

CODES CORRECTEURS

POLISANO KÉVIN
MP* AU LYCÉE FABERT

TPE 2009-2010

Table des matières

1	Etude théorique des corps finis	2
1.1	Structure additive et multiplicative	2
1.1.1	Corps premiers	2
1.1.2	Structure additive	3
1.1.3	Structure multiplicative	4
1.2	Corps de rupture et corps de décomposition	7
1.2.1	Idéaux	7
1.2.2	Corps de rupture	9
1.2.3	Corps de décomposition	12
1.2.4	Construction des corps finis	14
1.3	Polynômes cyclotomiques	15
1.3.1	Le polynôme ϕ_n	15
1.3.2	Racines des polynômes cyclotomiques	16
1.3.3	Décomposition des polynômes cyclotomiques dans un corps fini	17
1.4	Existence et unicité des corps finis	19
2	Constructions et calculs	23
2.1	Construction explicite des corps finis	23
2.1.1	Qu'appelle-t-on \mathbb{F}_q ?	23
2.1.2	Exemples de constructions	24
2.2	Calculs dans les corps finis	25
2.2.1	Table de correspondance	25
2.2.2	Logarithme de Zech	26
2.3	Mise en place d'un code correcteur	26
2.3.1	Table de correspondance de \mathbb{F}_{16}	26
2.3.2	Codage et décodage	27
3	Les codes correcteurs	30
3.1	Généralités sur les codes correcteurs	30
3.1.1	Codage	30
3.1.2	Poids et distance de Hamming	31
3.1.3	Décodage	32
3.2	Codes cycliques	34
3.2.1	Polynômes générateurs	34
3.2.2	Classes cyclotomiques	37
3.2.3	Distance minimale des codes cycliques	39
3.2.4	Codes de Hamming	40
3.3	Codes BCH	41
3.3.1	Présentation	41
3.3.2	Codes BCH binaires	42
3.3.3	Décodage des codes BCH	44

Partie 1 : Etude théorique des corps finis

1.1 Structure additive et multiplicative

1.1.1 Corps premiers

Dans toute cette partie nous ne considérerons que des anneaux commutatifs unitaires.

☞ Soit \mathcal{A} un anneau, il existe un unique morphisme dit canonique de \mathbb{Z} dans \mathcal{A} .

En effet $\phi : \mathbb{Z} \rightarrow \mathcal{A}$ doit vérifier $\phi(1_{\mathbb{Z}}) = 1_{\mathcal{A}}$ et par propriété du morphisme $\phi(1_{\mathbb{Z}} + 1_{\mathbb{Z}}) = 1_{\mathcal{A}} + 1_{\mathcal{A}} = 2_{\mathcal{A}}$.

Par une récurrence immédiate $\phi(n_{\mathbb{Z}}) = n_{\mathcal{A}}$. Et $\phi(-n_{\mathbb{Z}}) = -\phi(n_{\mathbb{Z}}) = -n_{\mathcal{A}} = (-n)_{\mathcal{A}}$.

On étend ainsi ϕ à tout \mathbb{Z} . Cette construction rend ϕ unique.

Inversement ϕ construit de cette façon est un morphisme.

Définition 1.1 *Ker ϕ sous-groupe de \mathbb{Z} donc de la forme $p\mathbb{Z}$ où p est la **caractéristique** de \mathcal{A} .*

Remarques :

- p est le plus petit entier naturel non nul tel que $p \cdot 1_{\mathcal{A}} = \underbrace{1_{\mathcal{A}} + \dots + 1_{\mathcal{A}}}_{p \text{ fois}} = 0_{\mathcal{A}}$.
- Si $p = 0 \Rightarrow \phi$ injective. Comme \mathbb{Z} est infini alors \mathcal{A} l'est aussi.
- Pour un anneau intègre, p est premier, sinon il se décomposerait $p = ab$ et on aurait :

$$\phi(p) = \phi(ab) = \phi(a)\phi(b) = 0$$

L'intégrité donne $\phi(a) = 0$ ou $\phi(b) = 0$ ce qui contredirait la minimalité de p .

Proposition 1.2 *Tout corps K contient un sous-corps premier : \mathbb{Q} si $p = 0$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sinon.*

Preuve : Pour démontrer le premier cas faisons la remarque liminaire suivante :

✎ Le **corps des fractions** $\text{Frac}(A)$ d'un anneau A est par définition le plus petit corps contenant A . Donc tout corps contenant A contient le corps des fractions de A .

Si on a un morphisme injectif $f : A \rightarrow K$ alors K « contient » A et d'après la remarque $\text{Frac}(A)$.

Dans le cas $p = 0$ on a donc bien K qui contient \mathbb{Q} le corps des fractions de \mathbb{Z} par définition.

Pour traiter le cas $p \neq 0$ premier, démontrons au préalable le **théorème d'isomorphisme** :

Théorème 1.3 *Si $f : A \rightarrow B$ est un morphisme d'anneau, alors $A/\text{Ker}f \simeq \text{Im}f$.*

Preuve : Considérons pour les éléments de A la relation suivante

$$x\mathcal{R}y \iff x - y \in \text{Ker}f$$

\mathcal{R} est une relation d'équivalence, et muni des opérations

$\overline{x+y} = \bar{x} + \bar{y}$ et $\overline{xy} = \bar{x}\bar{y}$ ce quotient est un anneau (voir **proposition 1.16**).

On vérifie aussi facilement que $\text{Im} f = f(A)$ est un anneau.

★ Construisons un isomorphisme de $A/\text{Ker} f$ dans $\text{Im} f$ en considérant la fonction :

$$g: A/\text{Ker} f \longrightarrow \text{Im} f \\ \bar{x} \longmapsto f(x)$$

Montrons que g est bien définie i.e si x et y représentent la même classe $\bar{x} = \bar{y}$ alors $g(x) = g(y)$.

C'est bien le cas car :

$$g(\bar{y}) = f(y) = f(y - x + x) = f(y - x) + f(x)$$

Or comme $\bar{x} = \bar{y}$ on a $y - x \in \text{Ker} f$ donc $f(y - x) = 0$ et par suite $g(\bar{y}) = f(x) = g(\bar{x})$.

De plus f étant un morphisme d'anneau, g est aussi un morphisme d'anneau par construction.

Montrons que g est injective :

$$g(\bar{x}) = g(\bar{y}) \Rightarrow f(x) = f(y) \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \text{Ker} f \Rightarrow \bar{x} = \bar{y}$$

Et g est surjective car tout $z \in \text{Im} f$ de la forme $z = f(x)$ admet \bar{x} comme antécédent par g .

Donc g est bijective, on obtient l'isomorphisme souhaité. \square

☞ On peut désormais appliquer ce théorème à l'application $\phi: \mathbb{Z} \rightarrow K$:

$\text{Im} f \subset K$ et $\text{Im} f \simeq \mathbb{Z}/\text{Ker} f = \mathbb{Z}/p\mathbb{Z}$ donc K « contient » $\mathbb{Z}/p\mathbb{Z}$ qui est un corps car p premier.

Les deux assertions de la proposition sont donc démontrées. \blacksquare

1.1.2 Structure additive

On s'intéresse à un corps K fini. Comme \mathbb{Q} est infini on en déduit que K contient \mathbb{F}_p .

Définition 1.4 K est un sous-corps d'un corps $L \iff L$ est une **extension** du corps K .

Ainsi, K est une extension de \mathbb{F}_p , on peut donc le voir comme \mathbb{F}_p -espace vectoriel.

Par conséquent, il existe une base (e_1, \dots, e_n) de K telle que

$$\forall x \in K, \exists! (\lambda_1, \dots, \lambda_n) \in (\mathbb{F}_p)^n, x = \sum_{i=1}^n \lambda_i e_i$$

L'ensemble des éléments de K est en bijection avec les n -uplets de \mathbb{F}_p donc ont même cardinal.

Théorème 1.5 Le **cardinal** d'un corps fini est de la forme p^n où p est sa caractéristique.

1.1.3 Structure multiplicative

Définition 1.6 $\phi(n)$ est le nombre d'entiers inférieurs et premiers avec n , φ **fonction d'Euler**.

Théorème 1.7 Le groupe multiplicatif K^* d'un corps fini est **cyclique**.

Preuve : Démontrons préalablement les points suivants :

- On a la relation $\sum_{d|n} \varphi(d) = n$. En effet, on note

$$D = \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n} \right\}$$

et pour d divisant n on définit

$$D_d = \left\{ \frac{k}{d} / k \wedge d = 1 \text{ et } 1 \leq k \leq d \right\}$$

De l'existence et l'unicité de l'écriture d'un nombre rationnel sous forme d'une fraction irréductible on déduit que les D_d forment une partition de D . D'où :

$$n = \text{Card}(D) = \sum_{d|n} \text{Card}(D_d) \quad \text{et} \quad \text{Card}(D_d) = \varphi(d)$$

- K un corps commutatif. Deux éléments $\neq 0$ de même ordre engendrent le même sous-groupe.

Soit d cet ordre, G_1 et G_2 les sous-groupes respectifs de K^* engendrés par ces éléments.

Les éléments de G_1 et G_2 sont donc racines du polynôme $X^d - 1$.

Puisqu'il est de degré d il a au plus d racines car K est un corps commutatif.

Enfin comme G_1 et G_2 ont d éléments, ce sont exactement les racines de $X^d - 1$ d'où $G_1 = G_2$.

- Il existe au plus $\varphi(d)$ éléments de K^* d'ordre d .

S'il n'existe aucun élément d'ordre d c'est immédiat, sinon il en existe au moins un a .

Par le point précédent, tous les éléments d'ordre d appartiennent au groupe engendré par a :

$$H = \{a^k, k \in \llbracket 0, d-1 \rrbracket\}$$

Ainsi les éléments d'ordre d sont exactement les générateurs de H . Et pour k fixé :

$$\langle a^k \rangle = H \Leftrightarrow \exists m, a^{km} = a \Leftrightarrow a^{km-1} = 1 \Leftrightarrow d | km - 1 \Leftrightarrow km + dm' = 1 \Leftrightarrow k \wedge d = 1$$

Par définition de φ , il y a $\varphi(d)$ k qui vérifient $k \wedge d = 1$, soit $\varphi(d)$ générateurs.

- Soit c_d le nombre d'éléments d'ordre d de K^* pour $d|n$ où $n = \text{Card}(K)$.

On sait d'après Lagrange que l'ordre $d|n$, donc tout élément a un ordre et ainsi

$$\sum_{d|n} c_d = n$$

Et la relation d'Euler donne

$$\sum_{d|n} c_d = \sum_{d|n} \varphi(d)$$

On vient de voir $c_d = 0$ ou $\varphi(d)$, comme ce sont des entiers il vient $c_d = \varphi(d)$, $\forall d|n$.

En particulier $c_n = \varphi(n)$ donc il existe des éléments d'ordre n , par conséquent K^* est cyclique.

Plus généralement $c_d = \varphi(d)$ montre que tout sous-groupe fini de K^* est cyclique. ■

Proposition 1.8 *Les q éléments de K sont les q racines distinctes dans K de $X^q - X$.*

Preuve : D'après Lagrange, si G est un groupe fini à n éléments et $x \in G$ d'ordre m :

$$m|n \Leftrightarrow n = mk \quad \text{d'où} \quad x^n = x^{mk} = (x^m)^k = 1$$

K^* a $p^n - 1 = q - 1$ éléments donc $\forall x \in K^*$, $x^{q-1} = 1$ soit en rajoutant 0 :

$$\forall x \in K, \quad x^q = x$$

Ainsi les éléments de K sont exactement les q racines dans K de $X^q - X$. ■

Remarque : comme K est commutatif, on a la relation $X^q - X = \prod_{a \in K} (X - a)$.

Définition 1.9 *Soit K corps fini de caractéristique p , on définit l'application de Frobenius :*

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

Proposition 1.10 *L'application de Frobenius est $\mathbb{Z}/p\mathbb{Z}$ -linéaire.*

Preuve : On a p premier, on montre tout d'abord que p divise $\binom{p}{i}$ pour $i \in \llbracket 2, p-1 \rrbracket$:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \iff \binom{p}{i} i! = p(p-1)\cdots(p-i+1)$$

p ne divise aucun terme de $i!$ car premier, donc d'après le théorème de Gauss il divise $\binom{p}{i}$.

• Soient $(x, y) \in K^2$, on a modulo p :

$$F(x+y) = (x+y)^p = \sum_{i=0}^p \binom{p}{i} x^{n-i} y^i = x^p + y^p = F(x) + F(y)$$

• Soit $x \in K$ et $n \in \mathbb{Z}/p\mathbb{Z}$,

$$F(nx) = n^p x^p = nx^p = nF(x)$$

d'après le petit théorème de Fermat, ce qui achève la preuve. ■

Proposition 1.11 *L'application de Frobenius est un **automorphisme** du corps K .*

Preuve : La propriété de morphisme découle de la proposition précédente et du fait que

$$F(xy) = (xy)^p = x^p y^p = F(x)F(y)$$

car K est commutatif. F est en outre injective car par intégrité on a :

$$F(x) = 0 \implies x^p = 0 \implies x = 0$$

Et comme K est fini on en déduit que F est bijective. ■

Proposition 1.12 *Le nombre d'éléments de tout sous-corps de K est de la forme p^r où $r|n$.*

Preuve : Soit k un sous-corps de K , c'est un corps fini donc $\text{Card}(k) = p^r$.

Pour montrer que $r|n$ prouvons tout d'abord le lemme suivant :

Lemme 1.13 *Soient $(p, n, r) \in (\mathbb{N}^3)^*$ et $p > 1$, on a $p^r - 1 | p^n - 1 \iff r|n$.*

\Rightarrow Effectuons la division euclidienne $n = qr + s$ avec $s < r$. On a bien sûr :

$$p^r \equiv 1 \pmod{p^r - 1}$$

En élevant à la puissance q et en multipliant par p^s on obtient :

$$p^{qr} \equiv 1 \pmod{p^r - 1} \implies p^n = p^{qr+s} \equiv p^s \pmod{p^r - 1}$$

Mais par hypothèse $p^n - 1 \equiv 0 \pmod{p^r - 1} \iff p^n \equiv 1 \pmod{p^r - 1}$ d'où :

$$p^s \equiv 1 \pmod{p^r - 1} \iff p^r - 1 | p^s - 1$$

Or puisque $s < r$ cela implique $s = 0$ d'où $n = qr$ et $r|n$.

\Leftarrow Réciproquement si $r|n \iff n = qr$ et vu ci-dessus :

$$p^n = p^{qr} \equiv 1 \pmod{p^r - 1} \iff p^r - 1 | p^n - 1$$

Ce qui termine la preuve du lemme. \square

k^* possède un élément d'ordre $p^r - 1$ qui divise $\text{Card}K^* = p^n - 1$ par Lagrange d'où $r|n$.

Remarque : $\forall \alpha \in k$, $\alpha^{p^r} = \alpha$, mais cette équation a au plus p^r solutions, qui sont donc les éléments de k . Cela montre que k est l'ensemble des racines dans K de cette équation, donc est l'unique sous-corps de K à p^r éléments. ■

Proposition 1.14 *Inversement pour tout $r|n$ il existe un unique sous-corps de K à p^r éléments : c'est l'ensemble des $a \in K$ tels que $a^{p^r} = a$.*

Preuve : Soit $r \mid n$, notons k l'ensemble des $a \in K$ tels que $a^{p^r} = a$.

L'application $f : a \mapsto a^{p^r}$ est un automorphisme du corps K car c'est $f = F^r$.

Donc k est l'ensemble des points fixes de f , qui est un sous-corps de K .

k a au plus p^r éléments (degré de $X^{p^r} - X$).

Puisque K^* est cyclique d'ordre $p^n - 1$ et que $p^r - 1 \mid p^n - 1$,

K^* possède un élément d'ordre $p^r - 1$ disons α .

0 et les $p^r - 1$ puissances de α sont solutions de l'équation donc elle a au moins p^r solutions.

Ainsi k a bien p^r éléments, ce qui achève la démonstration. ■

Remarque : L'unicité découle de la remarque précédente.

