3 ? de degré 4 ?*

Points essentiels à retenir

- l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier
- l'anneau $K[X]/(P)$ est un corps si et seulement si $P(X)$ est irréductible sur K
- savoir calculer un inverse dans $\mathbb{Z}/n\mathbb{Z}$ et $K[X]/(P)$
- savoir ce qu'est la caractéristique d'un anneau.

2 Corps finis, extensions de corps

2.1 Premières constructions de corps finis

La proposition 2 nous donne deux manières de construire un corps fini :

— prendre un nombre premier p et former le quotient $\mathbb{Z}/p\mathbb{Z}$,
— prendre un polynôme P irréductible sur le corps $\mathbb{Z}/p\mathbb{Z}$ et former le quotient $\mathbb{Z}/p\mathbb{Z}[X]/(P)$.

– Exercice 4. *Soit P un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ de degré n. Pourquoi l'anneau $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ a-t-il p^n éléments ?*

Les questions que nous voulons nous poser maintenant sont :

1. Ces constructions nous permettent-elles d'obtenir *tous* les corps finis, à isomorphisme près ?
2. Deux polynômes P et Q de $\mathbb{Z}/p\mathbb{Z}[X]$, irréductibles et de même degrés, donnent naissance à deux structures de corps à $q = p^n$ éléments. S'agit-il de structures essentiellement différentes, ou existe-t-il un isomorphisme caché entre les deux ?

Commençons par chercher la réponse à la première question. Soit donc un corps $\mathbb{F}$, que nous supposerons fini et à $|\mathbb{F}| = q$ éléments.

– Exercice 5. *Montrer que la caractéristique de $\mathbb{F}$ est un nombre premier p.*

Le corps $\mathbb{F}$ contient donc un sous-corps $\mathbb{F}_p$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On constate que $\mathbb{F}$ est naturellement muni d'une structure d'espace vectoriel sur $\mathbb{F}_p$ (il suffit de dégrader la multiplication interne dans $\mathbb{F}$ en la multiplication externe par $\mathbb{F}_p$. Puisque $\mathbb{F}$ a un nombre fini d'éléments, il ne peut-être que de dimension finie n sur $\mathbb{F}_p$, il a donc $q = p^n$ éléments. On peut donc soupçonner que la réponse à la question 1 est affirmative, auquel cas il s'agit de mettre en évidence un polynôme P irréductible de degré n sur $\mathbb{Z}/p\mathbb{Z}$ et un isomorphisme entre $\mathbb{F}$ et $\mathbb{Z}/p\mathbb{Z}[X]/(P)$. Pour ce faire, commençons par quelques généralités sur les extensions de corps.

2.2 Extensions de corps, extensions simples

Généralisons légèrement la situation précédente, soit K un corps (commutatif) qu'il n'est pas nécessaire pour l'instant de supposer fini, et soit L une *extension* du corps K. Ceci veut dire que L contient K comme sous-ensemble et que l'addition et la multiplication dans L prolongent celles de K : en d'autres termes, si $x, y \in K$, $x + y$ et $x \times y$ désignent le même élément (de K) que les opérations soient prises dans $(K, +, \times)$ ou dans $(L, +, \times)$. On note l'extension par L/K ou $L : K$.

Commençons par la même remarque qu'au paragraphe précédent : le corps L est muni d'une structure d'espace vectoriel sur K. Si cette espace vectoriel est de dimension finie on note $[L : K]$ sa dimension, on dit que l'extension L/K est *finie*, et on appelle $[L : K]$ le *degré* de l'extension.

On a la formule suivante.

Proposition 4 *Soient L/K et M/L des extensions finies. Alors M/K est une extension finie et $[M : K] = [M : L][L : K]$.*

Preuve : Soit $(\ell_i)_{i=1..a}$ une base de L sur K où $a = \dim_K L$. Soit $(m_j)_{j=1..b}$ une base de M sur L où $b = \dim_L M$. On vérifie, sans difficulté particulière, que $(\ell_i m_j)_{i=1..a,j=1..b}$ est une base de M sur K. ∎

Définition 5 *Soit L/K une extension et soit $\alpha \in L$. On note $K(\alpha)$ l'intersection de tous les sous-corps de L contenant K et α. On dit que c'est le plus petit corps contenant K et α, ou encore le corps engendré par K et α. On dit que L est une* extension simple *de K s'il existe $\alpha \in L$ tel que $L = K(\alpha)$. On dit encore que α est* algébrique *sur K si l'extension $K(\alpha)/K$ est finie.*

Lorsque α est algébrique sur K on appelle *polynôme minimal* $P_\alpha(X)$ de α, le polynôme unitaire non nul de $K[X]$ de plus petit degré s'annulant en α.

– Exercice 6. *Montrer que le polynôme minimal $P_\alpha(X)$ de α est irréductible sur K.*

– Exercice 7. *Soit $I_\alpha = \{P(X) \in K[X] \mid P(\alpha) = 0\}$. Montrer que I_α est l'idéal (P_α).*

– Exercice 8. *Lorsque α est algébrique sur K, montrer que $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ est une base de $K(\alpha)$ sur K, où $n = \deg(P_\alpha) = [K(\alpha) : K]$.*

On vient de montrer que l'application

$$\begin{array}{rccc} \phi & : K[X] & \longrightarrow & K(\alpha) \\ & P(X) & \mapsto & P(\alpha) \end{array}$$

induit par passage au quotient l'isorphisme $K[X]/(P_\alpha) \xrightarrow{\sim} K(\alpha)$.

Énonçons :

Proposition 6 *Lorsque α est algébrique sur K, son polynôme minimal est irréductible et le corps $K(\alpha)$ est isomorphe à $K[X]/(P_\alpha)$.*

Nous pouvons maintenant reformuler la question 1 de la section 2.1 ainsi : «tout corps fini $\mathbb{F}$ est-il une extension algébrique simple de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, où $p = car(\mathbb{F})$?»

3 Théorème de l'élément primitif

Dorénavant nous nous intéressons exclusivement aux corps finis. Le résultat principal de cette section est le théorème suivant, appelé «théorème de l'élément primitif» :

Théorème 7 *Le groupe multiplicatif K^* d'un corps fini K est un groupe cyclique. Tout générateur de ce groupe est appelé* élément primitif de K.

Pour démontrer ce théorème nous utiliserons le résultat suivant : rappelons que le nombre d'entiers k, $1 \leqslant k \leqslant n$, premiers avec l'entier $n \geqslant 1$ est habituellement noté $\phi(n)$ (indicateur d'Euler de n). Il s'agit du nombre de générateurs du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$. C'est aussi, (théorème 1) le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, x)$ (lorsque $n \geqslant 2$).

Lemme 8 *Pour tout entier strictement positif n, on a l'égalité :*

$$\sum_{d|n} \phi(d) = n.$$

Preuve : Un élément d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$ engendre un sous-groupe cyclique de $(\mathbb{Z}/n\mathbb{Z}, +)$, qui lui-même contient $\phi(d)$ générateurs, i.e. éléments d'ordre d. Pour tout $d|n$, il y a exactement un sous-groupe cyclique d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$, il y a donc exactement $\phi(d)$ éléments d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$. ∎

Preuve du théorème 7: Soit $n = |K^*|$. Le phénomène qui implique le théorème est qu'un polynôme de $K[X]$ a un nombre de racines majoré par son degré. En particulier le nombre d'éléments de K^* qui vérifient

$$x^d = 1 \tag{4}$$

est au plus d. Appelons N_d l'ensemble des $x \in K^*$ d'ordre (multiplicatif) d dans K^*. Soit $N_d = \emptyset$, soit N_d contient au moins un élément, disons x. Mais alors x engendre un sous-groupe cyclique de K^* qui contient donc d éléments, chacun desquels vérifie (4). Ce sous-groupe de K^* contient donc $\phi(d)$ générateurs, et on en déduit

$$|N_d| = \phi(d)$$

puisqu'il n'y a plus de place dans K pour d'autre solution de (4). On vient de montrer que $|N_d| = 0$ ou $|N_d| = \phi(d)$. Comme $(N_d)_{d|n}$ est une partition de K^*, d'après le lemme 8 on en déduit $|N_d| = \phi(d)$ pour tout d. En particulier $N_n \neq \emptyset$, i.e. il existe un générateur de K^*. ∎

Si K est un corps fini de caractéristique p, et si α est un élément primitif de K, on a clairement $K = \mathbb{F}_p(\alpha)$. le théorème 7 implique donc :

Proposition 9 *Tout corps fini de caractéristique p est une extension algébrique simple de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

D'après la proposition 6 on a donc répondu par l'affirmative à la question 1 de la section 2.1.

Polynômes primitifs.

Soit P un polynôme irréductible sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, et formons le corps $K = \mathbb{F}_p[X]/(P)$. Renommons α l'élément X modulo P de K, de telle sorte que l'on a $K = \mathbb{F}_p(\alpha)$. L'élément α de K peut être ou ne pas être un élément primitif de K. Qu'il le soit ou non dépend exclusivement du polynôme $P(X)$. On dit que le polynôme irréductible $P(X)$ est un *polynôme primitif* sur $\mathbb{F}_p$ si l'élément associé α est un élément primitif de $\mathbb{F}_p(\alpha)$. Attention, certains polynômes irréductibles sont primitifs, d'autre non.