1.2 Corps de rupture et corps de décomposition

1.2.1 Idéaux

Définition 1.15 $I \subset A$ est un **idéal** de $A \Leftrightarrow I$ est un sous-groupe additif de A et :

$$\forall (a, x) \in A \times I, \quad ax \in I \text{ (et } xa \in I \text{ car } A \text{ commutatif)}$$

☞ $\text{Ker}\phi = \{x \in \mathbb{Z}, \phi(x) = 0_A\}$ est un idéal bilatère de \mathbb{Z} :

Sous-groupe de \mathbb{Z} car $\text{Ker}\phi \subset \mathbb{Z}$, $0 \in \text{Ker}\phi$ ($\phi(0) = 0$ par morphisme) et stable par $-$:

$$\forall (x, y) \in (\text{Ker}\phi)^2, \quad \phi(x - y) = \phi(x) - \phi(y) = 0$$

$$\forall (x, y) \in \text{Ker}\phi \times \mathbb{Z}, \quad \phi(xy) = \phi(x)\phi(y) = 0 = \phi(y)\phi(x) = \phi(yx)$$

Proposition 1.16 Soit I un idéal de A , la relation \mathcal{R} suivante est une **relation d'équivalence** :

$$\forall (x, y) \in A^2, \quad x\mathcal{R}y \iff x - y \in I$$

Preuve :

◦ Réflexivité : $x - x = 0_A \in I$ car I sous-groupe de A donc $x\mathcal{R}x$.

◦ Symétrie : $x\mathcal{R}y \iff x - y \in I \iff -(x - y) = y - x \in I \iff y\mathcal{R}x$ car I est un sous-groupe de A .

◦ Transitivité : $x\mathcal{R}y$ et $y\mathcal{R}z$ d'où par stabilité de $+$: $(x - y) + (y - z) = x - z \in I \iff x\mathcal{R}z$.

Ainsi \mathcal{R} est une relation d'équivalence.

✎ On définit le quotient A/I comme l'ensemble des classes d'équivalences de \mathcal{R} .

Proposition 1.17 *Muni des opérations $\overline{x+y} = \bar{x} + \bar{y}$ et $\overline{xy} = \bar{x}\bar{y}$ ce quotient est un anneau.*

Preuve :

On s'assure comme en 1.3 que ces lois additives et multiplicatives sont bien définies.

Soit $\bar{x} = \bar{x}'$ et $\bar{y} = \bar{y}'$, alors :

- $\bar{x} + \bar{y} = \bar{x}' + \bar{y}'$ et comme $\begin{cases} \bar{x} + \bar{y} = \overline{x+y} \\ \bar{x}' + \bar{y}' = \overline{x'+y'} \end{cases}$ on a bien $\overline{x+y} = \overline{x'+y'}$.
- On écrit $xy - x'y' = (x - x')y - x'(y - y')$ et comme $\bar{x} = \bar{x}'$ on a $x - x' \in I$, de même $y - y' \in I$.

C'est ici que l'on se sert du fait que I est un idéal : $(x - x')y \in I$ et $x'(y - y') \in I$.

Comme I est un sous-groupe additif de A on obtient par soustraction

$$(x - x')y - x'(y - y') \in I \Leftrightarrow xy - x'y' \in I \Leftrightarrow \overline{xy} = \overline{x'y'}$$

Ces lois de composition internes (par construction) confèrent à A/I une structure d'anneau.

En effet $(A/I, +)$ est un groupe commutatif car pour tout représentant $(x, y, z) \in A^3$ on a :

- Associativité : $(\bar{x} + \bar{y}) + \bar{z} = \overline{x+y} + \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} + \overline{y+z} = \bar{x} + (\bar{y} + \bar{z})$.
- $\overline{0_A}$ est le neutre : $\bar{x} + \overline{0_A} = \overline{x+0_A} = \bar{x}$.
- L'inverse de \bar{x} est $\overline{-x}$ car $\bar{x} + \overline{-x} = \overline{x-x} = \overline{0_A}$.
- Commutativité : $\bar{x} + \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} + \bar{x}$ car A commutatif.

Vérifions enfin que la loi multiplicative est associative et distributive par rapport à + :

$$(\bar{x}\bar{y})\bar{z} = \overline{xy}\bar{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{xy}z = \bar{x}(\bar{y}\bar{z})$$

$$\bar{x}(\bar{y} + \bar{z}) = \overline{\bar{x}(y+z)} = \overline{xy+xz} = \overline{xy} + \overline{xz} = \bar{x}\bar{y} + \bar{x}\bar{z}$$

De même pour la distributivité à gauche. Ce qui démontre la proposition. ■

Définition 1.18 I est un **idéal maximal** de $A \Leftrightarrow I \neq A$ et $\forall J \supset I \Rightarrow J = I$ ou $J = A$.

Remarque : En d'autre termes il n'y a pas d'idéaux intermédiaires entre I et A , il est maximal.

Proposition 1.19 Soient $P \in A$ irréductible et l'idéal $(P) = \{PT, T \in A\}$, on a :

$$A \text{ euclidien} \xrightarrow{1} (P) \text{ maximal} \xrightarrow{2} A/(P) \text{ est un corps.}$$

¹ *Preuve :*

$\xRightarrow{1}$ P est irréductible donc non inversible, ainsi $(P) \neq A$ car sinon

$$1 \in (P) \Rightarrow \exists Q \in A / PQ = QP = 1$$

ce qui est exclu.

Soit un idéal $J \supset (P)$, on sait qu'il existe $Q \in A$ tel que $J = (Q)$ car A principal.

Mais alors $(Q) \supset (P) \Rightarrow Q$ divise P , et comme P irréductible on a :

Soit Q associé à P et donc $J = (Q) = (P)$ soit Q inversible auquel cas $J = (Q) = A$. \square

$\xRightarrow{2}$ Soit $Q \in A / \bar{Q} \neq \bar{0}$ c'est-à-dire Q n'est pas divisible par P soit encore $Q \notin (P)$.

Remarque : Rappelons qu'ici $I = (P)$ dans la proposition 1.16 donc $\bar{0} = \{T \in A / T - 0 = T \in (P)\}$.

Notons $J = \{xP + yQ, (x, y) \in A^2\}$ l'idéal engendré par P et Q .

On a $J \supset (P)$ et (P) maximal donc $J = (P)$ ou $J = A$. Or $Q \in J$ et $Q \notin (P)$ donc $J = A$.


En particulier $1 \in J$ donc $\exists(x_0, y_0) \in A^2 / 1 = x_0P + y_0Q$ et en passant aux classes :

$$\bar{1} = \overline{x_0P + y_0Q} = \bar{x}_0 \underbrace{\bar{P}}_{=\bar{0}} + \bar{y}_0 \bar{Q} = \bar{y}_0 \bar{Q}$$

L'inverse de \bar{Q} est \bar{y}_0 et par suite $A/(P)$ est un corps. \blacksquare

1.2.2 Corps de rupture

Soit P un polynôme irréductible sur un corps (commutatif) K quelconque.

 Soit k une extension du corps K et $\alpha \in k$. On note $k(\alpha)$ (resp. $k[\alpha]$) le plus petit sous-corps (resp. le plus petit sous-anneau) de k contenant K et α .

Définition 1.20 *Un corps de rupture de P sur K est une extension k de K dans laquelle P au moins une racine α telle que α engendre k . Plus précisément vérifiant $P(\alpha) = 0$ et $k = K(\alpha)$.*

* Construisons un corps de rupture en nous appuyant sur les résultats établis sur les idéaux :

$K[X]$ est euclidien et P irréductible, d'après la **proposition 1.19** $k = K[X]/(P)$ est un corps.

Montrons que k est un sur-corps de K c'est-à-dire que K s'injecte dans k soit $\bar{x} = \bar{y} \Leftrightarrow x = y$.

Pour cela on identifie les scalaires x et y à des polynômes (constants) de $K[X]$, alors :

$$\bar{x} = \bar{y} \Leftrightarrow \overline{x - y} = \bar{0} \Leftrightarrow x - y \in (P)$$

Le seul polynôme constant appartenant à (P) est le polynôme nul d'où $x - y = 0 \Rightarrow x = y$.

Réciproquement si $x = y$ on a bien sûr $\bar{x} = \bar{y}$.

Considérons maintenant la classe de l'indéterminée X que l'on note $x = \bar{X}$. Il s'ensuit :

$$P(x) = P(\bar{X}) = \overline{P(X)} = \bar{0}$$

Remarque : la deuxième égalité résulte des lois additives et multiplicatives sur les classes.

On a donc bien trouvé une racine x de P sur le sur-corps k . \square

Reste à montrer que $k = K[X]/(P) = K(x)$:

\square Soit $Q(X) = \sum a_i X^i \in K[X]$, en passant à la classe $\bar{Q} \in K[X]/(P)$ et :

$$\overline{Q(X)} = \sum a_i (\bar{X})^i = \sum a_i x^i \in K(x)$$

\square Le corps $K[X]/(P)$ contient $\bar{X} = x$ et K donc à fortiori le corps $K(x)$.

On a ainsi montré l'égalité par double inclusion. \blacksquare

✓ L'intérêt est de taille, cela signifie que si l'on a un polynôme irréductible sur un corps donné, il est toujours possible de cette façon de construire un corps « plus grand » sur lequel ce polynôme admet une racine.

Exemple : prenons le polynôme $X^2 + 1$ qui est irréductible sur le corps $\mathbb{R}[X]$.

Plaçons nous alors sur le sur-corps $k = \mathbb{R}[X]/(X^2 + 1)$ et notons $i = \bar{X}$.

D'après ce qui précède, i est racine de $X^2 + 1$ sur k c'est-à-dire $i^2 = -1$.

Nous venons de construire le **corps des complexes**...

Proposition 1.21 *Deux corps de rupture de $P \in K[X]$ irréductible sont isomorphes.*

Preuve : On a vu que $k = K[X]/(P)$ est un corps de rupture de P .

Soit k' un autre corps de rupture de P avec $k' = K(\alpha)$ et $P(\alpha) = 0$.

Alors l'application

$$\begin{aligned} f: K[X] &\longrightarrow k' \\ Q &\longmapsto Q(\alpha) \end{aligned}$$

est surjective, $\text{Ker } f = (P)$ car $(P) \subset \text{Ker } f$ et (P) maximal ($K[X]$ euclidien).

Le **théorème d'isomorphisme** donne donc

$$\text{Im } f = k' \simeq K[X]/\text{Ker } f = K[X]/(P) = k$$

On a bien un isomorphisme entre k et k' . \blacksquare

Supposons qu'il existe $P \in K[X]$ irréductible de degré s ,

alors $K[X]/(P)$ est un corps sur lequel $x = \bar{X}$ est racine de P . Et on a :

Proposition 1.22 *La famille $\mathfrak{F} = (1, x, \dots, x^{s-1})$ est une base de $K[X]/(P)$.*

Preuve :

- Prenons un polynôme $Q \in K[X]$ et effectuons la division euclidienne par P :

$$Q(X) = R(X)P(X) + S(X) \quad \text{avec} \quad \deg(S) < s = \deg(P)$$

Ainsi $R(X) = a_r X^r + \dots + a_1 X + a_0$ avec $r < s$. En passant à la classe on a :

$$\overline{Q(X)} = \overline{R(X)} \Leftrightarrow Q(x) \equiv R(x) \equiv a_r x^r + \dots + a_1 x + a_0 \pmod{P}$$

Ainsi la classe de Q est combinaison linéaire de $1, x, \dots, x^r$ donc \mathfrak{F} est génératrice.

☞ On remarque que les éléments de $K[X]/(P)$ sont des polynômes en x de degré $\leq s$.

- Montrer maintenant que \mathfrak{F} est libre. Supposons que :

$$\sum_{i=0}^{s-1} a_i x^i = \bar{0}$$

Introduisons le polynôme $Q(X) = \sum_{i=0}^{s-1} a_i X^i$, par hypothèse en passant à la classe :

$$\bar{Q} = \bar{0} \Leftrightarrow Q - 0 = Q \in (P) \Leftrightarrow P \mid Q$$

Or $\deg(P) = s > s-1 = \deg(Q)$ d'où nécessairement $Q = 0$ et par suite $\forall i \in \llbracket 0, s-1 \rrbracket$, $a_i = 0$. ■

Puisque K s'injecte dans $K[X]/(P)$ on peut voir le quotient comme K -espace vectoriel.

Dans l'exemple précédent $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ possède bien une copie de \mathbb{R} .

De plus la famille $(1, i)$ est bien une base de \mathbb{C} vu comme \mathbb{R} -espace vectoriel :

$$\forall z \in \mathbb{C}, \exists a, b \in \mathbb{R}, z = 1.a + i.b = a + ib$$

Si maintenant K est fini (donc à $q = p^n$ éléments) on peut raisonner comme au **théorème 1.5** :

Comme $(1, \dots, x^{s-1})$ est une base du K -espace vectoriel $K[X]/(P)$,

les éléments de $K[X]/(P)$ sont en bijection avec les s -uplets de K d'où :

Proposition 1.23 *Soient K fini et P irréductible de degré s alors $K[X]/(P)$ est un corps et*

$$\text{Card}(K[X]/(P)) = q^s = (p^n)^s = p^{ns}$$

Considérons maintenant le corps fini $K = \mathbb{F}_p$.

Il existe $P \in \mathbb{F}_p[X]$ irréductible de degré n (existence établie à la **proposition 1.35**).

On en déduit le corollaire suivant :

Corollaire 1.24 *Le corps $\mathbb{F}_p[X]/(P)$ possède p^n éléments.*

1.2.3 Corps de décomposition

Soit K un corps et P un polynôme sur K de degré $d > 1$.

Théorème 1.25 *Un corps de décomposition de P sur K est une extension k de K tel que :*

- i) P soit scindé dans $k[X]$, c'est-à-dire P a toutes ses racines dans k ,*
- ii) k est minimal pour cette propriété, c'est-à-dire que les racines de P engendrent k .*

Proposition 1.26 *Tout polynôme $P \in K[X]$ possède un corps de décomposition sur K .*

Preuve : Par récurrence sur le degré n de P .

- Si $n = 1$ alors K est corps de décomposition pour P sur K .
- Supposons la propriété vraie pour tout polynôme de degré strictement plus petit que n .

D'après le **paragraphe 1.2.2** il existe une extension E de K contenant une racine a de P .

Donc le polynôme $X - a$ divise P dans $E[X]$, soit :

$$P(X) = (X - a)Q(X) \text{ avec } \deg(Q) \leq n - 1$$

L'hypothèse de récurrence permet de trouver un corps de décomposition F pour Q sur $E[X]$:

$$Q(X) = \alpha \prod_{i=2}^n (X - a_i) \text{ dans } F[X]$$

Et alors en posant $a_1 = a$ on a dans $F[X]$:

$$P(X) = (X - a)Q(X) = (X - a)\alpha \prod_{i=2}^n (X - a_i) = \alpha \prod_{i=1}^n (X - a_i)$$

Ainsi F est un corps de décomposition pour P sur K . ■

Exemple : Prenons le polynôme $X^3 - 2$ et considérons son corps de rupture $K = \mathbb{Q}[X]/(X^3 - 2)$.

En notant comme tout à l'heure $x = \bar{X}$ et sachant que $\bar{2} = 2$ (\mathbb{Q} s'injecte dans le quotient) :

$$\overline{X^3 - 2} = x^3 - 2 = 0 \implies x^3 = 2$$

Ainsi dans le quotient :

$$T^3 - 2 = T^3 - x^3 = (T - x)(T^2 + xT + x^2)$$

Essayons de décomposer $T^2 + xT + x^2$, pour cela il faut que son discriminant $\Delta = -3x^2$ soit un carré.

C'est-à-dire qu'il existe un polynôme de degré 2 tel que :

$$-3 = (ax^2 + bx + c)^2 = (2ac + b^2)x^2 + (2bc + 2a^2)x + (4ab + c^2)$$

Comme $(1, x, x^2)$ est une base de K sur \mathbb{Q} on peut identifier :

$$\begin{cases} 2ac = -b^2 \\ 2bc = -2a^2 \\ 4ab + c^2 = -3 \end{cases}$$

Le produit des deux premières égalités montrent que $ab \geq 0$, ce qui contredit la dernière égalité.

Ainsi $T^2 + xT + x^2$ est irréductible sur K et le corps de rupture n'est pas corps de décomposition.

On réitère alors le procédé en considérant le corps de rupture du facteur irréductible restant :

$$L = K[T]/(T^2 + xT + x^2)$$

En notant $t = \bar{T}$ on a de nouveau $t^2 + xt + x^2 = 0$ soit encore $-x - t = \frac{x^2}{t}$.

On obtient les deux dernières racines de $X^3 - 2$ et L est son corps de décomposition.

Remarque : Un corps de décomposition s'obtient donc par des extensions successives. Chaque extension étant construite comme corps de rupture d'un facteur irréductible de degré > 1 du polynôme initial sur l'extension précédente.

Théorème 1.27 Soit p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.

Il existe des corps K à q éléments. Un tel corps est un corps de décomposition de $X^q - X$ sur \mathbb{F}_p .

Plus précisément les éléments de K sont les q racines de $X^q - X$.

Preuve : Considérons un corps de décomposition K de $X^q - X$ sur \mathbb{F}_p .

Notons R l'ensemble de ses racines dans K . Montrons que $R = K$ puis que $\text{Card}(K) = q$.