– Exercice 9. *Montrer que les trois polynômes irréductibles de degré 4 de* $\mathbb{F}_2[X]$ *sont* $X^4 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^3 + X^2 + X + 1$. *Exactement un de ces trois polynômes n'est pas primitif. Trouver lequel.*

Points essentiels à retenir

- Si L/K est une extension, L est un K-espace vectoriel, $[L : K] = \dim_K L$
- la formule des degrés, $[M : K] = [M : L][L : K]$
- ce qu'est le polynôme minimal P_α d'un élément algébrique α, il est unitaire, irréductible.
- L'extension algébrique simple $K(\alpha)$ est isomorphe à $K[X]/(P_\alpha)$
- le groupe multiplicatif $(K^*, \times)$ du corps fini $(K, +, \times)$ est cyclique, un générateur de K^* est dit élément primitif de K.
- Si K est un corps fini, p sa caractéristique, et si α est un élément primitif de K, alors $K = \mathbb{F}_p(\alpha)$. Attention, $K = \mathbb{F}_p(\alpha)$ n'implique pas forcément que α soit un élément primitif de K.
- Faire la distinction entre un polynôme *irréductible* de $\mathbb{F}_p[X]$, et un polynôme *irréductible primitif* de $\mathbb{F}_p[X]$.

4 Unicité du corps à p^n éléments, le polynôme $X^q - X$

4.1 La question de l'unicité

Soit K un corps à q éléments. Comme tout élément du groupe multiplicatif de K a pour ordre un diviseur de $q - 1$, on en déduit que tout élément de K est une

racine de $X^q - X$. On a donc :

Proposition 10 *Soit K un corps à q éléments. On a la factorisation*

$$X^q - X = \prod_{\alpha \in K} (X - \alpha) \tag{5}$$

Soit $P(X)$ un polynôme irréductible dans $\mathbb{F}_p[X]$ et soit $n = \deg P$ son degré. Notons $q = p^n$. Nous avons vu qu'il existe un corps d'extension de $\mathbb{F}_p$ dans lequel $P(X)$ admet une racine α (notamment $\mathbb{F}_p[X]/(P)$) et que $\mathbb{F}_p(\alpha)$ est un corps à q éléments. On constate que α est une racine commune à $P(X)$ et $X^q - X$: les deux polynômes $P(X)$ et $X^q - X$ ont donc un pgcd non-trivial dans $\mathbb{F}_p(\alpha)[X]$ et aussi dans $\mathbb{F}_p[X]$ (le pgcd s'obtient par divisions euclidiennes). Comme $P(X)$ est irréductible sur $\mathbb{F}_p$ on en déduit :

Proposition 11 *Soit $P(X) \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n. Le polynôme $P(X)$ est un diviseur de $X^q - X$, où $q = p^n$.*

Pour montrer l'unicité, à isomorphisme près, du corps à q éléments, il suffit de mettre en évidence, pour tout polynôme irrécuctible $Q \in \mathbb{F}_p[X]$ de degré n, un isomorphisme entre $\mathbb{F}_p(\alpha)$ et $\mathbb{F}_p[X]/(Q)$. Or soit Q un tel polynôme : d'après les propositions 10 et 11, il doit exister un élément $\beta \in \mathbb{F}_q(\alpha)$ racine de $Q(X)$. Comme $Q(X)$ est irréductible, $Q(X)$ est le polynôme minimal de β sur $\mathbb{F}_p$. Donc $\mathbb{F}_p(\beta) \xrightarrow{\sim} \mathbb{F}_p[X]/(Q)$. Mais $\mathbb{F}_p(\beta) \subset \mathbb{F}_p(\alpha)$ et $|\mathbb{F}_p(\beta)| = q$ donc $\mathbb{F}_p(\beta) = \mathbb{F}_p(\alpha)$. On a bien l'isomorphisme annoncé. En d'autres termes nous avons montré :

Théorème 12 *Soit q le cardinal d'un corps fini. Toutes les structures de corps à q éléments sont isomorphes.*

– Exercice 10. *Vérifier que $X^4 + X + 1$ et $X^4 + X^3 + X^2 + X + 1$ sont des polynômes irréductibles sur $\mathbb{F}_2$. Expliciter l'isomorphisme entre $\mathbb{F}_2[X]/(X^4 + X + 1)$ et $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$.*

4.2 Description globale du corps à q éléments. Existence de polynômes irréductibles de tous degrés

Soit $q = p^n$. Nous ne sommes pas encore sûr qu'il existe un corps à q éléments, car nous ne savons pas (encore) s'il existe un polynôme irréductible de degré n sur $\mathbb{F}_p$. Nous allons le démontrer d'une manière indirecte en construisant le corps à q éléments d'une autre façon.

Commençons par le lemme suivant.

Lemme 13 *Soit K un corps de caractéristique p. pour tous $a, b \in K$ on a :*

$$(a+b)^p = a^p + b^p \qquad (a+b)^{p^i} = a^{p^i} + b^{p^i}.$$

Preuve : Constater que le coefficient binomial $\binom{p}{m}$ est divisible par p pour $m \neq 0, p$. Faire une récurrence sur i. ∎

Nous avons encore besoin du lemme technique suivant.

Proposition 14 *Soit $q = p^n$ soit K un corps d'extension de $\mathbb{F}_p$. Sur le corps K, le polynôme $X^q - X$ n'a pas de racine multiple.*

Preuve : soit α une racine de $X^q - X$ dans K. On a :

$$X^q - X = X^q - \alpha^q + \alpha - X = (X-\alpha)^q - (X - \alpha)$$

d'après le lemme 13. Donc

$$X^q - X = (X-\alpha)((X-\alpha)^{q-1} - 1).$$

Or $(X-\alpha)^{q-1} - 1$ n'admet clairement pas α comme racine. ∎

Considérons maintenant le polynôme $X^q - X$ dans $\mathbb{F}_p[X]$. Il existe un corps K dans lequel $X^q - X$ se factorise entièrement, c'est-à-dire dans lequel la décomposition de $X^q - X$ en produit de facteurs irréductibles est constitué uniquement de monômes. Ceci n'est pas particulier à $X^q - X$ mais est vrai de tout polynôme. Pour obtenir un tel corps, il suffit de construire une suite d'extensions successives L de $\mathbb{F}_p$. Si $X^q - X$ ne se décompose pas entièrement sur L, prendre un facteur irréductible P de $X^q - X$ et remplacer L par le corps d'extension $L[X]/(P)$.

Soit donc un corps d'extension K de $\mathbb{F}_p$ dans lequel $X^q - X$ se factorise entièrement. On déduit de la proposition 14 que $X^q - X$ admet exactement q racines dans K. Soit R cet ensemble de racines. Le lemme 13 montre que R est stable par addition. Il est immédiat de vérifier que R est stable par multiplication. On en déduit que R est un corps, qui contient donc exactement q éléments. Les propositions 6 et 9 montrent donc :

Proposition 15 *Pour tout p premier, il existe des polynômes irréductibles sur $\mathbb{F}_p$ de tous degrés.*

Il est donc justifié de parler *du* corps fini à q éléments, pour tout q de la forme $q = p^n$, p premier. On le notera dorénavant $\mathbb{F}_q$. Concluons cette section par la remarque et définition suivantes : nous avons vu (Lemme 13) que l'application $\sigma : x \mapsto x^p$ est une application *linéaire* sur $\mathbb{F}_q$. Elle est appelée *automorphisme de Frobenius* de $\mathbb{F}_q$.

4.3 Factorisation de $X^q - X$ sur $\mathbb{F}_p$

Soit $q = p^n$. Nous avons vu (proposition 11) que *tous* les polynômes irréductibles de degré n sont des facteurs irréductibles de $X^q - X$ dans $\mathbb{F}_p[X]$. Quels sont les autres ?

Lemme 16 *Soit p un nombre premier. L'entier $p^d - 1$ divise $p^n - 1$ si et seulement si d divise n. Le polynôme $X^d - 1$ divise $X^n - 1$ si et seulement si d divise n.*

Preuve : Écrivons la division euclidienne de n par d, $n = qd + r$. On a :

$$p^n - 1 = (p^d)^q p^r - 1 = p^r - 1 \bmod (p^d - 1)$$

ce qui démontre la première affirmation. La deuxième se prouve de manière analogue. ∎

On peut maintenant énoncer :

Théorème 17 *Sur $\mathbb{F}_p[X]$, la décomposition en facteurs irréductibles de $X^q - X$, $q = p^n$, est :*

$$X^q - X = \prod_{\substack{P \text{ irréductible} \\ \deg P \mid n}} P(X). \tag{6}$$

Preuve : Pour tout diviseur d de n, le lemme 16 nous dit que $X^{p^d} - X$ divise $X^q - X$. Les polynômes irréductibles de $\mathbb{F}_p[X]$ de degré d, qui sont des diviseurs de $X^{p^d} - X$ d'après la proposition 11, sont donc des diviseurs de $X^q - X$. Le terme de droite de (6) divise donc le terme de gauche. Il reste à montrer qu'il n'y a pas d'autre facteur irréductible sur $\mathbb{F}_p$ de $X^q - X$. Soit donc $P(X)$ un polynôme irréductible de $\mathbb{F}_p[X]$, diviseur de $X^q - X$. Comme $X^q - X$ a toutes ses racines dans $\mathbb{F}_q$, $P(X)$ admet une racine α dans $\mathbb{F}_q$ et c'est même, à une constante multiplicative près, le polynôme minimal de α. On a donc $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg P$ (proposition 6). D'après la formule de multiplicativité des degrés (proposition 4) on a donc $n = [\mathbb{F}_q : \mathbb{F}_p(\alpha)] \deg P$ et $\deg P$ est un diviseur de n. ∎

– Exercice 11. *Montrer que $\mathbb{F}_q$ admet des sous-corps isomorphes à $\mathbb{F}_{p^d}$ pour tout d diviseur de n, et que ce sont les seuls sous-corps de $\mathbb{F}_q$.*

Points essentiels à retenir

- Pour tout p premier et tout entier strictement positif n, il existe, à isomorphisme près, un unique corps fini $\mathbb{F}_q$ à q éléments.
- Le corps $\mathbb{F}_q$ est constitué de l'ensemble des racines de $X^q - X$. En particulier on en déduit une méthode pour prouver l'appartenance à $\mathbb{F}_q$: élever le candidat à la puissance q et regarder s'il est inchangé.
- Les facteurs irréductibles sur $\mathbb{F}_p$ de $X^q - X$ sont les polynômes irréductibles de $\mathbb{F}_p[X]$ de degré n, ainsi que les polynômes irréductibles de degré d, pour tout diviseur d de n.
- Dans $\mathbb{F}_p[X]$ on a $X^d - 1 \mid X^n - 1$ si et seulement si $d \mid n$.
- Sur $\mathbb{F}_q$, on a $(a+b)^p = a^p + b^p$. L'application $x \mapsto x^p$ est un automorphisme de corps, c'est l'automorphisme de Frobenius.