Vérifions que R est un sous-corps de K . Si x et y sont dans R , les égalités :

$$(x + y)^q = F^n(x + y) = F^n(x) + F^n(y) = x + y \quad \text{et} \quad (xy)^q = x^q y^q = xy$$

montrent que $x + y$ et xy sont dans R car racines de $X^q - X$.

Remarque : F^n désigne la n -ième itérée de F , car $F(x + y) = (x + y)^p$ et $q = p^n$.

Enfin si $x \neq 0$ est dans R en multipliant $q + 1$ fois à gauche par x^{-1} :

$$x^q = x \Leftrightarrow x^{-1}x^q = x^{-1}x \Leftrightarrow x^{q-1} = 1 \Leftrightarrow x^{q-2} = x^{-1} \Leftrightarrow \dots \Leftrightarrow x^{-1} = (x^{-1})^q$$

x^{-1} est dans R et par suite R est un corps, constitué de toutes les racines de $X^q - X$.

De là R est égal au corps de décomposition K de $X^q - X$.

Les q racines de $X^q - X$ dans K sont \neq car ce polynôme et sa dérivée -1 sont étrangers.

$$\text{Card}(R) = \text{Card}(K) = q$$

Réciproquement, si l'on se donne un corps K à q éléments, on a vu que ses éléments sont les q racines dans K de $X^q - X$ et que K contient un sous-corps premier isomorphe à \mathbb{F}_p . Ceci montre bien que K est un corps de décomposition de $X^q - X$ sur \mathbb{F}_p . ■

1.2.4 Construction des corps finis

On souhaite construire un corps K à $q = p^n$ éléments comme corps de décomposition de $X^q - X$ sur \mathbb{F}_p . Nous avons vu qu'un corps de décomposition d'un polynôme se construit à l'aide de quotients successifs. Ici le polynôme considéré n'est jamais irréductible. On peut toujours écrire la factorisation :

$$X^q - X = X(X^{q-1} - 1) = X(X - 1)(1 + X + \dots + X^{q-2})$$

Pour obtenir un corps de décomposition, il s'agit donc à priori de finir la factorisation en facteurs irréductibles, puis de trouver successivement, des corps de plus en plus gros, dans lesquels tous ces facteurs irréductibles se décomposent.

Mais cela devient très abstrait puisque le corps fini ainsi construit résulte de plusieurs empilements $\mathbb{F}_p, K_1, \dots, K_i$ de corps de rupture où $K_{i+1} = K_i[X]/(Q)$ avec Q un facteur irréductible. Ce serait donc beaucoup plus économe de l'obtenir avec un seul quotient !

Proposition 1.28 *Une particularité des corps finis est que l'on peut trouver une facteur irréductible P de $X^q - X$ dont le corps de rupture $\mathbb{F}_p[X]/(P)$ est un corps de décomposition de tous les facteurs irréductibles de $X^q - X$.*

Preuve : On se place dans un corps fini **quelconque** K à q éléments.

On a vu que le groupe multiplicatif K^* est cyclique. Soit x un générateur de K^* .

Pour obtenir un tel polynôme P il suffit de choisir le **polynôme minimal** de x .

☞ le polynôme unitaire de plus bas degré à coefficient dans \mathbb{F}_p tel que $P(x) = 0$.

Comme $x^{q-1} = 1$, le polynôme minimal P divise $X^{q-1} - 1$ ou encore $X^q - X$ qui est annulateur.

Ainsi P est bien un facteur irréductible (car minimal) de $X^q - X$.

Il reste à voir si en quotientant par P on obtient bien un corps de décomposition de $X^q - X$.

🔗 $\mathbb{F}_p(x)$ est par définition le plus petit sous-corps de K contenant \mathbb{F}_p et x .

Or x engendre K^* d'où $\mathbb{F}_p(x) = K$.

Puis ce corps contient la racine x de P donc est un corps de rupture de P comme $\mathbb{F}_p[X]/(P)$.

Enfin deux corps de rupture de P étant isomorphes on en déduit $\mathbb{F}_p[X]/(P) \simeq F_p(x) = K$.

Mais on sait que les $q = p^n$ éléments de K sont les q racines de $X^q - X$.

Donc par isomorphisme $\mathbb{F}_p[X]/(P)$ contient ces q racines.

C'est donc effectivement un corps de décomposition de $X^q - X$. ■

Remarque : comme x engendre K^* , par isomorphisme la classe de X engendre $(\mathbb{F}_p[X]/(P))^*$.

✎ Un tel polynôme P irréductible où la classe de X engendre $\mathbb{F}_p[X]/(P)$ est dit **primitif**.

Pour construire un corps fini à $q = p^n$ éléments il suffirait alors de déterminer le polynôme minimal du générateur de K^* et de quotienter.

Cependant cette construction reste complètement abstraite car on n'a pas de moyen explicite de trouver un générateur de K^* tant que l'on n'a pas concrètement le corps K !

Proposition 1.29 *Un corps de rupture de P irréductible sur K en est un corps de décomposition.*

Preuve : Soit d le degré de P sur K de cardinal $q = p^n$.

Le corps de rupture $K_1 = K[X]/(P)$ de P sur K est de cardinal q^d .

Ce corps fini, ensemble des racines distinctes de $X^{p^d} - X$ contient une racine x de P .

Le polynôme P est donc un facteur irréductible sur K de $X^{q^d} - X$.

$X^{q^d} - X$ étant séparablement scindé dans K_1 , les racines du facteur P sont toutes dans K_1 .

Ainsi K_1 est corps de décomposition de P . ■

☞ Revenons à la recherche d'un corps de décomposition de $X^q - X = X(X^{q-1} - 1)$. Le facteur $X^{q-1} - 1$ conduit naturellement à regarder de plus près les racines de l'unité dans un corps fini et leur polynôme minimal sur \mathbb{F}_p , c'est l'objet de la section qui suit.

1.3 Polynômes cyclotomiques

1.3.1 Le polynôme ϕ_n

Dans \mathbb{C} les racines n -ième de l'unité sont les $e^{2i\pi r}$ où $nr \in \mathbb{Z}$.

✎ C'est une **racine primitive** n -ième si n est le dénominateur de la fraction r irréductible.

Lorsque k parcourt $\mathbb{Z}/n\mathbb{Z}$ on obtient les racines n -ième, et les primitives pour $k \in (\mathbb{Z}/n\mathbb{Z})^*$.

Soit $n > 0$ un entier et le produit $\prod_{\zeta} (X - \zeta)$ où ζ parcourt les racines primitives n -ième.

Définition 1.30 On appelle n -ième polynôme cyclotomique ce produit :

$$\phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - e^{2\pi ik/n})$$

Proposition 1.31 ϕ_n est un polynôme unitaire de degré $\varphi(n)$ à coefficients entiers, et

$$X^n - 1 = \prod_{d|n} \phi_d \quad (*)$$

Preuve : ϕ_n est clairement unitaire, et de degré $\varphi(n)$ car il y a $\varphi(n)$ éléments dans $(\mathbb{Z}/n\mathbb{Z})^*$.

On démontre cette égalité en regroupant les racines n -ième de l'unité suivant leur ordre :

$$X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mathbb{U}_n \\ \zeta \text{ d'ordre } d}} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mathbb{U}_d \\ \zeta \text{ primitive}}} (X - \zeta) = \prod_{d|n} \phi_d$$

Par récurrence supposons que tous les ϕ_d où $d|n$ et $d \neq n$ soient à coefficients entiers, alors :

$$X^n - 1 = \phi_n(X)h(X)$$

où $h(X)$ est un polynôme unitaire de $\mathbb{Z}[X]$. Par division euclidienne dans $\mathbb{Z}[X]$ on a :

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

avec $g(X)$ et $h(X)$ à coefficients entiers et $\deg(r) < \deg(h)$.

Mais par unicité de la division euclidienne dans $\mathbb{C}[X]$ il vient $\phi_n = g \in \mathbb{Z}[X]$. ■

Remarque : l'égalité des degrés dans (*) permet de retrouver la relation $n = \sum_{d|n} \varphi(d)$.

Et (*) donne un moyen récurrent de calculer les ϕ_n :

$$\phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d \neq n} \phi_d} \quad \text{où } d|n \text{ et } d \neq n$$

Les premiers polynômes cyclotomiques sont donc :

$$\begin{aligned} \phi_1(X) &= X - 1 \\ \phi_2(X) &= X + 1 \\ \phi_3(X) &= X^2 + X + 1 \\ \phi_4(X) &= X^2 + 1 \\ \phi_5(X) &= X^4 + X^3 + X^2 + X + 1 \\ \phi_6(X) &= X^2 - X + 1 \\ &\vdots \end{aligned}$$

1.3.2 Racines des polynômes cyclotomiques

Jusqu'ici nous nous étions placés dans le corps \mathbb{C} . Mais comme ϕ_n est à coefficients entiers, on peut calculer $\phi_n(a)$ pour tout élément a d'un anneau A .

Proposition 1.32 Soient A un anneau intègre et $n > 0$ un entier tel que $n \cdot 1_A \neq 0$.

- i) Les racines n -ièmes de l'unité dans A sont des racines simples du polynôme $X^n - 1$. Plus généralement, il n'existe pas de polynôme non constant $Q \in A[X]$ tel que Q^2 divise $X^n - 1$.
 ii) Les racines de ϕ_n dans A sont exactement les racines primitives n -ième de l'unité dans A .

Preuve :

- i) Supposons que l'on puisse écrire $X^n - 1 = Q(X)^2 R(X)$ et dérivons cette égalité, on obtient :

$$nX^{n-1} = Q(X)[2Q'(X)R(X) + Q(X)R'(X)]$$

Ecrivons alors

$$n \cdot 1_A = (nX^{n-1})X - n(X^n - 1)$$

et remplaçons nX^{n-1} et $X^n - 1$ par leur expression, il vient :

$$n \cdot 1_A = Q(X)[2Q'(X)R(X)X + Q(X)R'(X)X - nQ(X)R(X)]$$

$\implies Q(X)$ divise la constante non nulle $n \cdot 1_A$, donc est constant.

- ii) On vient de voir que les racines n -ième de l'unité dans A i.e de $X^n - 1$ sont simples.

Il en résulte qu'elles sont racines d'exactly un des polynômes ϕ_d pour $d|n$ d'après (*).

Mais les racines de ϕ_d pour $d|n$ et $d \neq n$ sont aussi racines des $X^d - 1$.

Donc ces racines ne sont pas primitives, et celles de ϕ_n restantes le sont. ■

1.3.3 Décomposition des polynômes cyclotomiques dans un corps fini

Comme déjà dit, les polynômes cyclotomiques sont construits sur \mathbb{C} et ont des coefficients entiers.

Mais un polynôme ϕ_n irréductible sur \mathbb{Q} ne l'est plus nécessairement modulo p .

Exemple : $\phi_7(X) = 1 + X + \dots + X^6$ est irréductible sur \mathbb{Q} mais ne l'est plus modulo 2 :

$$1 + X + \dots + X^6 \equiv (1 + X + X^3)(1 + X^2 + X^3)[2]$$

Nous allons plus généralement déterminer ce qu'il advient lorsque l'on considère un corps fini K à $q = p^m$ éléments et le polynôme à coefficients dans K obtenu en remplaçant chaque coefficient a_i de ϕ_n par son image $a_i \cdot 1_K$ dans K . Cela consiste évidemment à réduire ces coefficients modulo p , mais comme il y a plus d'éléments dans K que dans \mathbb{F}_p (son sous-corps premier), les facteurs irréductibles de ϕ_n dans $\mathbb{F}_p[X]$ ne restent pas nécessairement irréductibles dans $K[X]$.

La proposition suivante donne la réponse complète :

Proposition 1.33 K un corps fini à $q = p^n$ éléments et n tel que $n \wedge q = 1$. On note r l'ordre de la classe de q dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$, i.e le plus petit entier tel que $q^r \equiv 1[n]$. Alors $\phi_n(X)$ se décompose dans $K[X]$ en produit de polynômes unitaires irréductibles de degré r , tous différents.

Preuve : On a $X^n - 1 = \phi_n(X) \prod_{d|n} \phi_d(X)$ avec $d \neq n$.

D'après la proposition précédente $X^n - 1$ n'est pas divisible par Q^2 non constant.

Donc ϕ_n non plus, ce qui justifie le terme « tous différents ».

Il s'agit de montrer que tout facteur irréductible de ϕ_n dans $K[X]$ est de degré r .

Soit P un tel facteur et s son degré. On construit $k = K[X]/(P)$.

On a vu que $\text{Card}(k) = q^s$ et tout élément non nul de k satisfait $\alpha^{q^s-1} = 1$.

k contient une racine ζ de P donc de ϕ_n qui est primitive n -ième d'après la **proposition 1.32**.

$\zeta^{q^s-1} = 1$ donc $n|q^s - 1$ soit encore $q^s \equiv 1[n]$. D'où $r | s$.

Ainsi puisque $\zeta^n = 1$ et $n|q^r - 1$ (car $q^r \equiv 1[n]$) on a :

$$\zeta^{q^r-1} = 1 \iff \zeta^{q^r} = \zeta$$

L'ensemble des racines de $X^{q^r} - X$ est un sous-corps de k d'après la **proposition 1.14**, car $r | s$.

Or il contient ζ (qui les engendrent car primitive), de polynôme minimal P de degré s , donc :

$$(1, \zeta, \dots, \zeta^{s-1})$$

est une famille libre dans le K -espace vectoriel k . Donc c'est une base de $\text{Vect}(1, \dots, \zeta^{s-1})$.

Cet espace vectoriel est ainsi en bijection avec K^s donc a q^s éléments.

Ainsi le corps engendré par les racines est k tout entier.

Donc $q^s = \text{Card}(k) = q^r$, donc $s = r$. Ce qui clos la démonstration. ■

Remarque : L'hypothèse $n \wedge q = p^n = 1 \iff n \wedge p = 1$ est nécessaire, sinon $n = pm$ et par Frobenius :

$$X^n - 1 = (X^m - 1)^p$$

Donc par intégrité si $x^n - 1 = 0$ alors $x^m - 1 = 0$ donc x est au plus d'ordre $m < n$.

Ainsi il n'existe aucune racine primitive n -ième et le produit ϕ_n est vide égal à 1 par convention.

Exemple : On souhaite décomposer le polynôme cyclotomique ϕ_{11} sur le corps fini \mathbb{F}_3 .

On prend donc $n = 11$ et $q = 3$ qui sont premiers entre eux, ainsi que $r = 5$ car $3^5 \equiv 1[11]$.

Alors $\phi_{11} = 1 + X + \dots + X^{10}$ se décompose en produit de 2 polynômes irréductibles de degré 5.

Remarque : Si $r = 1$, ϕ_n est scindé donc possède des racines dans K . Cela signifie que K contient des racines primitives n -ième de l'unité. Pour qu'il en soit ainsi il faut et il suffit que $n|q - 1$.

A l'opposé, pour avoir un seul facteur dans la décomposition de ϕ_n sur k il faut que $r = \deg(\phi_n) = \varphi(n)$. D'où le corollaire suivant :

Corollaire 1.34 ϕ_n irréductible sur le corps K fini à q éléments $\iff q$ engendre $(\mathbb{Z}/n\mathbb{Z})^*$.

Preuve : ϕ_n irréductible sur $K \iff$ la décomposition de ϕ_n n'a qu'un facteur irréductible.

\iff tous les facteurs de la décomposition sont de degré $\varphi(n)$ (car ce facteur est ϕ_n)

$\iff q$ est d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Détail : le sens $\boxed{\Leftarrow}$ découle du théorème, l'autre $\boxed{\Rightarrow}$ par contraposée :

Si q est d'ordre $r < \varphi(n)$, le théorème stipule que ϕ_n se décompose en produit de degré $r \neq \varphi(n)$.

Finalement comme $(\mathbb{Z}/n\mathbb{Z})^*$ possède $\varphi(n)$ éléments on a la dernière équivalence :

$$q \text{ est d'ordre } \varphi(n) \text{ dans } (\mathbb{Z}/n\mathbb{Z})^* \iff q \text{ engendre } (\mathbb{Z}/n\mathbb{Z})^*$$

On a donc bien l'équivalence annoncée. ■

Exemple : La classe de 2 est générateur de $(\mathbb{Z}/3\mathbb{Z})^*$ donc ϕ_3 irréductible sur \mathbb{F}_2 .

En particulier pour $k = \mathbb{F}_p$ avec p premier et $n = p^m - 1$ on a $r = m$ et le corollaire :

Corollaire 1.35 Dans $\mathbb{F}_p[X]$, ϕ_{p^r-1} est produit de polynômes unitaires irréductibles de degré r .

1.4 Existence et unicité des corps finis

On déduit aussitôt du dernier corollaire :

Proposition 1.36 $\forall n > 0, p$ premier, il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$.