5 Conjugaison

5.1 Racines conjuguées

Soit un polynôme $P(X)$ de degré n, irréductible dans $\mathbb{F}_p[X]$. Nous savons maintenant que $P(X)$ se factorise entièrement, i.e. a n racines, dans $\mathbb{F}_q$ où $q = p^n$. Soit α une racine de $P(X)$. La question qui nous préoccupe maintenant est : quelles sont les *autres* racines de P dans $\mathbb{F}_q$, et s'expriment-elles en fonction de α ?

Proposition 18 *Soit α un élément de $\mathbb{F}_q$, $q = p^n$. Soit e le plus petit entier tel que $\alpha^{p^e} = \alpha$. Soit $\Pi(X)$ le polynôme défini par :*

$$\Pi(X) = \prod_{i=0}^{e-1} (X - \alpha^{p^i}).$$

Alors tous les coefficients de $\Pi(X)$ sont dans $\mathbb{F}_p$.

Preuve : Commençons par constater que e est bien défini et $e \leqslant n$ puisque $\alpha^q = \alpha$. Rappelons qu'un élément a de $\mathbb{F}_q$ appartient à $\mathbb{F}_p$ si et seulement si $a^p = a$. Pour montrer la proposition il suffit donc, d'après le lemme 13 de montrer

que $\Pi(X)^p = \Pi(X^p)$. Or on a :

$$\Pi(X)^p = \prod_{i=0}^{e-1}(X^p - \alpha^{p^{i+1}}).$$

Mais comme $\alpha^{p^e} = \alpha$, les ensembles (α^{p^i}) sont les mêmes lorsque i décrit l'ensemble $\{0, \dots e-1\}$ ou l'ensemble $\{1, \dots e\}$. Donc $\Pi(X)^p = \Pi(X^p)$. ∎

Soit maintenant $P(X)$ un polynôme irréductible sur $\mathbb{F}_p$ de degré n, et α une de ses racines dans $\mathbb{F}_q$. La proposition 18 met en évidence un polynôme $\Pi(X)$ de degré au plus n, de $\mathbb{F}_p[X]$, dont α est aussi une racine. On en déduit que :

1. $\deg \Pi = n$,
2. à multiplication par une constante (de $\mathbb{F}_p$) près, $\Pi(X)$ et $P(X)$ sont égaux.

Nous avons donc démontré le théorème suivant.

Théorème 19 *Soit $P(x) \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n. Soit α une racine de $P(X)$ dans $\mathbb{F}_q$, $q = p^n$. Alors l'ensemble des racines de $P(X)$ est l'ensemble :*

$$\{\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}\}.$$

– Exercice 12.

1. *Montrer que si α est un élément primitif de $\mathbb{F}_q$, alors α^p l'est aussi.*
2. *Combien y a-t-il de polynômes primitifs de degré n ?*

5.2 Trace

Théorème 20 (et définition) *L'application suivante, définie sur $\mathbb{F}_q$, $q = p^n$,*

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

Vérifie les propriétés :

1. *Pour tout $x \in \mathbb{F}_q$, $\mathrm{Tr}(x) \in \mathbb{F}_p$.*
2. *$x \mapsto \mathrm{Tr}(x)$ est une application* linéaire, *au sens des $\mathbb{F}_p$-espaces vectoriels, de $\mathbb{F}_q$ dans $\mathbb{F}_p$.*
3. *$\mathrm{Tr}(x^p) = \mathrm{Tr}(x)$ pour tout $x \in \mathbb{F}_q$.*
4. *Pour tout $a \in \mathbb{F}_p$ il existe exactement q/p éléments x de $\mathbb{F}_q$ tels que $\mathrm{Tr}(x) = a$.*

Cette application est appelée trace *de $\mathbb{F}_q$ sur $\mathbb{F}_p$.*

Preuve : On remarque que $\mathrm{Tr}(x)^p = \mathrm{Tr}(x^p) = x^p + x^{p^2} + \cdots + x^{p^{n-1}} + x^q$. Mais comme $x^q = x$ pour tout $x \in \mathbb{F}_q$, on obtient que $\mathrm{Tr}(x)^p = \mathrm{Tr}(x)$, ce qui prouve simultanément que $\mathrm{Tr}(x) \in \mathbb{F}_p$ et $\mathrm{Tr}(x) = \mathrm{Tr}(x^p)$. La linéarité de la trace n'est autre que le lemme 13. Enfin, pour démontrer le point 4, remarquons que le polynôme

$$X + X^p + \cdots + X^{q/p} - a$$

a au plus q/p racines. Mais $\mathbb{F}_q$ tout entier est réunion des p parties

$$\{x \in \mathbb{F}_q \, , \mathrm{Tr}(x) = a\}.$$

Donc, pour que leur réunion soit constituée d'exactement q éléments, chacune de ces parties doit comporter exactement q/p éléments. ∎

Points essentiels à retenir

- Les racines d'un polynôme irréductible $P(X)$ de $\mathbb{F}_p[X]$ sont simples et consistent en un ensemble de la forme

$$\alpha, \alpha^p, \ldots, \alpha^{p^{\deg P - 1}}$$

- ce qu'est l'application trace de $\mathbb{F}_q$ dans $\mathbb{F}_p$ ainsi que ses propriétés élémentaires.
- arguments récurrents dans les démonstrations :
  - L'ensemble E n'a pas plus de e éléments car il est constitué de racines d'un polynôme de degré e.
  - L'élément x de $\mathbb{F}_q$, $q = p^n$, est en fait dans $\mathbb{F}_p$ car $x^p = x$.

Deuxième partie

Applications des corps finis

6 Suites engendrées par des récurrences linéaires, m-séquences

6.1 Définition et propriétés des m-séquences

On s'intéresse aux suites $(a_i)_{1\leqslant i<\infty}$ à éléments dans un corps fini $\mathbb{F}_q$, et engendrées par une récurrence linéaire du type :

$$a_i = a_{i-1}h_{m-1} + \cdots + a_{i-m+1}h_1 + a_{i-m}h_0 \tag{7}$$

Pour simplifier l'exposé, et parce que ce sont les séquences les plus utilisées, on se limitera au cas du corps à deux éléments $\mathbb{F}_2$. La généralisation au cas q quelconque ne pose pas de difficulté particulière.

Examinons un exemple : prenons $m = 4$ registres, $h_0 = h_1 = 1$, $h_2 = h_3 = 0$. La récurrence (7) est donc $a_i = a_{i-3} + a_{i-4}$. Choisissons $a_0 = a_1 = a_2 = a_3 = 1$ et construisons les premiers termes de la suite. On obtient :

$$\boxed{1111}00010011010\boxed{1111}\cdots$$

On remarque que le quadruplet $(a_i, a_{i+1}, a_{i+2}, a_{i+3})$ ne redevient identique au quadruplet initial (a_0, a_1, a_2, a_3) que pour $i = 15$. La suite (a_i) est donc périodique de période 15. On constate aussi que cette période est maximale, car le quadruplet $(a_i, a_{i+1}, a_{i+2}, a_{i+3})$ a pris toutes les valeurs non nulles possibles avant de retrouver sa valeur initiale. Chaque fois que ce phénomène se produit, on parle de *m-séquence.*

Définition 21 *On appelle* m-séquence *toute suite engendrée par une récurrence linéaire* (7) *de degré m et de période maximale $P = 2^m - 1$.*

Comme nous venons de le voir, cette définition équivaut à dire que l'ensemble des m-uples $(a_{i+1}, a_{i+2}, \ldots, a_{i+m})$ prend toutes les valeurs non nulles possibles.

On en déduit :

Proposition 22 *Soit (a_i) une m-séquence de degré m engendrée par une récurrence de type* (7)*. Toute autre suite non nulle engendrée par la récurrence* (7) *est une décalée (a_{i+k}) de (a_i). De plus, la somme de deux décalées différentes quelconques de (a_i) est encore une suite décalée de (a_i).*

Preuve : comme chaque m-uple non nul apparaît dans (a_i), n'importe lequel des $2^m - 1$ choix de conditions initiales $(a_0, \ldots, a_{m-1})$ engendre une suite décalée de (a_i). Par ailleurs, l'ensemble des solutions de la récurrence (7) est un espace vectoriel de dimension m : si l'on enlève la suite nulle, il reste donc $2^m - 1$ suites solutions de (7). Elles coïncident donc avec l'ensemble des décalées d'une même solution non nulle de (7). ∎

Une m-séquence possède de très bonnes qualités pseudo-aléatoires. La raison essentielle en est la proposition suivante, conséquence directe de ce que le m-uple $(a_{i+1}, a_{i+2}, \ldots, a_{i+m})$ prenne toutes les valeurs non nulles possibles.

Proposition 23 *Soit $1 \leqslant k \leqslant m$. Le k-uple $(a_{i+1}, a_{i+2}, \ldots a_{i+k})$ décrit chaque k-uple non nul exactement 2^{m-k} fois lorsque i varie de 1 à $P = 2^m - 1$; le k-uple nul quant à lui est décrit $2^{m-k} - 1$ fois.*

6.2 Structure algébrique des m-séquences

Comment faut-il choisir les coefficients h_j de la réccurence (7) pour obtenir une m-séquence ? La clé consiste à chercher des solutions de la récurrence linéaire (7) dans une *extension* de $\mathbb{F}_2$. Cherchons une suite géométrique solution de (7), c'est à dire une suite (a_i) où $a_i = \alpha^i$, pour un certain $\alpha \neq 0$. La récurrence linéaire se réécrit alors :

$$\alpha^i + h_{m-1}\alpha^{i-1} + \cdots + \alpha^{i-m}h_0 = 0$$

pour tout $i \geqslant m$, ce qui en simplifiant par la puissance de α adéquate se réduit à la condition

$$\alpha^m + h_{m-1}\alpha^{m-1} + \cdots + h_0 = 0.$$

Introduisons donc le polynôme

$$h(X) = X^m + h_{m-1}X^{m-1} + \ldots + h_0.$$

Ce polynôme est parfois appelé *polynôme de rétroaction* (feedback polynomial) de la suite. la suite géométrique (α^i) est donc solution de la récurrence linéaire (7) si et seulement si α est une racine du polynôme $h(X)$ dans une extension de $\mathbb{F}_2$.

Supposons que les coefficients h_j soient choisis de telle sorte que le polynôme de rétroaction $h(X)$ soit irréductible sur $\mathbb{F}_2$. Dans ce cas il existe une racine α de $h(X)$ dans $\mathbb{F}_q$ où $q = 2^m$. Nous savons maintenant que les autres racines de $h(X)$ sont $\alpha^2, \alpha^4 \ldots$. Nous avons donc m solutions de la récurrences linéaire (7) qui sont les suites

$$([\alpha^{2^k}]^i)_{i \geqslant 0}$$

pour $k = 0, 1, \ldots 2^{m-1}$. Ces suites sont à valeurs dans $\mathbb{F}_q$, mais si nous les additionnons nous obtenons la suite (y_i) :

$$y_i = \alpha^i + \alpha^{2i} + \alpha^{2^2 i} + \cdots + \alpha^{2^{m-1} i}$$

qui elle est à valeurs dans $\mathbb{F}_2$. En effet, on a :

$$y_i = \mathrm{Tr}(\alpha^i).$$

Dans le cas où $h(X)$ est non seulement irréductible mais primitif, le point 4 du théorème 20 assure que la suite a_i n'est pas identiquement nulle et nous obtenons une solution *binaire* non triviale de (7). Quelle est sa période ?

Théorème 24 *Si le polynôme $h(X)$ est irréductible primitif, alors toute suite (a_i) solution non nulle de* (7) *est une m-séquence.*

Preuve : Soit π la période de (y_i), c'est-à-dire le plus petit entier strictement positif tel que $y_{i+\pi} = y_i$ pour tout $i \geqslant 0$. Nous avons donc, pour tout $i \geqslant 0$,

$$\mathrm{Tr}(\alpha^{i+\pi}) = \mathrm{Tr}(\alpha^i)$$

soit $\mathrm{Tr}(\alpha^{i+\pi} + \alpha^i) = \mathrm{Tr}(\alpha^i(\alpha^\pi + 1)) = 0$. Mais puisque α est primitif, les puissances de α décrivent tous les élements non nuls de $\mathbb{F}_q$, nous en déduisons donc que

$$\mathrm{Tr}(x(\alpha^\pi + 1)) = 0$$

pour tout $x \in \mathbb{F}_q$. Or, si $\alpha^i + 1 \neq 0$, l'application $x \mapsto x(\alpha^\pi + 1)$ est une bijection de $\mathbb{F}_q$ dans $\mathbb{F}_q$ et donc $x(\alpha^\pi + 1)$ décrirait $\mathbb{F}_q$ tout entier : nous aurions donc que tous les élements de $\mathbb{F}_q$ seraient de trace nulle, mais cela contredit le point 4 du théorème 20. Nous en concluons donc que $\alpha^\pi + 1 = 0$, c'est-à-dire que la période de la suite y_i est égale à l'ordre de α, soit $\pi = 2^m - 1$. La suite (y_i) est donc une m-séquence. D'après la proposition 22 nous avons que toute solution non nulle de la récurrence (7) est une décalée de (y_i) et est une m-séquence. ∎

Nous avons une réciproque. On peut énoncer :

Théorème 25 *La récurrence linéaire* (7) *admet une m-séquence comme solution si et seulement si son polynôme de rétroaction $h(X)$ est irréductible et primitif.*

Pour démontrer le théorème 25 nous avons besoin d'introduire un peu de notations. Soit n un entier et soit

$$\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$$

un n-uplet binaire. On lui associe la suite périodique $(a_i)_{i\geqslant 0}$, de période n, qui est obtenue en répétant le motif $\mathbf{a}$. En d'autres termes on pose $a_n = a_0, a_n{+}1 = a_1, \ldots$ et $a_{i+n} = a_i$ pour tout $i \geqslant 0$. En reformulant légèrement (7) on peut dire que la suite (a_i) est solution de la récurrence linéaire si et seulement si, pour tout $i \geqslant 0$,

$$a_i h_0 + a_{i+1} h_1 + \cdots + a_{i+m-1} h_{m-1} + a_{i+m} h_m = 0, \tag{8}$$

où on a posé $h_m = 1$. Introduisant maintenant le n-uple binaire $\overline{\mathbf{a}} = \mathbf{b} = (b_0, b_1, \ldots b_{n-1})$ où on a posé $b_0 = a_{n-1}, b_1 = a_{n-2}, \ldots, b_{n-1} = a_0$. En d'autres termes $\overline{\mathbf{a}}$ est le n-uple $\mathbf{a}$ lu de droite à gauche plutôt que de gauche à droite. Maintenant on créé la suite (b_i) à partir du n-uple $\mathbf{b}$ comme précédemment, en posant $b_{n+i} = b_i$ pour tout $i \geqslant 0$, i.e. en répétant à l'infini le motif $\mathbf{b}$. L'équation (8) se réécrit :

$$b_i h_0 + b_{i-1} h_1 + \cdots + b_{i-m+1} h_{m-1} + b_{i-m} h_m = 0 \quad \text{pour tout } i \geqslant m. \tag{9}$$

Définissons maintenant le polynôme de degré $n-1$,

$$b(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}.$$

Nous avons

Proposition 26 $b(X)h(X) = 0 \bmod (X^n + 1)$.

Preuve : Le produit $b(X)h(X)$ dans $\mathbb{F}_2[X]$ est un polynôme de degré $n+m-1$. Le réduire modulo X^n+1 consiste simplement à remplacer tous les termes X^j où $j \geqslant n$ par X^{j-n}. Une fois cette opération faite, on obtient que le terme constant de $b(X)h(X)$ dans $\mathbb{F}_2[X]/(X^n+1)$ vaut

$$b_0 h_0 + b_{n-1} h_1 + \cdots b_{n-m} h_m.$$

Notons que l'on a $b_0 = b_n$, de telle sorte que l'expression ci-dessus n'est autre que celle de (9) pour $i = n$. De même le terme de degré 1 de $b(X)h(X)$ modulo (X^n+1) vaut l'expression de (9) pour $i = n+1$, et plus généralement, tous les coefficients de $b(X)h(X)$ réduit modulo (X^n+1) sont de la forme (9) et valent donc 0. ∎

Inversement, soit $\mathbf{b} = (b_0, b_1, \ldots b_{n-1})$ un n-uplet binaire et soit $b(X) = b_0 + bX + \cdots b_{n-1}X^{n-1}$. Soit (b_i) la suite périodique associée à $\mathbf{b}$ et soit $\mathbf{a}$ l'image miroir de $\mathbf{b}$, c'est-à-dire le n-uple tel que $\overline{\mathbf{a}} = \mathbf{b}$. Soit enfin (a_i) la suite périodique associée. L'égalité $b(X)h(X) = 0 \bmod (X^n+1)$ se traduit par des égalités du type (9) pour n valeurs successives de i. La périodicité assure donc (9) est satisfaite pour tout i. L'équivalence entre (9), (8) et (7) permet donc d'énoncer :

Proposition 27 *Si $b(X)h(X) = 0 \bmod (X^n+1)$, alors la suite (a_i), périodique de période n, est une solution de la récurrence* (7).

Nous sommes maintenant en mesure de démontrer le théorème 25.