On peut préciser le dernier corollaire :

Proposition 1.37 Ces facteurs irréductibles sont les polynômes primitifs de degré r dans $\mathbb{F}_p[X]$.

Preuve : On sait qu'il existe des polynômes de degré n facteurs irréductible de $X^{p^n} - X$.

Plus précisément il existe des polynômes primitifs de degré n quelconques parmi ces facteurs, ce sont les polynômes minimaux sur \mathbb{F}_p des générateurs de K^* où K est un corps de décomposition de $X^{p^n} - X$ sur \mathbb{F}_p .

Posons $q = p^n$ et regardons où les chercher dans la décomposition citée :

$$X^q - X = X(X^{q-1} - 1) = X \prod_{d|q-1} \phi_d$$

Ce polynôme est scindé dans K (car K corps de décomposition). Par ailleurs :

$$x \text{ est générateur de } K^* \Leftrightarrow x \text{ est d'ordre } q-1 \Leftrightarrow x \text{ est racine de } \phi_{q-1}$$

Détaillons la dernière équivalence :

\Rightarrow Si x est d'ordre $q-1$, x ne peut annuler ϕ_d pour $d|q-1$ strictement.

Sinon x serait une racine primitive d -ième de l'unité ce qui contredirait la minimalité de $q-1$.

$$X^{q-1} - 1 = \phi_{q-1} \prod_{\substack{d|q-1 \\ d \neq q-1}} \phi_d \quad (*)$$

x annule $X^{q-1} - 1$ car d'ordre $q-1$ et n'annule pas les ϕ_d donc x racine de ϕ_{q-1} . \square

\Leftarrow Réciproquement si x est racine de ϕ_{q-1} , c'est une racine primitive $q-1$ -ième de l'unité.

Donc x est d'ordre $q-1$. \square

Le polynôme minimal sur \mathbb{F}_p d'un tel x est donc un diviseur de ϕ_{q-1} .

Réciproquement tout facteur irréductible P de ϕ_{q-1} a des racines d'ordre $q-1$ dans K^* .

Par conséquent, P est polynôme minimal d'un élément primitif de l'extension K de \mathbb{F}_p .

Ainsi, les polynômes primitifs de degré n sont les facteurs irréductibles de ϕ_{p^n-1} . \blacksquare

Proposition 1.38 Dans $\mathbb{F}_p[X]$, nous avons la relation :

$$X^{p^n} - X = \prod P_i$$

où les P_i décrivent l'ensemble des polynômes irréductibles dont le degré d divise n .

Preuve : Nous allons montrer que $X^{p^n} - X$ est exactement ce produit.

Soit P un polynôme irréductible de degré r .

On a vu que dans $K = \mathbb{F}_p[X]/(P)$ qui a p^r éléments, la classe x de X satisfait à $x^{p^r} = x$.

- Si $r|n \Leftrightarrow n = mr = \underbrace{r + \dots + r}_{m \text{ fois}}$; en élevant à la puissance p^r on obtient :

$$(x^{p^r})^{p^r} = x^{p^r} \Leftrightarrow x^{p^{2r}} = x \quad \text{répété } m \text{ fois donne } x^{p^n} = x$$

ce qui signifie que $X^{p^n} - X$ est un multiple de P .

- Inversement, si $X^{p^n} - X$ est un multiple de P on a $x^{p^n} = x$.

Mais les $a \in K$ tels que $a^{p^n} = a$ forment un sous-anneau de K .

Comme il contient x qui engendre K , il lui est égal. Donc $\forall a \in K, a^{p^n-1} = 1$.

Or K^* contient un élément d'ordre $p^r - 1$ d'où $p^r - 1 | p^n - 1$ et donc $r | n$.

On obtient ainsi exactement les facteurs irréductibles considérés.

☞ Reste à prouver qu'il n'y a pas de facteurs multiples.

C'est en effet le cas, car si $X^{p^n} - X$ est divisible par P^2 , son polynôme dérivé est divisible par P .

Or ce polynôme dérivé est $p^n X^{p^n-1} - 1 = -1$ dans $\mathbb{F}_p[X]$. ■

Théorème 1.39 *i) Il existe pour tout nombre premier p et tout entier n un corps à p^n éléments.*

ii) Deux corps finis qui ont le même nombre d'éléments sont isomorphes.

iii) Plus généralement, si K est un corps fini à p^n éléments et K' un autre corps fini à p^m tel que n divise m alors K se plonge comme un sous-corps de K' .

Preuve :

i) On a vu qu'il existe au moins un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.

Alors $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments.

ii) C'est le cas particulier $n = m$ du point suivant.

Mais on peut tout de même en donner une autre démonstration :

Soit P un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$,

et K un corps fini quelconque à p^n éléments. On veut montrer que $K \simeq k = \mathbb{F}_p[X]/(P)$.

Pour cela on choisit x une racine de P dans K , qui existe car :

$X^{p^n} - X$ est égal au produit de tous les polynômes irréductibles dont le degré divise n .

Donc P divise $X^{p^n} - X$ qui est scindé dans $K[X]$, donc P l'est également.

Et considérons le morphisme

$$\begin{aligned} f: \mathbb{F}_p[X] &\longrightarrow K \\ Q &\longmapsto Q(x) \end{aligned}$$

Son noyau $\text{Ker} f$ est principal (car $\mathbb{F}_p[X]$ l'est) et $P \in \text{Ker} f$.

Comme P est irréductible on a alors $\text{Ker} f = (P)$. D'après le **théorème d'isomorphisme** :

$$\mathbb{F}_p[X]/\text{Ker} f = \mathbb{F}_p[X]/(P) \simeq \text{Im} f = K$$

iii) On a vu aussi qu'on peut décrire K à l'aide d'un élément primitif x qui vérifie $P(x) = 0$, où P est un polynôme unitaire irréductible de degré n appartenant à $\mathbb{F}_p[X]$.

Le degré n de P divise m donc P divise $X^{p^m} - X$ dans $\mathbb{F}_p[X]$.

On sait par ailleurs que dans $K'[X]$:

$$X^{p^m} - X = \prod_{a \in K'} (X - a)$$

Ainsi P divise ce produit et possède donc des racines dans K' .

Par conséquent K se plonge dans K' . ■

Justifions le dernier point : Notons x' une racine de P dans K' .

Les deux corps K et K' ont même caractéristique p donc contiennent \mathbb{F}_p .

On a vu que le sous-corps $\mathbb{F}_p(x')$ de K' est isomorphe à $\mathbb{F}_p[X]/(P)$.

Or K lui est aussi isomorphe, donc est isomorphe au sous-corps de K' cité d'où $K \subset K'$.

Partie 2 : Constructions et calculs

2.1 Construction explicite des corps finis

2.1.1 Qu'appelle-t-on \mathbb{F}_q ?

\triangle **Attention** ici $q = p^n$ et contrairement à ce que l'on pourrait penser $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$.

Définition 2.1 On appelle \mathbb{F}_q « le » corps à q éléments.

La présence des guillemets résulte du théorème qui assure que tous les corps à q éléments sont isomorphes. C'est pourquoi on s'autorise à parler « du » corps à q éléments, et de le noter \mathbb{F}_q . Mais nous allons voir que cette notation est ambiguë :

Lorsque $q = p$ est premier, cela ne pose pas de problème, car si K et K' sont deux corps à p éléments, il n'y a qu'une façon de faire correspondre les éléments de K et K' : à 1_K correspond $1_{K'}$ car un isomorphisme $f : K \rightarrow K'$ vérifie $f(1_K) = 1_{K'}$, puis à 2_K correspond $2_{K'}$ et ainsi de suite.

Donc on peut écrire dans ce cas $K = K' = \mathbb{F}_p$.

Mais cela n'est plus vrai lorsque le nombre d'éléments n'est plus premier, car de manière générale il y a plusieurs isomorphismes entre deux tels corps. En effet, si un corps est défini comme quotient $K = \mathbb{F}_p[X]/(P)$, pour définir sur K différents morphismes, on peut permuter le rôle des racines de P , ou encore choisir un autre polynôme P .

☞ Un corps à $q = p^n$ éléments ($n > 1$) est « unique » à isomorphisme *non unique* près.

Exemple : Prenons un corps K à 4 éléments, d'après le théorème $\mathbb{F}_2 \subset K$ car $2|4$.

Les éléments de K sont donc 0, 1, α et β . On a $\alpha + \alpha = 2\alpha = 0$ et de même $\beta + \beta = 0$.

$\alpha + 1$ ne peut être ni 0, ni 1, ni α donc $\alpha + 1 = \beta$ et $\beta + 1 = \alpha$.

De même $\alpha^2 = \beta$, $\beta^2 = \alpha$ et $\alpha\beta = 1$, et on a complètement déterminé la table d'opérations.

Toutefois il n'y a aucun moyen de distinguer l'un de l'autre les éléments α et β .

Si K' est un autre corps à 4 éléments et si on note γ et δ les 2 éléments $\neq 0$ et 1,

il y a deux façons distinctes d'identifier K et K' , on peut décider que :

$$\alpha = \gamma \text{ et } \beta = \delta \quad \text{ou} \quad \alpha = \delta \text{ et } \beta = \gamma$$

Plus généralement pour deux corps K et K' à $q = p^n$ éléments, si l'on a identifié K et K' par l'application $f : K \rightarrow K'$, on peut aussi bien le faire par l'application $x \mapsto (f(x))^p = f(x^p)$ car l'application de Frobenius $x \mapsto x^p$ est un automorphisme non identique, c'est lui qui est la cause de nos ennuis.

2.1.2 Exemples de constructions

Nous allons ici décrire les différentes constructions des corps à 9 éléments, puis à 16 éléments.

★ Construction d'un corps à 9 éléments

Pour construire \mathbb{F}_9 , écrivons grâce à (*) la décomposition :

$$X^9 - X = X\phi_8\phi_4\phi_2\phi_1 = X(X^4 + 1)(X^2 + 1)(X + 1)(X - 1)$$

Ici $q = 9 = 3^2$ soit $p = 3$ et $n = 2$. Le degré de ϕ_{p^n-1} est $\varphi(p^n - 1) = \varphi(8) = 4 = 2n$.

\Rightarrow Donc ϕ_{p^n-1} a deux facteurs irréductibles de degré n en vertu du **corollaire 1.34**.

Effectivement, en factorisant astucieusement, on a dans $\mathbb{F}_3[X]$:

$$\phi_8(X) = X^4 + 1 = (X^2 - 1)^2 + 2X^2 = (X^2 - 1)^2 - X^2 = (X^2 - X - 1)(X^2 + X - 1)$$

On obtient ainsi deux polynômes irréductibles primitifs d'après la proposition 1.36.

Mais aussi un troisième polynôme irréductible non primitif : $X^2 + 1$ (n'a pas de racine dans \mathbb{F}_3).

On a donc le choix entre 3 constructions de \mathbb{F}_9 :

$$\mathbb{F}_3[X]/(X^2 - X - 1), \quad \mathbb{F}_3[X]/(X^2 + X - 1), \quad \mathbb{F}_3[X]/(X^2 + 1)$$

★ Construction d'un corps à 16 éléments

De même on écrit la décomposition :

$$X^{16} - X = X\phi_{15}\phi_5\phi_3\phi_1 = X\phi_{15}(X^4 + X^3 + X^2 + X + 1)(X^2 + X + 1)(X - 1)$$

Ici $q = 2^4$ soit $p = 2$ et $n = 4$. Le degré de ϕ_{15} est $\varphi(15) = \varphi(3)\varphi(5) = 8$.

ϕ_{15} a donc deux facteurs irréductibles de degré 4. Pour le calculer on divise $X^{15} - 1$ par

$$(X^4 + X^3 + X^2 + X + 1)(X^2 + X + 1)(X - 1)$$

On trouve $\phi_{15}(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1$ (sachant que $-1 = 1$ dans \mathbb{F}_2).

Dans $\mathbb{F}_2[X]$ on obtient, avec une certaine difficulté, la factorisation :

$$X^8 + X^7 + X^5 + X^4 + X^3 + X + 1 = (X^4 + X + 1)(X^4 + X^3 + 1)$$

Remarques : On voit sur cet exemple la difficulté pratique pour factoriser le polynôme ϕ_{15} . Il est plus rapide d'établir la liste des polynômes irréductibles de degré 4 sur \mathbb{F}_2 , en éliminant ceux qui ont une racine et ceux qui sont divisibles par le seul polynôme irréductible de degré 2 : $X^2 + X + 1$, puis de tester la division de ϕ_{15} par ces polynômes. On obtient :

$X^4 + X + 1$ et $X^4 + X^3 + 1$ irréductibles primitifs et $X^4 + X^3 + X^2 + X + 1$ irréductible non primitif.

On a donc également le choix entre 3 constructions de \mathbb{F}_{16} :

$$\mathbb{F}_2[X]/(X^4 + X + 1), \quad \mathbb{F}_2[X]/(X^4 + X^3 + 1), \quad \mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$$

2.2 Calculs dans les corps finis

2.2.1 Table de correspondance

L'intérêt de choisir un polynôme P primitif de degré n est que le groupe multiplicatif du quotient $K = \mathbb{F}_p[X]/(P)$ va être engendré par la classe x de X , donc tout élément de K^* s'exprimera comme une puissance x^i du générateur avec $0 \leq i \leq p^n - 1$. Par ailleurs $(1, x, x^2, \dots, x^{n-1})$ étant une base de K sur \mathbb{F}_p , les éléments de K s'exprimeront comme combinaison linéaire de $1, x, \dots, x^{n-1}$.

On peut donc établir une table de correspondance entre les puissances x^i du générateur de K^* et leur expression comme polynôme de degré strictement inférieur à n . Celle-ci étant établie une fois pour toute, on peut alors facilement additionner deux éléments de K en utilisant la forme polynomiale, et les multiplier en utilisant la forme en puissance.

Exemple : Considérons le corps \mathbb{F}_9 défini par $\mathbb{F}_3[X]/(X^2 - X - 1)$.

Nous avons vu que le polynôme $P(X) = X^2 - X - 1$ est primitif, donc $x = \bar{X}$ engendre \mathbb{F}_9^* .

Et les éléments de $\mathbb{F}_3[X]/(X^2 - X - 1)$ peuvent être vus comme des polynômes en x de degré 1.

Etablissons la correspondance entre les puissances de x et leur expression polynomiale $a_0 + a_1x$:

On a bien sûr $1 = 1 + 0 \cdot x$ et $x = 0 + 1 \cdot x$. Comme x est racine de P on a $x^2 = x + 1$.

En multipliant par x on a donc $x^3 = x^2 + x = (x + 1) + x = 2x + 1 = 1 - x$ car $2 = -1$ dans \mathbb{F}_3 .

$$\begin{aligned} x^4 &= x \cdot x^3 = x \cdot (1 - x) = x - x^2 = x - (x + 1) = -1 \\ x^5 &= x \cdot x^4 = x \cdot (-1) = -x \\ x^6 &= x \cdot x^5 = x \cdot (-x) = -x^2 = -x - 1 \\ x^7 &= x \cdot x^6 = x \cdot (-x - 1) = -x^2 - x = -(x + 1) - x = -2x - 1 = x - 1 \end{aligned}$$

On peut alors dresser la **table de correspondance** :

Puissance	Coefficient de 1	Coefficient de x
1	1	0
x	0	1
x^2	1	1
x^3	1	-1
x^4	-1	0
x^5	0	-1
x^6	-1	-1
x^7	-1	1

Remarques : Pour calculer certaines puissances on peut utiliser le morphisme de Frobenius :

$$x^{18} = (x^6)^3 = (-x - 1)^3 = (-x)^3 + (-1)^3 = -x^3 - 1 = -1 - (1 - x) = -2 + x = 1 + x$$

Ou bien utiliser l'ordre de x dans \mathbb{F}_9^* :

$$x^{18} = (x^8)^2 \cdot x^2 = 1^2 \cdot x^2 = x^2 = x + 1$$

-> L'ordre de x est efficace pour calculer l'inverse d'une puissance.

2.2.2 Logarithme de Zech

On peut aussi utiliser une autre méthode pour additionner des puissances de x en remarquant :

$$x^i + x^j = x^i(1 + x^{j-i})$$

Si l'on connaît $1 + x^{j-i}$ sous forme de puissance de x : $1 + x^{j-i} = x^k$ on termine le calcul.

Pour systématiser cette méthode il suffit d'établir une table de correspondance entre les expressions $1 + x^i$ et les puissances de x . Cette correspondance est appelée **logarithme de Zech**.

Exemple : on reprend la construction précédente (les exposants étant définis modulo 8).

On a $1+x = x^2$ et $1+x^2 = 1+(1+x) = 2+x = x^7$. D'après le morphisme de Frobenius $(1+x^i)^3 = 1+x^{3i}$

$$1 + x^3 = 6 \quad \text{et} \quad 1 + x^6 = x^{21} = x^5$$

Enfin $1 + x^5 = 1 + (-x) = x^3$ et $1 + x^7 = 1 + (-1 + x) = x$ d'où la table de correspondance :

$1 + x$	$1 + x^2$	$1 + x^3$	$1 + x^4$	$1 + x^5$	$1 + x^6$	$1 + x^7$
x^2	x^7	x^6	0	x^3	x^5	x

Avec cette table on calcule

$$x^3 + x^5 = x^3 \cdot (1 + x^2) = x^3 \cdot x^7 = x^{10} = x^2$$

L'intérêt de cette table réside dans son petit volume : seulement deux colonnes en relations au lieu de $n+1$ colonnes dans le cas de la première table pour un corps défini par un polynôme de degré n .

Remarques : Cette table garde en mémoire l'application qui à i associe $s(i)$ tel que $1 + x^i = x^{s(i)}$.

2.3 Mise en place d'un code correcteur

2.3.1 Table de correspondance de \mathbb{F}_{16}

Le but de cette partie est d'élaborer un code correcteur permettant de détecter et de corriger 2 erreurs lors de la transmission d'un message de 7 bits. Pour cela nous allons utiliser la structure des corps finis en nous plaçant sur F_{16} précédemment construit.

Nous avons vu 3 constructions possibles de \mathbb{F}_{16} , choisissons par exemple :

$$\mathbb{F}_2[X]/(X^4 + X + 1)$$

où $P(X) = X^4 + X + 1$ a l'avantage d'être primitif. On peut donc dresser la table de correspondance :

Puissance	coef. de 1	coef. de x	coef. de x^2	coef. de x^3
1	1	0	0	0
x	0	1	0	0
x^2	0	0	1	0
x^3	0	0	0	1
x^4	1	1	0	0
x^5	0	1	1	0
x^6	0	0	1	1
x^7	1	1	0	1
x^8	1	0	1	0
x^9	0	1	0	1
x^{10}	1	1	1	0
x^{11}	0	1	1	1
x^{12}	1	1	1	1
x^{13}	1	0	1	1
x^{14}	1	0	0	1

On la remplit à partir de $x^4 = -x - 1 = x + 1$ dans \mathbb{F}_2 , et en multipliant successivement par x .

2.3.2 Codage et décodage

L'idée est d'envoyer un code de longueur 15 de façon à ce que le polynôme de degré 14 formé par ces coefficients ait pour racine x et x^3 .

★ Recherche du polynôme minimal

Le polynôme minimal de x est $P(X) = X^4 + X + 1$, cherchons le polynôme minimal de x^3 .

On veut donc trouver des coefficients a, b, c, \dots tels que $Q(x^3) = a + bx^3 + c(x^3)^2 + \dots = 0$ où

$$Q(X) = a + bX + cX^2 + \dots$$

Essayons par exemple de déterminer a, b et c en supposant que Q est de degré 2, alors :

$$a + bx^3 + cx^6 = 0$$

On remplace x^6 par son expression polynomiale déterminée par la table de correspondance :

$$a + bx^3 + c(x^3 + x^2) = 0 \iff a + cx^2 + (b+c)x^3 = 0$$

Et en identifiant on trouve $a = b = c = 0$. Donc le degré de Q n'est pas suffisant !

En fait il faut pousser jusqu'au degré 4 pour avoir des coefficients non tous nuls :

$$a + bx^3 + cx^6 + dx^9 + ex^{12} = 0$$

On remplace x^6, x^9 et x^{12} par leur expression polynomiale :

$$a + bx^3 + c(x^3 + x^2) + d(x^3 + x) + e(x^3 + x^2 + x + 1) = 0$$

On réordonne et on identifie :

$$\begin{cases} a + e = 0 \\ d + e = 0 \\ c + e = 0 \\ b + c + d + e = 0 \end{cases}$$

D'où $a = b = c = d = e$ et la seule solution non nulle est lorsque tous ces termes valent 1.

$$Q(X) = 1 + X + X^2 + X^3 + X^4$$

On vérifie que 0 et 1 ne sont pas racines et que Q n'est pas divisible par $X^2 + X + 1$.

Q est donc bien irréductible, on a notre polynôme minimal de x^3 .

Par conséquent le polynôme minimal ayant pour racines x et x^3 est le produit PQ , à savoir :

$$T(X) = P(X)Q(X) = X^8 + X^7 + X^6 + X^4 + 1$$

★ Codage

Imaginons que nous voulions envoyer le mot $(a_{14}, a_{13}, \dots, a_8)$. Formons le polynôme :

$$C_l(X) = a_{14}X^{14} + a_{13}X^{13} + \dots + a_8X^8$$

Divisons C_l par T :

$$C_l(X) = T(X)S(X) - C_R(X) \quad \text{avec} \quad \deg(C_R) < \deg(T) = 8$$

Donc C_R est de degré au plus 7 :

$$C_R(X) = a_7X^7 + \dots + a_1X + a_0$$

Formons le polynôme :

$$C(X) = a_{14}X^{14} + \dots + a_0 = C_R(X) + C_l(X) = T(X)S(X)$$

Remarque : Puisque le reste dans la division euclidienne est unique, $C(X)$ est l'unique polynôme de degré ≤ 14 qui a comme coefficients a_{14}, \dots, a_8 et pour racines x et x^3 .

Posons $C = (a_{14}, a_{13}, \dots, a_0)$ et envoyons le code C .

★ Décodage

Supposons que l'on reçoive le mot R comportant 2 éventuelles erreurs :

$$R = C + E$$

avec E le vecteur erreur possédant 0, 1 ou 2 composantes non nulles.

Revenons à la forme polynomiale, puisque $T(X)$ divise $C(X)$ on a :

$$\begin{aligned} R(x) &= R(x) \text{ car } T(x) = 0 \\ R(x^2) &= E(x^2) \text{ car } T(x) = 0 \text{ d'où } T(x^2) = (T(x))^2 = 0 \\ R(x^3) &= 0 \text{ car } T(x^3) = 0 \end{aligned}$$

Considérons le polynôme :

$$N(X) = R(x)X^2 + R(x^2)X + R(x^3) + R(x)R(x^2)$$

Plusieurs cas peuvent se présenter :

- Si $E(X) = 0$ alors $N(X) = 0$.
- Si $E(X) = X^e$ alors

$$N(X) = x^e X^2 + x^{2e} X + x^{3e} + x^{2e} x^e = (x^e X)(X + x^e)$$

- Si $E(X) = X^e + X^f$ alors $N(X) = (x^e + x^f)X^2 + (x^{2e} + x^{2f})X + (x^{3e} + x^{3f}) + (x^{2e} + x^{2f})(x^e + x^f)$

$$N(X) = (x^e + x^f)[X^2 + (x^e + x^f)X + x^e x^f] = (x^e + x^f)(X + x^e)(X + x^f)$$

Si $N(X) \neq 0$, les exposants des racines renseignent sur le nombre et l'emplacement des erreurs.

☞ Cette section a mis en évidence la puissance des corps finis au service de la correction d'erreurs, mais ne dévoile pas les secrets qui se cachent derrière tout cela. Qu'est-ce qui nous a suggéré de chercher le polynôme minimal ayant pour racines x , x^2 et x^3 ? Pourquoi envoyer un mot C plus grand que celui que l'on souhaite transmettre? Comment nous est venue l'idée de considérer ce mystérieux polynôme $N(X)$? Toutes ces questions nécessitent de regarder d'un peu plus près ce qu'on appelle les codes correcteurs et plus précisément les codes cycliques. C'est ce que nous allons faire dans la dernière partie.

Partie 3 : Les codes correcteurs

3.1 Généralités sur les codes correcteurs

3.1.1 Codage

Dans notre société, la diffusion de l'information joue un rôle primordial, elle est inscrite au coeur de tous les domaines de communications : radio, internet, sondes spatiales, CD-ROM, etc. Mais lors de l'acheminement ou le stockage de données, des erreurs peuvent survenir. Il est donc nécessaire de pouvoir les détecter et les corriger, ce qu'assure les codes correcteurs.

☞ Le codage est l'opération qui consiste à protéger le message avant de le transmettre. Pour cela il faut bien sûr ajouter de l'information au message d'origine, c'est la redondance. Un exemple très simple est l'ajout d'un bit de parité : le message 01101 est transformé en 011011 où le dernier bit est égal à la somme des bits initiaux. A la réception on somme les bits, si on obtient 1 c'est qu'une erreur s'est produite. On suppose ici que le canal de transmission est peu perturbé, c'est-à-dire qu'un message comporte au plus une erreur une fois transmis. Ce code dit de parité détecte une erreur sans pouvoir la corriger.

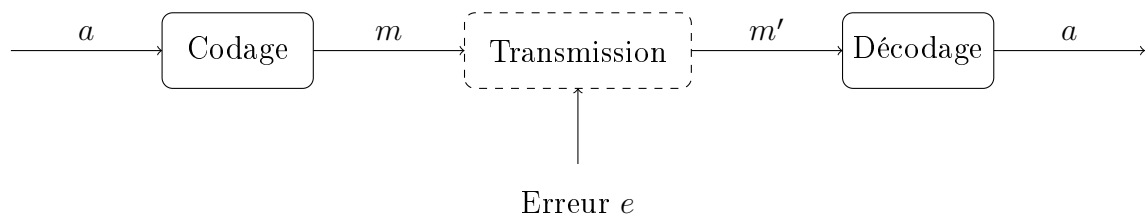
Formalisons ce que nous venons de voir dans la proposition suivante :

Proposition 3.1 *Modèle du codage*

Soit E un ensemble fini à q éléments. Soient k et n deux entiers naturels non nuls avec $0 \leq k \leq n$. L'ensemble des messages à transmettre est E^k , et l'on introduit une application injective :

$$\begin{aligned} f : E^k &\longrightarrow E^n \\ a = (a_1, \dots, a_k) &\longmapsto m = (m_1, \dots, m_n) \end{aligned}$$

appelée application de codage. Le message ou mot a est un élément de E . Il est modifié pour fournir le mot $m = f(a)$ qui sera transmis et lu par un système quelconque pour donner un message reçu m' comportant éventuellement des erreurs. L'objectif est de reconstituer m (donc a) à partir de m' , c'est le décodage.



Remarque : Notons $C = f(E)$. Comme f est injective on a une bijection de E sur C qui est appelé code de longueur n et dont les éléments sont appelés mots du code.

Choisissons $E = \mathbb{F}_q$ un corps fini à q éléments. L'ensemble des messages est donc \mathbb{F}_q^k qui est un espace-vectoriel sur \mathbb{F}_q de dimension k . Il est naturel de ne considérer que les fonctions d'encodage f linéaires. Ainsi $f(\mathbb{F}_q^k)$ est un sous-espace vectoriel de \mathbb{F}_q^n . Ce qui nous amène à la définition :

Définition 3.2 *Un code linéaire est un sous-espace vectoriel de \mathbb{F}_q^n de dimension k .*

3.1.2 Poids et distance de Hamming

Proposition 3.3 *L'application **poids** est une norme dans \mathbb{F}_q^n vu comme \mathbb{F}_q espace vectoriel.*

$$w : \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{N} \\ x = (x_1, \dots, x_i, \dots, x_n) & \longmapsto & \text{Card}\{x_i \neq 0, 1 \leq i \leq n\} \end{array}$$

Preuve : On choisit comme application valeur absolue l'application constante égale à 1.

◦ Homogénéité : Dans la mesure où \mathbb{F}_q est un corps, en multipliant une coordonnée $x_i \in \mathbb{F}_q$ non nulle par un scalaire $\alpha \in \mathbb{F}_q$ non nul, le produit $\alpha x_i \neq 0$. En effet sinon en multipliant par l'inverse de α on aurait $x_i = 0$ ce qui est exclu. Donc on ne change pas le nombre de coordonnées non nulles en multipliant par $\alpha \neq 0$ d'où :

$$w(\alpha x) = w(x) = \underbrace{|\alpha|}_{=1} w(x)$$

◦ Sous-additivité : Soit x et y deux mots, notons x_k les N coordonnées nulles de x .

Maximisons $w(x + y)$. Pour cela il faut que les composantes y_k soient toutes non nulles et que les sommes partielles restantes $x_i + y_i$ pour $i \neq k$ ne s'annulent pas par exemple en prenant $y_i = 0$ pour tout $i \neq k$. Dans cette configuration optimale les n coordonnées de $x + y$ sont non nulles, soit $w(x + y) = n$ et $w(x) = n - N$, $w(y) = N$. C'est le cas d'égalité $w(x + y) = w(x) + w(y)$. Mais si une des sommes partielles $x_i + y_i$ s'annule modulo q pour un certain y_i alors $w(x + y) < w(x) + w(y)$. Finalement :

$$\forall x, y \in \mathbb{F}_q^n, w(x + y) \leq w(x) + w(y)$$

◦ Séparation : si $w(x) = 0$ c'est que toutes les coordonnées sont nulles donc $x = 0$. ■

Proposition 3.4 *On munit l'espace vectoriel \mathbb{F}_q^n de la **distance de Hamming** :*

$$\forall x, y \in \mathbb{F}_q^n, d(x, y) = w(x - y)$$

Concrètement la distance de Hamming est le nombre de coordonnées où x et y diffèrent.

Définition 3.5 *La **distance minimale** du code C est la distance minimale entre 2 mots de C .*

$$d = \text{Min} \{d(x, y), (x, y) \in C^2 \text{ et } x \neq y\}$$

Remarque : Comme $d(x, y) = w(x - y)$ si on note $x_0, y_0 \in \mathbb{F}_q^n$ tels que

$$d = d(x_0, y_0) = w(x_0 - y_0)$$

alors $d = w(z_0)$ avec $z_0 = x_0 - y_0 \in \mathbb{F}_q^n$ car C est un espace vectoriel, donc on a aussi :

$$d = \text{Min} \{w(x), x \in C\}$$

 On dit que le code C est de paramètres $[n, k, d]$.

3.1.3 Décodage

Proposition 3.6 Code t -correcteur. Soit C un code de distance minimale d , si :

$$\exists t \in \mathbb{N}, 2t + 1 \leq d$$

alors pour tout vecteur $x \in \mathbb{F}_q^n$, il existe au mieux un seul $m \in C$ tel que $d(x, m) \leq t$.

Preuve : L'existence de $m \in C$ vérifiant $d(x, m) \leq t$ n'est pas assurée d'où le « au mieux ».

En revanche si un tel m existe alors il est unique. En effet prenons $u \in C$ distinct de m .

L'inégalité triangulaire nous donne alors :

$$d(x, u) \geq d(m, u) - d(x, m) \geq d - t \geq (2t + 1) - t = t + 1 > t$$

Ce qui démontre l'unicité. ■.

On peut illustrer la proposition précédente par le schéma ci-dessous :

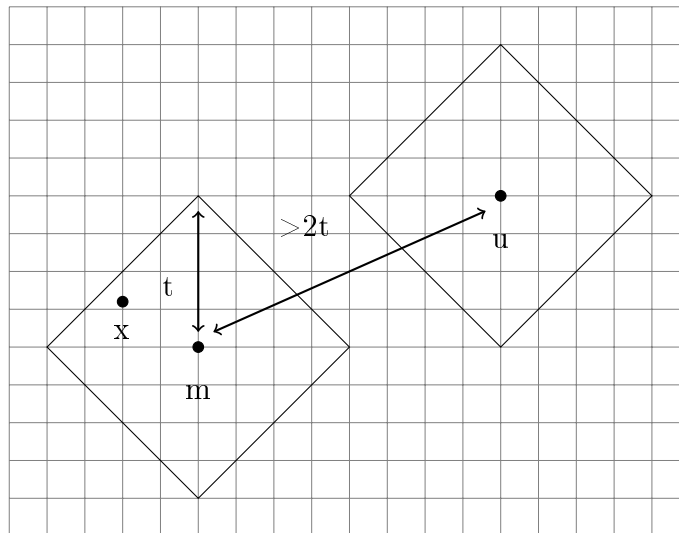



FIG. 3.1 – Représentation d'un code t -correcteur

Commentaires : La distance de m à u est bien $> 2t$ car $d \geq 2t + 1 > 2t$. De cette manière si on reçoit un mot $x = m'$ n'appartenant pas au code, qui se trouve dans la boule de rayon t centrée en m , il est très probable que le message originel soit ce centre. A partir du message erroné m' on peut donc retrouver m tel que $d(m, m') \leq t$ et comme cette distance correspond au nombre de coordonnées qui diffèrent de m et m' , le code peut corriger au plus t erreurs. Dire que C est t -correcteur, c'est aussi dire que les q^k boules de rayon t centrées en les éléments du code sont deux à deux disjointes (ce que traduit $d(m, u) > 2t$).