Preuve du Théorème 25: Supposons que la récurrence (7) admette une m-séquence (a_i) comme solution. Quitte à remplacer la suite (a_i) par une suite décalée, nous pouvons supposer que ses $m-1$ premiers symboles sont des zéros. Le vecteur $\mathbf{b}$ correspondant se termine donc par $m-1$ zéros. Le polynôme $b(X)$ associé est donc de degré $n-1-(m-1)=n-m$, (où $n=2^m-1$). Le polynôme $b(X)h(X)$ est donc de degré n. Et puisque la proposition 26 nous dit que $b(X)h(X)$ est un multiple de X^n+1, la seule possibilité est donc qu'on ait $b(X)h(X)=X^n+1$ dans $\mathbb{F}_2[X]$. On a donc que $X^{2^m-1}+1$ est un multiple du polynôme de rétroaction $h(X)$ dans $\mathbb{F}_2[X]$. Par ailleurs la proposition 27 implique que, pour $1 \leqslant n < 2^m-1$, le polynôme X^n+1 ne peut pas être un multiple de $h(X)$ (sinon il existerait une solution non nulle de la récurrence de période strictement plus petite que 2^m-1, mais ceci n'est pas possible car d'après la proposition 22 toutes les solutions non nulles de la récurrence (7) ont comme plus petite période 2^m-1).

Nous avons donc montré que dans le groupe multiplicatif de $\mathbb{F}_2[X]/h(X)$, l'ordre de X est 2^m-1. Ceci implique qu'il y a 2^m-1 éléments dans le groupe multiplicatif, et donc que $\mathbb{F}_2[X]/h(X)$ est un corps, autrement dit que $h(X)$ est irréductible, et que $h(X)$ est un bien un polynôme primitif. ∎

Expression algébrique d'une m-séquence. on déduit en particulier de l'analyse ci-dessus que toute m-séquence (a_i) associée à (7) peut toujours s'écrire :

$$a_i = \mathrm{Tr}(\alpha^{i+k})$$

où α est une racine du polynôme de rétroaction $h(X)$.

Enfin, nous avons la généralisation suivante du théorème 24, à des polynômes de rétroaction irréductibles, mais non forcément primitifs.

Théorème 28 *Supposons le polynôme de rétroaction $h(X)$ de la récurrence linéaire* (7) *irréductible de degré m. Soit e l'ordre de X dans $\mathbb{F}_2[X]/h(X)$. Alors toute solution non nulle (a_i) de la récurrence* (7) *est périodique de période e, et admet la représentation :*

$$a_i = \mathrm{Tr}(x\alpha^i) \quad \textit{pour tout } i \geqslant 0$$

où α est une racine de $h(X)$ dans $\mathbb{F}_{2^m}$ et où x est un élément non nul de $\mathbb{F}_{2^m}$.

Preuve : Soit $x \neq 0$ dans $\mathbb{F}_{2^m}$ et soit α une racine de $h(X)$ dans $\mathbb{F}_{2^m}$. Considérons la suite (a_i) où $a_i = \mathrm{Tr}(x\alpha^i)$, qui est clairement une solution de la récurrence (7). Soit π une période de la suite. On a donc $a_{i+\pi} = a_i$ pour tout $i \geqslant 0$, soit

$$\mathrm{Tr}(x\alpha^{i+\pi} + x\alpha^i) = \mathrm{Tr}(x(\alpha^\pi+1)\alpha^i) = 0$$

pour tout $i \geqslant 0$. Par linéarité de la trace on obtient donc que pour tout polynôme $P(X) \in \mathbb{F}_2[X]$,

$$\mathrm{Tr}(x(\alpha^\pi + 1)P(\alpha)) = 0$$

puisque $P(\alpha)$ n'est autre qu'une somme de puissances de α. Mais tout élément de $\mathbb{F}_{2^m}$ s'écrit comme $P(\alpha)$, $P(X) \in \mathbb{F}_2[X]$: en déduit donc que $\alpha^\pi + 1 = 0$, sinon tout élément de $\mathbb{F}_{2^m}$ serait de trace nulle, ce qui contredirait le Théorème 20. La période π est donc un multiple de e qui est donc la plus petite période de (a_i).

Maintenant considérons deux suites $(\mathrm{Tr}(x\alpha^i))$ et $(\mathrm{Tr}(y\alpha^i))$. Si l'une est égale à une décalée de l'autre, on doit avoir $\mathrm{Tr}(x\alpha^i) = \mathrm{Tr}(y\alpha^{i+j})$ pour tout i, pour un certain décalage j. On en déduit $\mathrm{Tr}((x + y\alpha^j)\alpha^i) = 0$ pour tout i, et par le même argument que précédemment, on en déduit $\mathrm{Tr}((x + y\alpha^j)P(\alpha)) = 0$ pour n'importe quel polynôme $P(X) \in \mathbb{F}_2[X]$. On en déduit de nouveau que ceci ne peut se produire que si $x + y\alpha^j = 0$. Par conséquent, si x décrit un système de représentants du groupe quotient $\mathbb{F}_{2^m}^*/H$, où H est le groupe multiplicatif d'ordre e engendré par α, nous obtenons $(2^m - 1)/e$ suites de la forme $(\mathrm{Tr}(x\alpha^i))$ dont aucune n'est égale à la décalée d'une autre. Si maintenant nous considérons toutes les décalées de ces suites, nous obtenons $2^m - 1$ solutions non nulles distinctes de la récurrence (7), qui avec la suite nulle nous donnent donc toutes les solutions de la récurrence linéaire. Il n'y a donc pas d'autre suite solution que celles que nous avons considérées. ∎

7 Factorisation de $X^n - 1$ et codes cycliques

7.1 Factorisation de $X^n - 1$

On s'intéresse ici à la factorisation du polynôme $X^n - 1$ dans $\mathbb{F}_p[X]$. On supposera p premier avec n.

Quitte à prendre des extensions successives de $\mathbb{F}_p$, par un argument similaire à celui de la discussion précédant la proposition 15 on peut considérer une extension $\mathbb{F}_q$ de $\mathbb{F}_p$ dans laquelle $X^n - 1$ se factorise entièrement. On peut être plus explicite sur le degré de cette extension.

Comme p est premier avec n, p est inversible modulo n et il existe m tel que $p^m = 1 \bmod n$. Soit $q = p^m$ et considérons l'extension $\mathbb{F}_q$ de $\mathbb{F}_p$. Soit α un élément primitif de $\mathbb{F}_q$, i.e. d'ordre $p^m - 1$. Soit $\zeta = \alpha^{(q-1)/n}$. On constate que les éléments

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$$

sont distincts et qu'ils constituent donc l'ensemble des racines de $X^n - 1$ dans $\mathbb{F}_q$.

Souvenons-nous que l'ensemble des racines d'un polynôme à coefficients dans $\mathbb{F}_p$ est stable par l'automorphisme de Frobenius (cf. section 5.1). Par conséquent, un

facteur $\mathbb{F}_p$-irréductible de degré k de X^n-1 est le polynome minimal d'un certain ζ^i et l'ensemble de ses racines dans $\mathbb{F}_q$ est de la forme

$$\{\zeta^i, \zeta^{ip}, \zeta^{ip^2}, \ldots, \zeta^{ip^{k-1}}\}$$

où $p^k i = i \bmod n$. On constate donc qu'à chaque facteur irréductible de $X^n - 1$ est associée, par passage aux exposants de l'ensemble de ses racines, un ensemble d'entiers modulo n d'une forme très particulière appelée *classe cyclotomique*. Plus précisément :

Définition 29 *On appelle* classe cyclotomique p-aire modulo n *de l'entier i, l'ensemble des entiers modulo n de la forme ip^j.*

Il y a une correspondance bijective entre facteurs $\mathbb{F}_p$-irréductibles de $X^n - 1$ et classes cyclotomiques p-aires modulo n. En particulier le nombre de facteurs irréductibles de $X^n - 1$ égale le nombre de classes cyclotomiques. Le degré d'un facteur irréductible égale le cardinal de la classe cyclotomique associée.

Exemple : soit $p = 2$ et $n = 21$. L'ordre de 2 dans $(\mathbb{Z}/21\mathbb{Z})^*$ est 6. L'ensemble des racines de $X^{21} - 1$ se trouve donc dans $\mathbb{F}_{64}$. Les classes cyclotomiques binaires modulo 21 sont :

$$\{0\}$$
$$\{1, 2, 4, 8, 16, 11\}$$
$$\{3, 6, 12\}$$
$$\{5, 10, 20, 19, 17, 13\}$$
$$\{7, 14\}$$
$$\{9, 18, 15\}.$$

La décomposition en facteurs irréductibles dans $\mathbb{F}_2[X]$ de $X^{21} - 1$ comporte donc un facteur de degré 1, un facteur de degré 2, deux facteurs de degré 3, et deux facteurs de degré 6.

– Exercice 13. *Démontrer que le polynôme $1+X+X^2+\cdots+X^{10}$ est irréductible sur $\mathbb{F}_2$. (Remarquer que c'est un diviseur de $X^{11} - 1$).*

– Exercice 14. *S'aider de la liste des classes cyclotomiques binaires modulo 21 ci-dessus pour trouver la factorisation dans $\mathbb{F}_2[X]$ de $X^{21} - 1$. On pourra remarquer que $X^{21} - 1 = (X^3)^7 - 1$.*

Points essentiels à retenir

- On trouve des racines du polynôme X^n-1 de $\mathbb{F}_p[X]$ dans l'extension $\mathbb{F}_{p^m}$ où $p^m = 1 \mod n$. Dans cette extension $X^n - 1$ se factorise entièrement et toutes ses racines sont des puissances d'une même racine ζ.

- Ce que sont les classes cyclotomiques p-aires modulo n.
- Les classes cyclotomiques sont en correspondance avec les facteurs irréductibles de $X^n - 1$ dans $\mathbb{F}_p[X]$. Le nombre d'éléments dans une classe est le degré du polynôme irréductible correspondant.