 La méthode de décodage la plus évidente consiste, m' étant donné, à inspecter les q^k mots du code jusqu'à ce qu'on en trouve un tel que $d(m, m') = w(m - m') \leq t$. Il s'agit là bien évidemment d'un algorithme très lent, impraticable lorsque k est grand. Toute la difficulté réside dans le fait de trouver des algorithmes de décodage praticables.

Proposition 3.7 *Le nombre d'éléments d'une boule de rayon t est :*

$$1 + n(q - 1) + \binom{n}{2}(q - 1)^2 + \dots + \binom{n}{t}(q - 1)^t$$

Preuve : Soit une telle boule centrée en un élément $m \in C$.

On va dénombrer les éléments x contenus dans cette boule suivant leur distance à m :

- Si $d(m, x) = 0$ par séparation $x = m$ donc 1 élément.
- Si $d(m, x) = 1$ une coordonnée de x diffère de m . On a le choix parmi n coordonnées de x et sur la coordonnée elle-même qui peut prendre $q - 1$ valeurs différentes de celle de m à cet emplacement. Donc il y a $n(q - 1)$ éléments à distance 1 de m .
- Si $d(m, x) = 2$ deux coordonnées diffèrent. On a de même $\binom{n}{2}$ choix pour les coordonnées et $q - 1$ valeurs possibles pour chacune d'elles, donc $\binom{n}{2}(q - 1)^2$ éléments à distance 2 de m .

Et ainsi de suite, en sommant le nombre total correspond bien à la quantité annoncée. ■

Remarque : Pour $t = n$ on retrouve bien par le binôme $(1 + (q - 1))^n = q^n$. Et dans le cas d'un code t -correcteur, les q^k boules sont disjointes donc chaque boule contient au plus $\frac{q^n}{q^k} = q^{n-k}$ éléments (dans le cas d'une partition) d'où l'inégalité :

$$1 + n(q - 1) + \binom{n}{2}(q - 1)^2 + \dots + \binom{n}{t}(q - 1)^t \leq q^{n-k}$$

Définition 3.8 *C est un code t -correcteur **parfait** si ces boules forment une partition de \mathbb{F}_q^n .*

On peut illustrer ceci par le schéma ci-dessous :

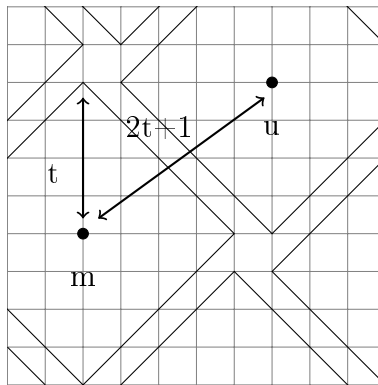


FIG. 3.2 – Représentation d'un code t -correcteur parfait

Théorème 3.9 *On possède une majoration de la distance minimale dite **borne de singleton** :*

$$d \leq n + 1 - k$$

Preuve : Considérons pour cela le sous-espace G de \mathbb{F}_q^n formé des mots dont les $k-1$ dernières composantes sont nulles, donc les mots de la forme :

$$x = (x_1, \dots, x_{n-k+1}, \underbrace{0, \dots, 0}_{k-1 \text{ fois}})$$

Il est clair que G est engendré par les $e_i = (0, \dots, i, \dots, 0, \underbrace{0, \dots, 0}_{k-1})$ car tout mot de G s'écrit :

$$x = x_1(1, 0, 0, \dots, 0) + x_2(0, 1, 0, \dots, 0) + \dots + x_{n-k+1}(0, \dots, 1, \underbrace{0, \dots, 0}_{k-1}) = x_1e_1 + x_2e_2 + \dots + x_{n-k+1}e_{n-k+1}$$

Par ailleurs si on a :

$$\sum_{i=1}^{n-k+1} \lambda_i e_i = (0, 0, \dots, 0) \Rightarrow (\lambda_1, \lambda_2, \dots, \lambda_{n-k+1}, 0, \dots, 0) = (0, 0, \dots, 0) \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_{n-k+1} = 0$$

La famille (e_1, \dots, e_{n-k+1}) est libre et génératrice, c'est une base de G d'où $\dim(G) = n - k + 1$.

$$\dim(C) + \dim(G) = k + (n - k + 1) = n + 1$$

Comme $\dim(C + G) \leq n = \dim(\mathbb{F}_q^n)$ la formule de Grassmann nous donne :

$$\dim(C \cap G) = \dim(C) + \dim(G) - \dim(C + G) \geq (n + 1) - n = 1$$

Donc il existe un élément non nul $m \in C \cap G$.

Ce mot étant dans G , il a au minimum $k-1$ coordonnées nulles donc :

$$w(m) \leq n - (k - 1) = n + 1 - k$$

Et comme pour tout $m \in C$, $d \leq w(m)$ on a le résultat voulu. ■

☞ La borne de singleton quantifie le fait que l'on ne peut pas avoir à la fois le beurre (une capacité de correction importante) et l'argent du beurre (un nombre de mots de code important), pour une longueur n fixée. Car on a vu que $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ donc si on augmente le nombre de mots donc k , on diminue la fourchette de d et donc celle du taux de correction t , et réciproquement.

📎 On désigne par $\frac{d}{n}$ et $\frac{k}{n}$ respectivement le taux de correction et d'information de C .

3.2 Codes cycliques

3.2.1 Polynômes générateurs

Les plus importants des codes linéaires sont les codes cycliques.

Définition 3.10 On dit que C est cyclique si

$$\forall m = (m_0, \dots, m_{n-2}, m_{n-1}) \in C \implies \sigma(m) = (m_{n-1}, m_0, \dots, m_{n-2}) \in C$$

Autrement dit le mot $\sigma(m)$ déduit par décalage circulaire à droite est aussi dans le code. Par itération C contient tous les décalés circulaires de m . Un code cyclique est un code linéaire stable par l'application de décalage σ .

☞ L'intérêt des codes cycliques est qu'ils bénéficient d'une description algébrique particulièrement simple en termes de polynômes. Établissons la correspondance :

$$\begin{aligned} \mathbb{F}_q^n & \longrightarrow \mathbb{F}_q[X] \\ m = (m_0, \dots, m_{n-1}) & \longmapsto m(X) = m_0 + m_1X + \dots + m_{n-1}X^{n-1} \end{aligned}$$

Cette opération est linéaire, respecte l'addition et la multiplication par un scalaire.

Soit $m'_\sigma(X) = m_{n-1} + m_0X + m_1X^2 + \dots + m_{n-2}X^{n-1}$ le polynôme du vecteur décalé $m' = \sigma(m)$.

$$Xm(X) = m_0X + m_1X^2 + \dots + m_{n-2}X^{n-1} + m_{n-1}X^n = m'_\sigma(X) - m_{n-1} + m_{n-1}X^n = m_{n-1}(X^n - 1) + m'_\sigma(X)$$

On reconnaît ici une division euclidienne par $X^n - 1$, donc modulo $X^n - 1$:

$$(\sigma(m))(X) \equiv Xm(X) \pmod{X^n - 1}$$

Ainsi modulo $X^n - 1$, le décalage des mots correspond à la multiplication des polynômes par X .

remarques : Faisons de l'algèbre avec les mains afin de comprendre d'où provient la proposition qui va suivre. Vu ce que l'on vient de voir, on peut naturellement identifier \mathbb{F}_q^n avec le quotient $\mathbb{F}_q[X]/(X^n - 1)$. Dans cette identificatin, le décalage correspond à la multiplication par X .

Les codes cycliques de longueur n correspondent aux sous-espaces stables par la multiplication par X - et à plus forte raison par tout polynôme $P(X)$ - c'est-à-dire aux idéaux de $\mathbb{F}_q[X]/(X^n - 1)$. Or ces derniers correspondent par image réciproque aux idéaux de $\mathbb{F}_q[X]$ contenant $X^n - 1$. Et ceux-ci correspondent à leur tour aux diviseurs (unitaires) de $X^n - 1$.

☞ En définitive, ces codes cycliques correspondent bijectivement aux polynômes unitaires à coefficients dans \mathbb{F}_q qui divisent $X^n - 1$. Ce que nous exposons dans cette proposition :

Proposition 3.11 Soient $g(X) = a_0 + \dots + \underbrace{a_{n-k}}_{=1} X^{n-k}$ un diviseur unitaire de $X^n - 1$ dans $\mathbb{F}_q[X]$

et $m = (a_0, \dots, a_{n-k}, 0, \dots, 0)$ le mot correspondant, alors :

- i) Les k mots $m, \sigma(m), \dots, \sigma^{k-1}(m)$ forment une base d'un code cyclique de dimension k .
- ii) Tout code cyclique de longueur n sur \mathbb{F}_q s'obtient par la construction précédente.

Preuve : i) Formons la matrice dont les lignes correspondent aux k mots considérés :

$$M = \begin{pmatrix} a_0 & \cdots & a_{n-k} & 0 & \cdots & 0 \\ 0 & \cdots & a_{n-k-1} & a_{n-k} & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & \cdots & a_{n-k} \end{pmatrix}$$

La matrice carrée extraite encadrée est triangulaire de déterminant $\det(M) = a_{n-k}^k = 1$.

M est ainsi inversible et de taille maximale donc

$$\text{rang}(M) = k$$

Or puisque M a k lignes soit les k mots, ceux-ci sont linéairement indépendants.

☞ Il reste à démontrer que le sous-espace C qu'ils engendrent est stable par σ .

Mais comme :

$$\sigma(c_0m + \dots + c_{k-1}\sigma^{k-1}(m)) = c_0\sigma(m) + \dots + c_{k-1}\sigma^k(m)$$

Les $k-1$ premiers termes sont dans C donc leur somme aussi, il suffit de prouver $\sigma^k(m) \in C$.

Or puisque g divise $X^n - 1$, on peut écrire :

$$X^n - 1 = h(X)g(X) = (b_0 + \dots + b_{k-1}X^{k-1} + X^k)g(X)$$

Ce qui donne en développant, modulo $X^n - 1$:

$$X^k g(X) \equiv -b_0 g(X) - \dots - b_{k-1} X^{k-1} g(X) \pmod{(X^n - 1)}$$

Soit encore :

$$\sigma^k(m) = -b_0 m - \dots - b_{k-1} \sigma^{k-1}(m) \in C$$

Par conséquent C est bien cyclique. \square

ii) Soit C un code cyclique. Choisissons un mot qui ait un maximum de 0 à la fin :

$$m = (a_0, \dots, a_{n-k}, 0, \dots, 0) \text{ avec } a_{n-k} \neq 0$$

Quitte à multiplier m par l'inverse de a_{n-k} , on peut supposer que $a_{n-k} = 1$.

Ce mot est unique, sinon la différence de 2 tels mots aurait au moins un 0 de plus à droite.

Comme C est cyclique, les $k-1$ mots déduits par décalages successifs appartiennent aussi à C .

De même qu'en i) ils sont linéairement indépendants, prouvons qu'ils engendrent C :

Soit $n \in C$ un mot quelconque, $n(X)$ son polynôme que l'on divise par $g(X)$ celui de m .

$$n(X) = (b_0 + \dots + b_{k-1}X^{k-1})g(X) + r(X) \text{ avec } \deg(r) < n - k$$

En développant la parenthèse on obtient la relation :

$$n = b_0 m + b_1 \sigma(m) + \dots + b_{k-1} \sigma^{k-1}(m) + r$$

Comme n , m et ses décalés appartiennent à C , par différence $r \in C$.

Or $\deg(r) < n - k$ donc r est de la forme :

$$r = (r_0, \dots, r_{n-k-1}, 0, \dots, 0)$$

et posséderait au moins un zéro de plus que m , absurde donc $r = 0$:

$$n = b_0 m + b_1 \sigma(m) + \dots + b_{k-1} \sigma^{k-1}(m)$$

Ainsi les mots considérés engendrent bien C .

☞ Reste à prouver que le polynôme $g(X)$ de m divise $X^n - 1$:

En décalant encore, le mot $p = (a_{n-k}, 0, \dots, 0, a_0, \dots, a_{n-k-1}) \in C$ et son polynôme est :

$$p(X) = \underbrace{a_{n-k}}_{=1} + 0 \cdot X + \dots + 0 \cdot X^{k-1} + a_0 X^k + \dots + a_{n-k-1} X^{n-1} = 1 + X^k (a_0 + a_1 X + \dots + a_{n-k-1} X^{n-k-1})$$

On reconnaît le polynôme $g(X)$:

$$p(X) = 1 + X^k (g(X) - a_{n-k} X^{n-k}) = X^k g(X) - (X^n - 1)$$

On applique à $p(X)$ ce qui précède, il se décompose sur la base des k mots considérés :

$$p(X) = X^k g(X) - (X^n - 1) = (b_0 + \dots + b_{k-1} X^{k-1}) g(X)$$

Que l'on réécrit :

$$X^n - 1 = (-b_0 - \dots - b_{k-1} X^{k-1} + X^k) g(X) = h(X) g(X)$$

Donc $g(X)$ divise bien $X^n - 1$ et achève la démonstration. ■

Définition 3.12 *Un tel polynôme g est dit **générateur** du code cyclique C .*

3.2.2 Classes cyclotomiques

Il s'agit donc à présent de déterminer les diviseurs de $X^n - 1$ dans $\mathbb{F}_q[X]$.

On va comme à la **proposition 1.32** supposer que $n \wedge q = 1$ et on considère le corps

$$K = R_n(\mathbb{F}_q)$$

obtenu en adjoignant à \mathbb{F}_q l'ensemble des racines n -ièmes de l'unité. (Rappelons qu'elles sont toutes des racines simples de $X^n - 1$ d'après la **proposition 1.31**). K contient au moins une racine primitive α , qui engendre toutes les autres, donc $K = \mathbb{F}_q(\alpha)$. On a vu (**proposition 1.36**) que le polynôme minimal d'une telle racine est un facteur irréductible de ϕ_n dans $\mathbb{F}_q[X]$ et de degré r la classe de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. Comme on identifie $K = \mathbb{F}_q(\alpha)$ à $\mathbb{F}_q[X]/(P)$ on en déduit que K a q^r éléments. Ce qui permet (à isomorphisme près) de le noter $K = \mathbb{F}_{q^r}$.

On peut écrire dans $K[X]$ (puisque les α^i engendrent les racines n -ième) :

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \alpha^i)$$

Tout diviseur de $X^n - 1$ dans $K[X]$ s'écrira donc sous la forme :

$$g_\Sigma(X) = \prod_{i \in \Sigma} (X - \alpha^i) \in K[X]$$

où Σ est une partie de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 3.13 $g_\Sigma \in \mathbb{F}_q[X] \Leftrightarrow \Sigma$ stable par multiplication par q .

Preuve : Par double implication. Notons $g_\Sigma(X) = \sum a_i X^i$.

\Rightarrow Si $g_\Sigma(X) \in \mathbb{F}_q[X]$ c'est que $\forall i, a_i \in \mathbb{F}_q$. Par Lagrange :

$$\forall i, a_i^q = a_i$$

Par ailleurs on a montré par Frobenius que $(x + y)^q = x^q + y^q$ et $(xy)^q = x^q y^q$ donc :

$$(g_\Sigma(X))^q = (\sum a_i X^i)^q = \sum (a_i)^q (X^i)^q = \sum a_i (X^q)^i$$

C'est-à-dire :

$$(g_\Sigma(X))^q = g(X^q)$$

Donc si α est racine de g_Σ , α^q également.

L'ensemble des racines de g est stable par passage à la puissance q -ième : $(\alpha^i)^q = \alpha^{qi} = \alpha$.

Ce qui signifie que Σ est stable par multiplication par q . \square

\Leftarrow Réciproquement supposons Σ stable par multiplication par q .

Autrement dit la multiplication par q définit une permutation de Σ .

$$(g_\Sigma(X))^q = \left(\prod_{i \in \Sigma} (X - \alpha^i) \right)^q = \prod_{i \in \Sigma} (X - \alpha^i)^q = \prod_{i \in \Sigma} (X^q - \alpha^{qi})$$

Par permutation les α^{qi} décrivent aussi les racines.

Donc on retrouve les mêmes termes dans le produit avec X^q à la place de X .

Par conséquent $(g_\Sigma(X))^q = g_\Sigma(X^q)$. Utilisons maintenant la forme développée :

$$(g_\Sigma(X))^q = g(X^q) \iff \sum (a_i)^q (X^q)^i = \sum a_i (X^q)^i$$

En identifiant on a $\forall i, a_i^q = a_i$. Et $\forall x \in \mathbb{F}_q, x^q = x$.

Donc les q éléments de \mathbb{F}_q sont racines du polynôme $X^q - X$.

Or étant de degré q , les éléments de \mathbb{F}_q sont exactement les racines de $X^q - X$.

Ainsi comme les a_i le sont également, c'est qu'ils appartiennent à \mathbb{F}_q . \blacksquare

\Rightarrow Nous avons ramené la détermination des codes cycliques de longueur n sur \mathbb{F}_q à celle des facteurs de $X^n - 1$ dans $\mathbb{F}_q[X]$, puis à celle des parties stables par multiplication par q de $\mathbb{Z}/n\mathbb{Z}$. Soit Σ une telle partie, le code correspondant est le sous-espace vectoriel de l'espace des polynômes de $\mathbb{F}_q[X]$ de degré $< n$ formé des polynômes R multiples de g_Σ (puisque'il est générateur du code cyclique), c'est-à-dire tels que $R(\alpha^i) = 0$ pour tout $i \in \Sigma$.

Définition 3.14 *Classe cyclotomique* : Σ_j la plus petite partie stable contenant $j \in \mathbb{Z}/n\mathbb{Z}$.

On l'obtient de cette façon : on considère le plus petit entier $s > 0$ tel que $q^s j \equiv j[n]$ et on a

$$\Sigma_j = \{j, qj, \dots, q^{s-1}j\}$$

☞ g_j correspondant à Σ_j est le **polynôme minimal** sur \mathbb{F}_q de α^j .

Donc les différents g_j sont les facteurs irréductibles de $X^n - 1$ dans $\mathbb{F}_q[X]$.

Exemple : Prenons $q = 2$ et $n = 7$. Par multiplication par 2 modulo 7 on a les cycles :

$$1 \mapsto 2 \mapsto 4 \mapsto 1 \quad \text{et} \quad 3 \mapsto 6 \mapsto 5 \mapsto 3$$

Ce qui donne les deux classes cyclotomiques $\{1, 2, 4\}$ et $\{3, 5, 6\}$ sans oublier $\{0\}$.

On obtient donc la décomposition $X^7 - 1 = (X - 1)g_1(X)g_3(X)$ avec

$$g_1(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4)$$

$$g_3(X) = (X - \alpha^3)(X - \alpha^5)(X - \alpha^6)$$

D'après la proposition 1.37, g_1 et g_3 sont les seuls polynômes irréductibles de degré 3 sur \mathbb{F}_2 . A savoir $1 + X + X^3$ et $1 + X^2 + X^3$ (il suffit de vérifier que 0 et 1 ne sont pas racine et que $1 + X + X^2$ ne les divise pas). Ces polynômes étant générateurs du code on obtient comme mot :

$$m = (1, 1, 0, 1, 0, 0, 0) \quad \text{ou} \quad m = (1, 0, 1, 1, 0, 0, 0)$$

Nous venons de construire le code de Hamming $[7, 4, 3]$ ($d = 3$ sera démontré plus tard).

3.2.3 Distance minimale des codes cycliques

Nous avons vu finalement que le code cyclique C de longueur n sur \mathbb{F}_q est formé des polynômes $R \in \mathbb{F}_q[X]$ qui possèdent comme racines tous les α^i pour $i \in \Sigma$ (une partie stable de $\mathbb{Z}/n\mathbb{Z}$). Dire que la distance minimale d du code C est $\geq d'$, c'est dire qu'un tel polynôme non nul R possède au moins d' coefficients non nuls. En effet s'il n'avait par exemple que $\ell \leq d' - 1$ coefficients non nuls, le mot associé r n'aurait également que ℓ coefficients non nuls, donc son poids serait $w(r) = \ell \leq d' - 1$ et $d \leq w(r) \leq d' - 1 < d'$.

La distance minimale n'est pas facile à calculer, mais on dispose d'une minoration :

Proposition 3.15 Si $\exists a, s > 0$ tels que $\{a + 1, a + 2, \dots, a + s\} \in \Sigma$ alors $d \geq s + 1$.

Preuve : Il s'agit donc de montrer que si un mot $r \in C$ avec $w(r) < s \Rightarrow r = 0$.

C'est-à-dire si $R(X)$ a au plus s coefficients $\neq 0$ et vérifie :

$$R(\alpha^i) = 0 \quad \text{pour} \quad i = a + 1, \dots, a + s \quad \Rightarrow R(X) = 0$$

Posons

$$R(X) = \sum \lambda_j X^{d_j} \quad \text{avec} \quad 0 \leq d_1 < \dots < d_s < n \quad \text{et} \quad (\lambda_1, \dots, \lambda_s) \in \mathbb{F}_q$$

On traduit le fait que $R(\lambda^i) = 0$ pour $i = a + 1, \dots, a + s$:

$$\begin{aligned} R(\alpha^{a+1}) &= \lambda_1 \alpha^{(a+1)d_1} + \dots + \lambda_s \alpha^{(a+1)d_s} = 0 \\ R(\alpha^{a+2}) &= \lambda_1 \alpha^{(a+2)d_1} + \dots + \lambda_s \alpha^{(a+2)d_s} = 0 \\ &\vdots \\ R(\alpha^{a+s}) &= \lambda_1 \alpha^{(a+s)d_1} + \dots + \lambda_s \alpha^{(a+s)d_s} = 0 \end{aligned}$$

Ce qui se réécrit sous forme matricielle :

$$\begin{pmatrix} (\alpha^{d_1})^{a+1} & \dots & (\alpha^{d_s})^{a+1} \\ (\alpha^{d_1})^{a+2} & \dots & (\alpha^{d_s})^{a+2} \\ \vdots & \ddots & \vdots \\ (\alpha^{d_1})^{a+s} & \dots & (\alpha^{d_s})^{a+s} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Le déterminant de cette matrice est un déterminant de Vandermonde en les α^{d_j} tous distincts.

Donc cette matrice est inversible et $\lambda_1 = \lambda_2 = \dots = \lambda_s = 0$. ■

3.2.4 Codes de Hamming

On prend ici $q = 2$ et $n = q^r - 1 = 2^r - 1$. Ainsi r est l'ordre de 2 modulo n .

En effet notons s l'ordre de 2 modulo n , on a :

$$2^s \equiv 1[2^r - 1] \Leftrightarrow 2^s - 1 \equiv 0[2^r - 1] \Leftrightarrow 2^r - 1 \mid 2^s - 1$$

Mais $2^s - 1 \leq 2^r - 1$ donc on a l'égalité et par suite $s = r$.

On a alors $K = R_n(\mathbb{F}_2) = \mathbb{F}_{2^r}$ et les classes cyclotomiques de la forme :

$$\{a, 2a, 4a, \dots, 2^{r-1}a\}$$

Celles dont les éléments sont premiers à n ont toutes r éléments, elles correspondent aux facteurs irréductibles de ϕ_n qui sont donc les polynômes minimaux des racines primitives n -ièmes de l'unité dits primitifs (voir **corollaire 1.34** et **proposition 1.36**). Fixons l'un de ces facteurs g (ils donnent tous des codes isomorphes), et α une de ses racines. On a donc $K = \mathbb{F}_2(\alpha)$ et

$$g(X) = \prod_{i=0}^{r-1} (X - \alpha^{2^i})$$

et $g(X)$ correspond à la classe cyclotomique $\Sigma = \{1, 2, \dots, 2^{r-1}\}$.



Le code cyclique C correspondant est le **code de Hamming** de longueur $n = 2^r - 1$ et de dimension $k = n - \deg(g) = 2^r - 1 - r$.

Proposition 3.16 *Le code de Hamming est de type $(2^r - 1, 2^r - r - 1, 3)$, est 1-correcteur et parfait.*

Preuve : Puisque Σ contient 1 et 2, $d \geq 3$ d'après la **proposition 3.15**.

Et d'après la **proposition 3.6** C est 1-correcteur.

Chaque boule de rayon 1 possède $n + 1$ éléments (voir **proposition 3.7**)

Comme $n + 1 = 2^r$, les boules centrées aux points de C ont en tout :

$$(n + 1) \times \text{Card}(C) = 2^r \times q^k = 2^r \times 2^{2^r - r - 1} = 2^{2^r - 1} = 2^n$$

éléments, donc forment une partition de l'espace \mathbb{F}_2^n d'où C parfait.

Par conséquent la distance minimale d est exactement égale à 3. ■

3.3 Codes BCH

3.3.1 Présentation

Nous venons de voir les codes de Hamming, qui sont des cas particuliers des codes BCH binaires, eux mêmes spécifiques des codes BCH généraux, dont les initiales représentent le nom des trois inventeurs de cette famille de codes : Bose, Chaudhuri et Hocquenghem.

Nous prenons n de la forme $q^m - 1$. D'où $r = m$ et $K = R_{q^m - 1}(\mathbb{F}_q) = \mathbb{F}_{q^m}$. On choisit une racine primitive $(q^m - 1)$ -ième de l'unité dans \mathbb{F}_{q^m} à partir d'un facteur irréductible de $\phi_{q^m - 1}$ sur \mathbb{F}_q . On fixe également un entier δ avec $1 < \delta \leq q^m - 1$.

$\forall 0 < i < n$, notons g_i le polynôme minimal de α^i sur \mathbb{F}_q . On a :

$$g_i(X) = \prod_{j \in \Sigma_i} (X - \alpha^j) \in \mathbb{F}_q[X]$$

où Σ_i est la classe cyclotomique engendrée par i .

Définition 3.17 On appelle **code BCH de distance assignée** δ le code cyclique de longueur $n = q^m - 1$ sur \mathbb{F}_q dont le générateur est le ppcm des g_i pour $0 < i < \delta$.

Ce code est aussi défini par la réunion Σ des classes Σ_i pour $0 < i < \delta$:

Définition 3.18 Le polynôme générateur g de ce code est égal à :

$$g(X) = \prod_{j \in \Sigma} (X - \alpha^j) \in \mathbb{F}_q[X]$$

où Σ est la plus petite partie de $\mathbb{Z}/(q^m - 1)\mathbb{Z}$ contenant $\{1, \dots, \delta - 1\}$ et stable par q .

☞ Un polynôme $m(X) \in \mathbb{F}_q[X]$ appartient au code si et seulement si

$$m(\alpha) = m(\alpha^2) = \dots = m(\alpha^{\delta-1}) = 0$$

Remarque : Le code obtenu est de dimension $k = q^m - 1 - \deg(g) = q^m - 1 - \text{Card}(\Sigma)$.

Par ailleurs puisque Σ contient $\{1, \dots, \delta - 1\}$, on a d'après la **proposition 3.15** :

Proposition 3.19 La distance minimale d de ce code est $\geq \delta$.

3.3.2 Codes BCH binaires

On prends ici $q = 2$ et δ donnée, que l'on choisit impaire.

Pourquoi? Car si δ est paire, $\frac{\delta}{2} \in \Sigma$ car $\Sigma \supset \{1, \dots, \delta - 1\}$.

Et comme Σ est stable par multiplication par 2 on aurait $\frac{\delta}{2} \times 2 = \delta \in \Sigma$.

On obtiendrait donc la même partie en partant de $\delta + 1$.

Posons donc $\delta = 2t + 1$ de sorte que C soit au moins t -correcteur ($d \geq \delta$).

★ Construction

Prenons $n = 15 = 2^4 - 1$, on se place donc dans \mathbb{F}_{16} et on choisit une racine primitive α .

Pour cela on choisit un facteur irréductible de ϕ_{15} sur \mathbb{F}_q .

On a vu que le polynôme $g_1(X) = 1 + X + X^4$ convenait. Soit α une de ses racines.

Par multiplication par 2 modulo 15 on obtient les chaînes :

$$1 \mapsto 2 \mapsto 4 \mapsto 8 \mapsto 1$$

$$3 \mapsto 6 \mapsto 12 \mapsto 9 \mapsto 3$$

$$5 \mapsto 10 \mapsto 5$$

$$7 \mapsto 14 \mapsto 13 \mapsto 11 \mapsto 7$$

Soit quatre classes cyclotomiques :

$$\Sigma_1 = \{1, 2, 4, 8\} \quad \Sigma_3 = \{3, 6, 9, 12\}$$

$$\Sigma_5 = \{5, 10\} \quad \Sigma_7 = \{7, 11, 13, 14\}$$

☞ Dressons le tableau suivant qui énumère en fonction de δ les ensembles Σ correspondants, la dimension k du code, sa distance minimale d , le nombre d'erreurs t qu'il peut corriger ainsi que le polynôme générateur g .

δ	Σ	k	d	t	g
2,3	$\{1, 2, 4, 8\}$	11	3	1	g_1
4,5	$\{1, 2, 3, 4, 6, 8, 9, 12\}$	7	5	2	$g_1 g_3$
6,7	$\{1, 2, 3, 4, 5, 6, 8, 9, 10, 12\}$	5	7	3	$g_1 g_2 g_3$
8, ..., 15	$\{1, \dots, 14\}$	1	15	7	$1 + \dots + X^{14}$

Commentaires.

Expliquons à titre d'exemple le cas $\delta = 4, 5$. Σ doit contenir $\{1, \dots, \delta - 1\} = \{1, \dots, 4\}$ et être

stable par multiplication par 2. L'ensemble $\Sigma_1 = \{1, 2, 4, 8\}$ est bien stable par construction mais il lui manque le chiffre 3, qui se trouve dans $\Sigma_3 = \{3, 6, 9, 12\}$ donc on prend

$$\Sigma = \Sigma_1 \cup \Sigma_3 = \{1, 2, 3, 4, 6, 8, 9, 12\}$$

qui est bien sûr stable par multiplication par 2 et minimal pour cette propriété.

La dimension k du code est donnée par

$$k = q^m - 1 - \text{Card}(\Sigma) = 15 - 8 = 7$$

D'abord, $g_1(X) = 1 + X + X^4$ est le polynôme minimal de α . Ensuite

$$(\alpha^3)^5 = \alpha^{15} = 1$$

α^3 est une racine primitive 5-ième et comme ϕ_5 est irréductible sur \mathbb{F}_2

$$g_3(X) = \phi_5(X) = 1 + X + X^2 + X^3 + X^4$$

est le polynôme minimal de α^3 . Enfin par Frobenius $g_1(\alpha^2) = (g_1(\alpha))^2 = 0$.

Puisque g_1 et g_3 n'ont pas de facteurs communs, leur ppcm g est :

$$g(X) = g_1(X)g_3(X) = 1 + X^4 + X^6 + X^7 + X^8$$

On obtient de même

$$g(X) = g_1(X)g_3(X)g_5(X) = 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}$$

On notera par ailleurs que le poids des générateurs est

$$w(g_1) = 3, \quad w(g_1g_3) = 5, \quad w(g_1g_3g_5) = 7$$

qui sont égaux à δ . Et comme $\delta \leq d$ il vient $d = \delta$ dans ces trois cas.

Proposition 3.20 *La distance minimale d'un code BCH binaire est **impair**.*

Preuve : Notons s l'application définie par

$$\alpha^{s(i)} = 1 + \alpha^i \quad \text{pour } 0 < i < 2^m - 1$$

et pour $R(X) = \sum m_i X^i$ un mot de code définissons le polynôme $R^{[s]}(X)$ défini par

$$R^{[s]}(X) = \sum_{i \neq 0} m_i X^{s(i)}$$

Démontrons au préalable le lemme qui suit.

Lemme 3.21 *Le polynôme $R(1) + R^{[s]}(X)$ est un mot du code.*

Fixons un entier j avec $0 < j < \delta$. Il s'agit de calculer $R^{[s]}(\alpha^j)$.

On a déjà

$$(\alpha^j)^{s(i)} = (\alpha^{s(i)})^j = (1 + \alpha^i)^j = \sum_{0 \leq k \leq j} \binom{j}{k} \alpha^{ik}$$

D'où

$$R^{[s]}(\alpha^j) = \sum_{i \neq 0} m_i (\alpha^j)^{s(i)} = \sum_{i \neq 0} \sum_{0 \leq k \leq j} \binom{j}{k} m_i (\alpha^k)^i = \sum_{0 \leq k \leq j} \binom{j}{k} \left(\sum_{i \neq 0} m_i (\alpha^k)^i \right) = \sum_{0 \leq k \leq j} \binom{j}{k} (R(\alpha^k) - m_0)$$

Mais d'une part

$$\forall k \neq 0, \quad R(\alpha^k) = 0$$

Et d'autre part modulo 2 on a

$$\sum_{0 \leq k \leq j} \binom{j}{k} = 2^j = 0$$

Donc au final il ne reste plus que le terme pour $k = 0$:

$$R^{[s]}(\alpha^j) = \binom{j}{0} R(\alpha^0) = R(1)$$

D'où modulo 2 :

$$\forall 0 < j < \delta \quad R^{[s]}(\alpha^j) + R(1) = 0$$

Ce qui prouve que ce polynôme appartient bien au code. \square

Prenons maintenant un mot de code de poids minimal, disons R .

Quitte à lui appliquer un décalage circulaire, on peut supposer $m_0 \neq 0$.