7.2 Codes cycliques

Un *code* de longueur n est une partie de $\mathbb{F}_q^n$. Un code *linéaire* C de longueur n sur le corps fini $\mathbb{F}_q$ est un sous-espace vectoriel de $\mathbb{F}_q^n$. Par défaut, un code sera supposé linéaire. Lorsque $q = 2$ on parle de code *binaire*, sinon de code q-aire.

Notons k la dimension, en tant que $\mathbb{F}_q$-espace vectoriel, d'un code C. Une *matrice génératrice* de C est une matrice $k \times n$ à éléments dans $\mathbb{F}_q$, dont les *lignes* constituent une base de C. Le code C contient q^k mots de code.

Définition 30 *On appelle* code cyclique q-aire de longueur n *tout $\mathbb{F}_q$-sous-espace vectoriel C de $\mathbb{F}_q^n$ stable par décalage circulaire, c'est-à-dire tel que :*

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$$

Il est commode d'identifier les vecteurs de $\mathbb{F}_q^n$ avec l'ensemble des polynômes de $\mathbb{F}_q[X]$ de degré inférieur ou égal à $n-1$ par la correspondance

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}.$$

L'ensemble des polynômes de degré $\leqslant n-1$ est lui-même un système de représentants de l'anneau quotient $A = \mathbb{F}_q[X]/(X^n - 1)$. L'intérêt de cette identification est que le décalage circulaire est exactement la multiplication par X dans l'anneau A. Ceci nous permet d'énoncer :

Proposition 31 *Les codes cycliques q-aires de longueur n sont les idéaux de l'anneau $A = \mathbb{F}_q[X]/(X^n - 1)$.*

Définition 32 *On appelle* polynôme générateur *du code cyclique $C \subset \mathbb{F}_q^n$ le polynôme unitaire non nul de plus petit degré représentant un élément de C.*

Théorème 33 *Soit C un code cyclique q-aire de longueur n et soit $g(X)$ son polynôme générateur. Alors*

1. *Le code C est l'idéal $(g(X))$ de l'anneau A.*

2. *Le polynôme de $g(X)$ divise $X^n - 1$ dans $F_q[X]$ (et dans A).*
3. *La dimension de C, en tant que $\mathbb{F}_q$-espace vectoriel, égale $n - \deg g(X)$ et une base en est $(g(X), Xg(X), \ldots, X^{n-\deg g-1}g(X))$.*

Preuve :

1. Un quelconque élément de C peut être représenté par un polynôme $c(X)$ de degré $\leqslant n-1$. La division euclidienne de $c(X)$ par $g(x)$ s'écrit

$$c(X) = q(X)g(X) + r(X)$$

où $\deg r(X) < \deg g(X)$. Mais dans A on a $r(X) = c(X) - q(X)g(X)$ où $c(X)$ et $q(X)g(X)$ sont tous les deux dans C. On en déduit que $r(X) \in C$ et que $r(X) = 0$ par hypothèse de minimalité du degré de $g(X)$.
3. Comme $\deg c(X) \leqslant n-1$, on a $\deg q(X) \leqslant n-1-\deg g(X)$, ce qui montre que $c(X)$ est une combinaison linéaire des polynômes

$$g(X), Xg(X), \ldots, X^{n-\deg g-1}g(X).$$

Par ailleurs, comme toute combinaison linéaire de ces polynômes est de degré au plus $n-1$, ils forment un système libre dans A.
2. L'argument est similaire à celui du *1*. On écrit la division euclidienne dans $\mathbb{F}_q[X]$ de $X^n - 1$ par $g(X)$

$$X^n - 1 = q(X)g(X) + r(X)$$

où $\deg r(X) < \deg g(X)$. On en déduit donc que $r(X) = q(X)g(X) \bmod (X^n - 1)$, donc que $r(X) \in C$, ce qui implique $r(X) = 0$ par hypothèse de minimalité du degré de $g(X)$. ∎

Le *code dual* $C^\perp$ de C est l'ensemble des vecteurs $\mathbf{y} = (y_1 \ldots y_n)$ de $\mathbb{F}_q^n$ tels que, pour tout $\mathbf{x} = (x_1 \ldots x_n) \in C$,

$$\mathbf{x}.\mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n = 0 \quad \text{dans } \mathbb{F}_q.$$

Le code dual $C^\perp$ a pour dimension $\dim C^\perp = n - \dim C$. Le théorème suivant donne le polynôme générateur du code dual $C^\perp$ en fonction du polynôme générateur de C.

Théorème 34 *Soit $g(X)$ le polynôme générateur d'un code cyclique C de longueur n sur $\mathbb{F}_q$ et de dimension $k = n - \deg g(X)$. Soit $h(X) = h_0 + h_1X + \cdots + h_{k-1}X^{k-1} + X^k = (X^n - 1)/g(X)$. Alors le code dual $C^\perp$ de C a comme polynôme générateur le polynôme unitaire réciproque de $h(X)$*

$$h_0^{-1}(h_0X^k + h_1X^{k-1} + \cdots + h_{k-1}X + 1) = h_0^{-1}X^k h(1/X).$$

Preuve : Il suffit de montrer que le vecteur des coefficients du polynôme $1 + h_{k-1}X + \cdots + h_1X^{k-1} + h_0X^k$, soit le vecteur

$$\mathbf{h} = (1, h_{k-1}, \ldots, h_1, h_0, 0 \ldots 0)$$

est orthogonal à une base de C, soit les vecteurs associés aux polynômes

$$g(X), Xg(X), \ldots, X^{k-1}g(X).$$

Mais le vecteur associé au polynôme $g(X)$ est

$$\mathbf{g} = (g_0, g_1, \ldots, g_{n-k}, 0 \ldots 0).$$

On voit que $\mathbf{h}.\mathbf{g}$ est le coefficient de X^{k-1} du polynôme $h(X)g(X)$. De même, lorsque $\mathbf{x}$ décrit les vecteurs décalés de $\mathbf{g}$, les produits $\mathbf{h}.\mathbf{x}$ égalent les autres coefficients du produit $h(X)g(X)$ modulo $X^n - 1$. Mais ce produit est justement nul. ∎

Points essentiels à retenir

- Les mots d'un code cyclique de longueur n sur $\mathbb{F}_q$ se représentent comme des polynômes de degré $\leqslant n-1$ qui eux-mêmes représentent des éléments de l'anneau $\mathbb{F}_q[X]/(X^n - 1)$.
- Le polynôme générateur d'un code cyclique est le polynôme unitaire $g(X)$ de plus petit degré appartenant au code. Tout mot de code est un multiple de $g(X)$.
- Un code cyclique q-aire de longueur n est en particulier un espace vectoriel sur $\mathbb{F}_q$ de dimension $n - \deg g(X)$.
- Un polynôme $g(X) \in \mathbb{F}_q[X]$ est le polynôme générateur d'un code cyclique de longueur n si et seulement si c'est un diviseur de $X^n - 1$.
- Ce qu'est le code dual $C^\perp$ de C.
- si $g(X)$ est le polynôme générateur d'un code cyclique C, le polynôme générateur du code dual de C est le polynôme unitaire réciproque de $(X^n - 1)/g(X)$.

7.3 Distance, Codes de Hamming, codes BCH

La *distance de Hamming* $d(\mathbf{x}, \mathbf{y})$ entre deux vecteurs $\mathbf{x}$ et $\mathbf{y}$ de $\mathbb{F}_q^n$ est le nombre de coordonnées où les deux vecteurs diffèrent.

La *distance minimale* du code (non nécessairement cyclique, ni même linéaire) C est la plus petite distance non nulle entre deux mots du code C. C'est aussi, dans le cas des codes linéaires, le plus petit poids (nombre de coordonnées non nulles) d'un mot non nul de C.

Les *paramètres* $[n, k, d]$ d'un code C sont sa longueur, sa dimension (en tant que $\mathbb{F}_q$-espace vectoriel), sa distance minimale.

Si $t < d/2$, les boules de Hamming centrées sur les mots de code sont disjointes. Toute configuration de t erreurs peut être corrigée en cherchant le mot de code le plus proche (pour la distance de Hamming). C'est la notion de distance qui donne toute sa particularité à la théorie des codes correcteurs.

Nous avons vu que la dimension d'un code cyclique se déduit de manière immédiate de son polynôme générateur. Ce n'est pas le cas de sa distance minimale. C'est l'étude des *racines* du polynôme minimal, (le cas échéant dans un corps d'extension de $\mathbb{F}_q$), qui permet d'évaluer la distance minimale. Nous allons l'illustrer maintenant.

Dans cette section nous nous limitons à des codes binaires. Supposons d'abord que $g(X)$ soit un polynôme irréductible *primitif* de degré m dans $\mathbb{F}_2[X]$. Soit $n = 2^m - 1$. Comme $g(X)$ est un diviseur de $X^n - 1$, (Théorème 17) il engendre un code cyclique C de longueur n. Un tel code est appelé *code de Hamming.*

Soit α une racine de $g(X)$ dans $\mathbb{F}_{2^m}$. Comme $g(X)$ est irréductible, tout polynôme de $\mathbb{F}_2[X]$ est un multiple de $g(X)$ si et seulement s'il admet α comme racine. Comme α est aussi une racine de $X^n - 1$, on en déduit que le code C, en représentation polynomiale, est constitué de l'ensemble des polynômes $c(X)$ modulo $X^n - 1$ tels que $c(\alpha) = 0$. Cette caractérisation du code C permet d'étudier facilement sa distance minimale.