Ainsi comme le polynôme $R^{[s]}(X)$ a les « mêmes » m_i sauf m_0 on a

$$w(R^{[s]}) = w(R) - 1$$

Si $w(R)$ était pair $w(R) = 2k$ on aurait modulo 2

$$R(1) = \sum m_i = \underbrace{1 + \dots + 1}_{2k \text{ fois}} = 0$$

Et $R(1) + R^{[s]}(X) = R^{[s]}(X)$ serait un mot de code de poids inférieur à celui de R , absurde. \blacksquare

3.3.3 Décodage des codes BCH

On prend toujours $q = 2$, $n = 2^m - 1$ et $\alpha \in K = \mathbb{F}_{2^m}$ une racine primitive n -ième.

On définit Σ comme précédemment avec $\delta = 2t + 1$, et on prend

$$g(X) = \prod_{i \in \Sigma} (X - \alpha^i) \in \mathbb{F}_2[X]$$

Le code C obtenu est constitué des polynômes $R(X) \in \mathbb{F}_2[X]$ de $\deg < n$ multiples de $g(X)$.

☞ Le problème est le suivant : le mot de code R est perturbé par l'erreur E , donnant ainsi lieu au mot erroné $R' = R + E$ et sachant que $w(E) \leq t$, il faut pouvoir retrouver R .

Par définition, R est un multiple de g , donc $\forall i \in \llbracket 1, 2t \rrbracket$, $R(\alpha^i) = 0$.

Définition 3.22 On appelle **syndrome** de R' la suite (S_1, \dots, S_{2t}) donnée par :

$$S_i = R'(\alpha^i) = E(\alpha^i) \in K$$

Par ailleurs l'erreur E a au plus t termes non nuls (donc égaux à 1) car $w(E) \leq t$.

$$E(X) = X^{r_1} + \dots + X^{r_e} \quad \text{avec} \quad 0 \leq r_1 < \dots < r_e < n \quad \text{et} \quad 0 \leq e \leq t$$

Posons pour alléger l'écriture $x_j = \alpha^{r_j} \in K$,

$$S_i = E(\alpha^i) = \sum_{j=1}^e \alpha^{ir_j} = \sum_{j=1}^e (x_j)^i$$

Définition 3.23 On introduit le **polynôme-syndrome** défini par :

$$S(Z) = \sum_{i=1}^{2t} S_i Z^{i-1} \in K[Z]$$

Définition 3.24 On introduit de même le **polynôme-localisateur** :

$$\sigma(Z) = \prod_{j=1}^e (1 - x_j Z) \in K[Z]$$

Principe du décodage

Celui-ci s'effectue en 3 étapes :

- Calcul des $S_i = R'(\alpha^i)$ donc du polynôme-syndrome.
- Calcul du polynôme-localisateur à partir du polynôme-syndrome.
- Calcul des racines du polynôme-localisateur dans K .

-> Le premier point ne pose aucune difficulté, le dernier non plus il suffit simplement de tester les éléments de K . Une fois les racines β_j du polynôme-localisateur trouvées à savoir $x_j \beta_j = 1$, le calcul de leur inverse nous donnera les $x_j = \alpha^{r_j}$ et donc les r_j soit E et enfin R . Le point délicat est donc le second sur lequel nous allons travailler.

Proposition 3.25 Il existe un polynôme $\omega(Z) \in K[Z]$ de degré $< t$ tel que

$$S(Z)\sigma(Z) = \omega(Z) \pmod{Z^{2t}}$$

Preuve : Déroulons les calculs.

$$S(Z) = \sum_{i=1}^{2t} S_i Z^{i-1} = \sum_{i=1}^{2t} \left(\sum_{j=1}^e x_j^i \right) Z^{i-1} = \sum_{i=1}^{2t} x_j \left(\sum_{j=1}^e (x_j Z)^{i-1} \right)$$

On intervertit les deux sommes :

$$S(Z) = \sum_{j=1}^e x_j \left(\sum_{i=1}^{2t} (x_j Z)^{i-1} \right) = \sum_{j=1}^e x_j \frac{1 - (x_j Z)^{2t}}{1 - x_j Z}$$

D'où en multipliant par le polynôme-localisateur :

$$S(Z)\sigma(Z) = \sum_{j=1}^e \left(x_j (1 - x_j^{2t} Z^{2t}) \prod_{k \neq j} (1 - x_k Z) \right)$$

Donc en développant $x_j(1 - x_j^{2t} Z^{2t})$ on obtient modulo Z^{2t} :

$$\omega(Z) = \sum_{j=1}^e x_j \prod_{k \neq j} (1 - x_k Z) = \sigma(Z) \sum_{j=1}^e \frac{x_j}{1 - x_j Z}$$

On voit au passage que $\deg(\omega) < \deg(\sigma) \leq e \leq t$. ■

Lemme 3.26 Soient $(\sigma', \omega') \in K[Z]^2$ avec $\deg(\sigma') \leq t$, $\deg(\omega') < t$ et $S(Z)\sigma'(Z) \equiv \omega'(Z) \pmod{Z^{2t}}$.

$$\exists C \in K[Z] \quad \text{tel que} \quad \sigma'(Z) = C(Z)\sigma(Z) \quad \text{et} \quad \omega'(Z) = C(Z)\omega(Z)$$

Preuve : Redonnons l'expression de $\omega(Z)$:

$$\omega(Z) = \sum_{j=1}^e x_j \prod_{k \neq j} (1 - x_k Z)$$

Les racines de σ sont les x_j^{-1} et aucune n'est racine de ω .

Donc les polynômes σ et ω sont premiers entre eux. Par ailleurs modulo Z^{2t} :

$$\omega(Z)\sigma'(Z) \equiv (S(Z)\sigma(Z))\sigma'(Z) \equiv (S(Z)\sigma'(Z))\sigma(Z) \equiv \omega'(Z)\sigma(Z)$$

Donc le polynôme $\omega(Z)\sigma'(Z) - \omega'(Z)\sigma(Z)$ est divisible par Z^{2t} .

Mais celui-ci est de degré $< 2t$ donc il est nul d'où :

$$\omega(Z)\sigma'(Z) = \omega'(Z)\sigma(Z)$$

Ainsi $\omega(Z) \mid \omega'(Z)\sigma(Z)$ mais $\omega(Z) \wedge \sigma(Z) = 1$ donc d'après Gauss $\omega(Z) \mid \omega'(Z)$:

$$\exists C \in K[Z], \quad \omega'(Z) = C(Z)\omega(Z)$$

Et en reportant dans l'égalité on obtient de même :

$$\sigma'(Z) = C(Z)\sigma(Z)$$

Ce qui achève la démonstration du lemme. ■

Nous donnons maintenant un moyen effectif de calculer $\sigma(Z)$ et $\omega(Z)$.

Pour cela nous utiliserons l'algorithme d'Euclide que nous commençons par présenter.

Proposition 3.27 *Algorithme d'Euclide.* Entrées : a et b , Sortie : $\text{pgcd}(a, b)$.

```

 $R_0 := |a|;$ 
 $R_1 := |b|;$ 
Tant que  $R_1 > 0$  faire
   $R := \text{Reste Division}(R_0, R_1);$ 
   $R_0 := R_1;$ 
   $R_1 := R;$ 
Fin Tant que ;

```

Prouvons la terminaison (arrêt) ainsi que la correction (résultat correct) de cet algorithme.

Notons $D(x, y)$ l'ensemble des diviseurs de x et y .

Les conditions

$$\begin{cases} D(R_0, R_1) = D(a, b) \\ R_1 \geq 0 \end{cases}$$

constituent un invariant de boucle (vérifiées à chaque passage dans la boucle Tant que).

Preuve : Initialement les conditions sont vérifiées car $R_0 = |a|$ et $R_1 = |b|$.

Notons R'_0 et R'_1 les nouvelles valeurs de R_0 et R_1 en sortie d'un tour de boucle.

Nous avons alors :

$$R'_0 = R_1 \quad \text{et} \quad R'_1 = R_0 - QR_1 \quad \text{avec} \quad 0 \leq R'_1 < R_1$$

On voit qu'un diviseur de R_0 et R_1 est un diviseur de R'_0 et R'_1 , et réciproquement. \square

L'algorithme se termine car R_1 décroît strictement à chaque tour de boucle.

A la fin $R_1 = 0$ donc $D(R_0, R_1)$ revient à l'ensemble des diviseurs de R_0 .

D'où $R_0 = \text{pgcd}(a, b) = d$. \blacksquare

Améliorons cet algorithme afin qu'il fournisse U_0 et V_0 tels que $d = aU_0 + bV_0$.

Proposition 3.28 *Algorithme d'Euclide étendu.* Entrées : (a, b) , Sorties : (d, U_0, V_0) .


```

R0 := a; (a ≥ 0)
R1 := b; (b > 0)
U0 := 1; U1 := 0;
V0 := 0; V1 := 1;
Tant que R1 > 0 faire
  Q := Quotient Division(R0, R1);
  R2 := Reste Division(R0, R1);
  U2 := U0 - Q × U1;
  V2 := V0 - Q × V1;
  R0 := R1; R1 := R2;
  U0 := U1; U1 := U2;
  V0 := V1; V1 := V2;
Fin Tant que ;

```

Prouvons la correction de ce nouvel algorithme.

L'algorithme se termine comme précédemment avec $R_1 = 0$ et $R_0 = \text{pgcd}(a, b)$.

Montrons que les conditions

$$\begin{cases} U_0 a + V_0 b = R_0 \\ U_1 a + V_1 b = R_1 \\ R_1 \geq 0 \end{cases}$$

sont invariants de boucle.

Avec les affectations initiales la condition est bien vérifiée.

Comme tout à l'heure notons $R'_0, R'_1, U'_0, U'_1, V'_0$ et V'_1 les nouvelles valeurs.

On a après un passage dans la boucle :

$$\begin{aligned} R_0 &= Q \times R_1 + R_2 \\ U_2 &= U_0 - Q \times U_1 \\ V_2 &= V_0 - Q \times V_1 \end{aligned}$$

Et

$$\begin{aligned} R'_0 &= R_1 & R'_1 &= R_2 = R_0 - Q \times R_1 \\ U'_0 &= U_1 & U'_1 &= U_2 = U_0 - Q \times U_1 \\ V'_0 &= V_1 & V'_1 &= V_2 = V_0 - Q \times V_1 \end{aligned}$$

Si bien que (en utilisant la condition initiale) :

$$U'_0 a + V'_0 b = U_1 a + V_1 b = R_1 = R'_0$$

La première condition est bien réalisée en sortie. De même :

$$U'_1 a + V'_1 b = (U_0 - Q \times U_1) a + (V_0 - Q \times V_1) b = (U_0 a + V_0 b) - Q \times (U_1 a + V_1 b) = R_0 - Q \times R_1 = R_2 = R'_1$$

et la deuxième condition est aussi réalisée.

Puisqu'à la fin $R_0 = \text{pgcd}(a, b)$ on trouve bien $U_0 a + V_0 b = R_0 = \text{pgcd}(a, b)$. ■

Cet algorithme s'applique également à deux polynômes $a = P_0$ et $b = P_1$ où $\deg(P_1) \leq \deg(P_0)$.

A ceci près qu'ici on ne fait pas décroître la valeur de R mais le degré de P .

On peut aussi voir l'algorithme en terme de suites $(R_i) = (P_i)$, (Q_i) , (U_i) et (V_i) :

$$P_{i-1} = P_i Q_i + P_{i+1} \quad \text{avec} \quad \deg(P_{i+1}) < \deg(P_i) \quad \text{donc} \quad \deg(Q_i) = \deg(P_{i-1}) - \deg(P_i)$$

$$U_{i+1} = U_{i-1} - Q_i U_i \quad \text{et} \quad V_{i+1} = V_{i-1} - Q_i V_i$$

avec $U_0 = V_1 = 1$ et $U_1 = V_0 = 0$. Et on possède déjà l'invariant

$$P_i = U_i P_0 + V_i P_1$$

On peut également mettre en évidence l'invariant ci-après :

$$U_i V_{i+1} - U_{i+1} V_i = (-1)^i$$

Cela se prouve par récurrence sur i :

Initialisation : $U_0 V_1 - U_1 V_0 = 1 = (-1)^0$. Supposons la propriété vraie au rang i , alors

$$U_{i+1} V_{i+2} - U_{i+2} V_{i+1} = U_{i+1} (V_i - Q_{i+1} V_{i+1}) - (U_i - Q_{i+1} U_{i+1}) V_{i+1} = U_{i+1} V_i - U_i V_{i+1} = -(-1)^i = (-1)^{i+1}$$

Cet invariant nous donne grâce à Bézout $U_i \wedge V_i = 1$, ce qui nous servira plus tard.

Lemme 3.29 *Pour $i \geq 2$, on a $\deg(V_i) = \deg(P_0) - \deg(P_{i-1})$.*

Preuve : On commence par montrer par récurrence que $\deg(V_i)$ croît strictement.

Initialisation : $V_2 = V_0 - Q_1 V_1 = -Q_1$ et $V_3 = V_1 - Q_2 V_2 = 1 + Q_2 Q_1$ donc $\deg(V_3) > \deg(V_2)$.

Hérédité : Supposons $\deg(V_i) > \deg(V_{i-1})$ donc $\deg(Q_i V_i) > \deg(V_{i-1})$. Ainsi

$$\deg(V_{i-1} - Q_i V_i) > \deg(Q_i V_i) = \deg(Q_i) + \deg(V_i) > \deg(V_i)$$

C'est-à-dire $\deg(V_{i+1}) > \deg(V_i)$. \square

Montrons maintenant par récurrence le lemme.

Initialisation : $V_2 = -Q_1$ donc $\deg(V_2) = \deg(Q_1) = \deg(P_0) - \deg(P_1)$.

Hérédité : Supposons $\deg(V_i) = \deg(P_0) - \deg(P_{i-1})$. On a

$$\deg(P_i) = \deg(P_{i-1}) - \deg(Q_i) = \deg(P_0) - \deg(V_i) - \deg(Q_i) = \deg(P_0) - \deg(Q_i V_i) = \deg(P_0) - \deg(V_{i+1})$$

car $\deg(Q_i V_i) > \deg(V_{i-1})$. Ce qui achève la récurrence. \blacksquare

Executons l'algorithme à partir des polynômes $P_0 = Z^{2t}$ et $P_1 = S$.

On obtient des suites (P_i) , (U_i) et (V_i) avec $\deg(P_i) < \deg(P_{i-1})$ et

$$P_i = U_i Z^{2t} + V_i S \quad \text{donc} \quad S V_i \equiv P_i \pmod{Z^{2t}}$$

Il existe un unique i pour lequel $\deg(P_{i-1}) \geq t$ et $\deg(P_i) < t$.

On a alors d'après

$$\deg(V_i) = \deg(P_0) - \deg(P_{i-1}) \leq 2t - t = t$$

Ainsi les polynômes $\sigma' = V_i$ et $\omega' = P_i$ satisfont aux hypothèses du lemme 3.26.

Il en résulte qu'il existe $C \in K[Z]$ tel que

$$V_i = C\sigma \quad \text{et} \quad P_i = C\omega$$

Par ailleurs on a $S\sigma \equiv \omega \pmod{Z^{2t}}$ donc

$$\exists A \in K[Z], \quad \omega - S\sigma = AZ^{2t}$$

Multiplions cette égalité par C :

$$C\omega - S(C\sigma) = (CA)Z^{2t}$$

Et comme $C\omega = P_i$ et $C\sigma = B_i$ il vient

$$P_i - SV_i = (CA)Z^{2t} \iff P_i = (CA)Z^{2t} + V_iS$$

Or $P_i = U_iZ^{2t} + V_iS$ donc on en déduit

$$U_i = CA$$

Ainsi le polynôme C divise à la fois U_i et V_i .

Mais comme on a vu que $U_i \wedge V_i = 1$ alors le polynôme C est constant.

Enfin comme $\sigma(0) = 1$ on a $C = U_i(0)$. D'où la proposition :

Proposition 3.30 *Avec les notations précédentes, on a :*

$$U_i(0) \neq 0, \quad \sigma(Z) = \frac{U_i(Z)}{U_i(0)}, \quad \omega(Z) = \frac{P_i(Z)}{U_i(0)}$$

Remarque : En pratique on ne divisera pas par $U_i(0)$ car seules les racines de σ nous intéressent.

Bibliographie

- [Chi] L. Childs, *A concrete introduction to higher algebra*, Springer Verlag, 1979.
- [Dem] M. Demazure, *Cours d'algèbre*, Cassini, 1997.
- [Esc] J-P. Escofier, *Théorie de galois*, Dunod, 1997.
- [Pau] A. Paugam, *Questions délicates en algèbre et géométrie*, Dunod, 2007.