Proposition 35 *Les paramètres d'un code de Hamming sont*

$$[n = 2^m - 1, n - m, 3].$$

Preuve : La dimension du code est donnée par le théorème 33.

Soit $c = (c_0, c_1, \ldots, c_{n-1})$ un mot du code de Hamming C. Nous venons de voir que le polynôme associé $c(X) = c_0 + c_1 X + \cdots c_{n-1} X^{n-1}$ a pour racine α, ce qui s'écrit

$$\sum_{i-0}^{n-1} c_i \alpha^i = 0.$$

Comme les α^i sont non nuls, le poids de c n'est pas 1. Le poids de c n'est pas 2 non plus car cela se traduirait par $\alpha^i + \alpha^j = 0$ pour $0 \leqslant i, j \leqslant n-1$, $i \neq j$. Mais comme α est un élément primitif de $\mathbb{F}_{2^m}$, on a $\alpha^i \neq \alpha^j$, contradiction. Le poids

minimum de C est donc au moins 3. Ce n'est pas plus. En effet, comme α est primitif, il existe i tel que $1 + \alpha = \alpha^i$. Le polynôme $1 + X + X^i$ s'annulle donc en α, le vecteur de poids 3 associé appartient donc au code C. ∎

Codes BCH. Cherchons maintenant à obtenir un code de distance minimale 5. Soit α de nouveau un élément primitif de $\mathbb{F}_{2^m}$. Définissons C comme le code cyclique de longueur $n = 2^n - 1$ constitué des polynômes $c(X)$ de $\mathbb{F}_2[X]/(X^n - 1)$ ayant *simultanément* α et α^3 comme racines. Dis autrement, il s'agit du code cyclique de polynôme générateur $P_\alpha(X)P_{\alpha^3}(X)$ où P_α et P_{α^3} sont les polynômes minimaux de α et α^3.

Proposition 36 *Le code cyclique C défini ci-dessus a un distance minimale $d \geqslant 5$.*

Preuve : Soit $c(X) = c_0 + c_1X + \cdots c_{n-1}X^{n-1}$ un mot du code C. Notons, qu'outre les racines α et α^3, il a aussi α^2 et α^4, conjuguées de α, comme racines. Ceci s'écrit :

$$\sum_{i=0}^{n-1} c_i \begin{bmatrix} \alpha^i \\ \alpha^{2i} \\ \alpha^{3i} \\ \alpha^{4i} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Si $c(X)$ est un mot de poids 4 ou moins, alors tous les c_i sont nuls, sauf au plus quatre d'entre eux. Ceci veut dire qu'il existe une combinaison linéaire non triviale sommant à zéro des colonnes de la matrice

$$\begin{bmatrix} x & y & z & t \\ x^2 & y^2 & z^2 & t^2 \\ x^3 & y^3 & z^3 & t^3 \\ x^4 & y^4 & z^4 & t^4 \end{bmatrix}$$

où x, y, z, t sont des puissances distinctes de α. Mais cette matrice (van der Monde) est non singulière si x, t, z, t sont des éléments distincts du corps $\mathbb{F}_{2^m}$, ce qui est le cas puisque α est primitif. Contradiction. ∎

Généralisation. Tout code cyclique de longueur $n = 2^m - 1$ dont le polynôme générateur a s racines consécutives, soit $\alpha, \alpha^2, \ldots \alpha^s$ où α est un élément primitif de $\mathbb{F}_{2^m}$, a une distance minimale $d \geqslant s + 1$. En particulier le code cyclique de longueur $n = 2^m - 1$ constitué des polynômes ayant pour racines $\alpha, \alpha^3, \ldots, \alpha^{2t-1}$ a une distance minimale $d \geqslant 2t + 1$. Sa dimension est au moins $n - tm$ (regarder le degré du polynôme générateur). De tels codes sont appelés codes BCH t-correcteurs.

Remarque. La construction s'étend à des longueurs n qui ne sont pas nécessairement de la forme $n = 2^m - 1$. Il suffit de remplacer l'élément α par une racine

primitive n-ème de 1, c'est-à-dire une racine ζ de $X^n - 1$ telle que toutes les racines de $X^n - 1$ soient des puissances de ζ. Nous avons constaté à la section 7.1 qu'un tel ζ existe toujours. Tout polynôme diviseur de $X^n - 1$ dont $\zeta, \zeta^2, \ldots \zeta^s$ sont des racines engendre un code cyclique de distance minimale au moins $s + 1$.

Points essentiels à retenir

- Ce que sont les paramètres $[n, k, d]$ d'un code linéaire.
- Si la distance minimale d d'un code vérifie $d \geqslant 2t+1$, le code permet de corriger n'importe quelle configuration de t erreurs en allant chercher le mot de code le plus proche (pour la distance de Hamming) du vecteur reçu.
- Un code de Hamming binaire est un code cyclique binaire de longeur $n = 2^m - 1$ et de polynôme générateur un polynôme irréductible primitif de degré m sur $\mathbb{F}_2$. Ses paramètres sont $[2^m - 1, 2^m - 1 - m, 3]$.
- Un code cyclique sur $\mathbb{F}_q$ peut se définir, plutôt que par son polynôme générateur, par un ensemble de racines du polynôme générateur dans un corps d'extension de $\mathbb{F}_q$.
- Les matrices à coefficients dans un corps commutatif quelconque de la forme
$$\begin{bmatrix} x_1 & x_2 & \ldots & x_s \\ x_1^2 & x_2^2 & \ldots & x_s^2 \\ \ldots & \ldots & \ldots & \ldots \\ \vdots & \vdots & \vdots & \vdots \\ x_1^s & x_2^s & \ldots & x_s^s \end{bmatrix}$$
sont singulières si et seulement il existe i, j, $1 \leqslant i, j \leqslant s$, $i \neq j$ tels que $x_i = x_j$.
- Comment fabriquer un code (BCH) 2-correcteur (de distance minimale au moins 5).
- Un code cyclique binaire de longueur n et de polynôme minimal $g(X)$ est de distance minimale au moins $s + 1$, si $g(X)$ admet comme racines $\alpha, \alpha^2, \ldots, \alpha^s$ dans une extension appropriée de $\mathbb{F}_2$ et si les n puissances successives de α, à savoir $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ sont toutes distinctes.

8 Codes de Reed-Solomon, reconstruction polynomiale

8.1 Codes de Reed-Solomon, introduction

Soit $\{\alpha_1, \ldots, \alpha_n\}$ une partie à n éléments du corps $\mathbb{F}_q$. Soit C l'ensemble des vecteurs de $\mathbb{F}_q^n$ de la forme $(f(\alpha_1), \ldots, f(\alpha_n))$ où $f(X)$ est un polynôme de degré strictement inférieur à $k \leqslant n$.

– Exercice 15. *Montrer que C est un code linéaire sur $\mathbb{F}_q$ de longueur n, dimension k, et distance minimale $d = n - k + 1$.*

On appelle un tel code, *code de Reed-Solomon.*

– Exercice 16. *Borne de Singleton. Quel est le nombre maximal de vecteurs $(x_1, x_2, \ldots, x_{k-1})$ différents, lorsque $(x_1, x_2, \ldots, x_n)$ décrit l'ensemble des mots d'un code linéaire C de paramètres $[n, k, d]$? En déduire que quel que soit le code C on a :*

$$d \leqslant n - k + 1.$$

Interpolation. Soit $(c_1, c_2, \ldots, c_n)$ un mot d'un code de Reed-Solomon de paramètres $[n, k, d]$. Soit $K \subset [1, n]$, $|K| \geqslant k$. Rappelons que *l'interpolation de Lagrange* permet de reconstituer le polynôme $f(X)$ à partir des valeurs $(c_i)_{i \in K}$.

$$f(X) = \sum_{i \in K} c_i \frac{\prod_{j \in K, j \neq i}(X - \alpha_j)}{\prod_{j \in K, j \neq i}(\alpha_i - \alpha_j)}.$$

– Exercice 17.

1. *Montrer qu'une matrice génératrice* $\mathbf{G}$ *du code de Reed-Solomon C est donnée par :*

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}.$$

2. *Lorsque $n = q - 1$, que γ est un élément primitif de $\mathbb{F}_q$, et que*

$$\alpha_1 = 1, \alpha_2 = \gamma, \alpha_3 = \gamma^2, \ldots, \alpha_n = \gamma^{q-1},$$

vérifier que le code C est un code cyclique.

8.2 Correction d'erreurs

Soit $(c_1, \ldots, c_n)$ un mot de code associé au polynôme $f(X)$. Notons le vecteur reçu $(r_1, \ldots, r_n)$. Soit e le nombre de symboles erronés, $e = \#\{i, r_i \neq c_i\}$. On appelle *polynôme localisateur d'erreur* le polynôme

$$E(X) = \prod_{i, r_i \neq c_i} (X - \alpha_i).$$

On a clairement

$$\forall i, \quad f(\alpha_i)E(\alpha_i) = r_i E(\alpha_i).$$

Écrivons $Q(X) = f(X)E(X)$. Soit $t = \lfloor (n-k)/2 \rfloor$ et supposons $e \leqslant t$. On constate que le couple $(Q(X), E(X))$ vérifie les conditions

1. $\deg E \leqslant t$, $\deg Q < k + t$, $E(X)$ est unitaire,
2. $\forall i, \quad Q(\alpha_i) = r_i E(\alpha_i)$.

Le théorème suivant assure que le décodage équivaut à la recherche d'un tel couple $(Q(X), E(X))$.

Théorème 37 *Tout couple $(Q(X), E(X))$ vérifiant les conditions 1 et 2 ci-dessus est tel que :*

$$f(X) = \frac{Q(X)}{E(X)}.$$

Preuve : On a déjà constaté l'existence d'un tel couple $(Q(X), E(X))$. Soit $(Q_1(X), E_1(X))$ un autre couple satisfaisant aux mêmes conditions. On a alors

$$\forall i, \quad Q(\alpha_i)E_1(\alpha_i)r_i = r_i E(\alpha_i)Q_1(\alpha_i)$$

ce qui implique

$$\forall i, \quad Q(\alpha_i)E_1(\alpha_i) = E(\alpha_i)Q_1(\alpha_i)$$

puisque si $r_i = 0$ alors $Q(\alpha_i) = Q_1(\alpha_i) = 0$. Mais la condition 1 implique $\deg(QE_1 - EQ_1) < n$, d'où $QE_1 - EQ_1 = 0$ et $\frac{Q_1(X)}{E_1(X)} = \frac{Q(X)}{E(X)}$. ∎

Les coefficients des polynômes $Q(X), E(X)$ peuvent se trouver simultanément par la résolution d'un système linéaire de n équations à au plus n inconnues (condition 2). On peut être plus efficace.

8.3 Décodage rapide

8.3.1 Fractions continues et algorithme d'Euclide

L'écriture $[a_0, a_1, \ldots, a_{m-1}, a_m]$, où $a_i \in \mathbb{F}_q(X)$, désigne la fraction rationnelle

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_m}}}}$$

appelée *fraction continue*. On définit les suites (p_k) et (q_k), $k = 0 \ldots m$, d'éléments de $\mathbb{F}_q(X)$, par :

$$\left\{ \begin{array}{rcl} p_0 & = & a_0 \\ q_0 & = & 1 \end{array} \right. \qquad \left\{ \begin{array}{rcl} p_1 & = & a_0 a_1 + 1 \\ q_1 & = & a_1 \end{array} \right.$$

et la récurrence, pour $k \geqslant 2$,

$$\left\{ \begin{array}{rcl} p_k & = & a_k p_{k-1} + p_{k-2} \\ q_k & = & a_k q_{k-1} + q_{k-2}. \end{array} \right. \tag{10}$$

La fraction rationnelle p_k/q_k est appelée *k-ème réduite* de la fraction continue.

– Exercice 18. *Montrer que, pour tout $k \leqslant m$, on a :*

$$\frac{p_k}{q_k} = [a_0, a_1, \ldots, a_k] \tag{11}$$

et que, pour tout k, $1 \leqslant k \leqslant m$,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}. \tag{12}$$

– Exercice 19. *Montrer que toute fraction rationnelle $Z(X)$ admet une unique écriture $Z(X) = [a_0, a_1, \ldots, a_m]$ où tous les a_k sont des polynômes, de degré $\geqslant 1$ pour $k \geqslant 1$. Cette fraction continue est appelée* développement en fraction continue *de $Z(X)$.*

Remarque. Les a_i sont donnés par les quotients successifs de l'algorithme d'Euclide appliqué au numérateur et au dénominateur de $Z(X)$.

Théorème 38 *Si $Z(X) = \frac{N(X)}{D(X)}$ et p/q sont des fractions rationnelles telles que $\deg(Z(X) - p/q) < -2 \deg q$, alors p/q est une réduite du développement en fraction continue de $Z(X)$.*

Preuve : Soit $p/q = [a_0, \dots a_{k+1}]$ le développement en fraction continue de p/q, de telle sorte que la dernière réduite p_{k+1}/q_{k+1} égale p/q. La fraction p_k/q_k est donc l'avant-dernière réduite. On pose

$$Z(X) = \frac{yp + p_k}{yq + q_k} \tag{13}$$

où y est une certaine fraction rationnelle : ceci est toujours possible, sauf si $Z(X) = p/q$ auquel cas il n'y a rien à montrer. D'après (10) l'égalité (13) s'écrit aussi

$$Z(X) = [a_0, \dots, a_{k+1}, y].$$

Le théorème sera donc démontré dès que l'on montre que $\deg(y) > 0$. Or,

$$Z(X) - \frac{p}{q} = \frac{yp + p_k}{yq + q_k} - \frac{p}{q} = \frac{p_k q - p q_k}{q(yq + q_k)} = \frac{\pm 1}{q(yq + q_k)}$$

d'après (12). On en déduit $yq^2 + qq_k = \pm 1/(Z(X) - p/q)$, soit

$$y = \frac{\pm 1}{q^2(Z(X) - \frac{p}{q})} - \frac{q_k}{q}.$$

D'après (10), on a $\deg q_k < \deg q$: de plus l'hypothèse du théorème implique $\deg(q^2(Z(X) - \frac{p}{q}) < 0$. On en déduit $\deg(y) > 0$. ∎

8.3.2 Décodage par l'algorithme d'Euclide

Comme précédemment, soit $(c_1, \dots c_n)$ le mot de code émis, soit $f(X)$ le polynôme associé, et soit $(r_1, \dots r_n)$ le vecteur reçu.

– EXERCICE 20. *Montrer que* $\prod_{x \neq 0} x = -1$.

– **Solution.** $X^{n-1} - 1 = \prod_{x \neq 0}(X - x)$.

Posons $L_i(X) = \prod_{j \neq i}(X - \alpha_j)$. Soit $R(X)$ le polynôme interpolateur des r_i. On a :

$$R(X) = -\sum_{i=1}^{n} r_i L_i(X).$$

On a :

$$\forall i \quad R(\alpha_i)E(\alpha_i) = f(\alpha_i)E(\alpha_i)$$

d'où l'on déduit

$$R(X)E(X) = f(X)E(X) \bmod X^n - X$$

ou encore

$$R(X)E(X) = f(X)E(X) + k(X)(X^n - X)$$

ce qui se réécrit

$$\frac{R(X)}{X^n - X} - \frac{k(X)}{E(X)} = \frac{f(X)}{X^n - X}.$$

Comme

$$\deg \frac{f(X)}{X^n - X} < k - n \leqslant -2 \deg E,$$

le théorème 38 s'applique et $k(X)/E(X)$ est une des réduites du développement en fraction continue de $R(X)/(X^n - X)$. Il suffit donc de tester, pour toutes les réduites $k(X)/E(X)$ de dénominateur de degré $\leqslant t$, si

$$R(X) - k(X)(X^n - X)/E(X)$$

est un polynôme de degré $< k$. Dès que c'est le cas, il s'agit forcément du polynôme $f(X)$.

Exemple. Soit le code de Reed-Solomon de dimension 3 sur $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$. Soit le vecteur reçu

$$(-2, 3, 2, 0, 0, 3, -1)$$

avec deux erreurs. On forme

$$R(X) = 2X^6 - 2X^5 - X^4 + 4X^3 + 2X^2 + 5.$$

On a $a_0 = 0$. Pour trouver a_1 on effectue la division euclidienne

$$X^7 - X = (4X + 4)R(X) - 2X^5 + 2X^4 + 4X^3 - X^2 + 1$$

ce qui nous donne $a_1 = 4X + 4 = 4(X + 1)$. Puis

$$R(X) = (-X)(-2X^5 + 2X^4 + 4X^3 - X^2 + 1) + 3X^4 + 3X^3 + 2X^2 + X - 2$$

nous donne $a_2 = -X$. On a $p_0 = 0$, $q_0 = 1$, $p_1/q_1 = 1/a_1 = 1/(4X+4)$, et d'après (10) $p_2 = -X$, $q_2 = -X(4X + 4) + 1$. D'où

$$\frac{k(X)}{E(X)} = \frac{2X}{(X - 1)(X - 5)}$$

et le polynôme $f(X)$ est donné par

$$f(X) = R(X) - 2X[X(X - 2)(X - 3)(X - 4)(X - 6)] = X^2 - 2.$$

– Exercice 21. *On considère le code de Reed-Solomon de dimension* 3 *sur* $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$. *Soit* $(-1, 0, 3, 3, 1)$ *le vecteur reçu. Trouver le mot de code le plus proche.*

Points essentiels à retenir

- Un code de Reed-Solomon de longueur n sur $\mathbb{F}_q$ est l'ensemble des vecteurs de la forme $(f(\alpha_1), \ldots, f(\alpha_n))$ où $f(X)$ est un polynôme de degré $< k \leqslant n$ et où $\alpha_1 \ldots \alpha_n$ sont des éléments distincts de $\mathbb{F}_q$. La dimension du code est k et sa distance minimale $d = n - k + 1$.
- Savoir donner une matrice génératrice d'un code de Reed-Solomon.
- S'il existe γ élément primitif de $\mathbb{F}_q$ tel que $\alpha_i = \gamma^{i-1}$, alors le code de Reed-Solomon est cyclique.
- La formule d'interpolation pour les polynômes.
- La définition du polynôme localisateur d'erreurs,

$$E(X) = \prod_{i, c_i \neq r_i} (X - \alpha_i)$$

  où (c_i) est le mot émis et (r_i) est le mot reçu.
- Si $R(X)$ est le polynôme interpolateur des symboles reçus, r_i, alors le polynôme localisateur d'erreurs $E(X)$ est le dénominateur d'une réduite du développement en fraction continue de $R(X)/\prod_i (X - \alpha_i)$, i.e. dans le cas où $n = q$, de $R(X)/(X^n - X)$.