TER : DES CORPS FINIS AUX CODES CORRECTEURS D'ERREURS

Salim Irzoudine

Semestre 2

Table des matières

1 Préliminaires algébriques

1.1 Définition : Caractéristique

.
Soit $\mathbb{K}$ un corps, on appelle caractéristique de $\mathbb{K}$ (et on le note car($\mathbb{K}$)), le plus petit entier naturel p$\neq$0, tel que : $\forall x \in \mathbb{K} : p.x = 0_K$

1.2 Proposition : Caractéristique

Soit $\mathbb{K}$ un corps et **a** sa caractéristique :
- Si $a = 0$ alors $\mathbb{K}$ est infini.
- Si $a \neq 0$, alors a est premier.

Preuve :

Soit $\mathbb{K}$ un corps, considérons l'application :

$$\varphi : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{K} \\ \text{n} \longmapsto n.1_{\mathbb{K}} \end{cases}$$

L'application est un homomorphisme d'anneau unitaire. Alors $ker(\varphi)$ est un idéal de l'anneau $\mathbb{Z}$, or les seuls les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, où $a \geq 0$.
$ker(\varphi)= \{n \in \mathbb{Z}/n.1_{\mathbb{K}}= 0_{\mathbb{K}}\}$ est un ideal de $\mathbb{Z}$, donc :
$\exists\ a \geq 0$ tel que : $ker(\varphi) = a\mathbb{Z}$.
$\forall z \in ker(\varphi)$, si $z \geq 0$ alors $\exists k \in \mathbb{Z}^*$ tel que $z = ak$, donc $z \geq a$.
Donc a est le plus petit entier naturel tel que :
$ax = 0_{\mathbb{K}}, \forall x \in \mathbb{K}$, donc a est la caractéristique de $\mathbb{K}$.
- $a = 0$ alors φ injective. Dans ce cas $\mathbb{Z} \hookrightarrow \mathbb{K}$ et donc $\mathbb{K}$ est infini.
- Si $a \neq 0$, $ker(\varphi)$ est un idéal premier de $\mathbb{Z}$ car $\mathbb{Z}$ est integre, donc a est premier car les idéaux de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$ avec a premier.

1.3 Définition et Proposition : Sous corps premier

On appelle sous corps premier d'un corps $\mathbb{K}$, le plus petit corps inclus dans $\mathbb{K}$ et contenant $1_{\mathbb{K}}$.
- $car(\mathbb{K}) = 0$, le corps premier de $\mathbb{K}$ est $\mathbb{Q}$.
- Si $car(\mathbb{K}) = p$, le sous corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Preuve :
- $car(\mathbb{K}) = 0$, si et seulement si φ injective. (Prop 1.2), donc $\mathbb{Z} \hookrightarrow \mathbb{K}$.

Or $\mathbb{K}$ est un corps, s'il contient $\mathbb{Z}$,il contient le plus petit corps qui contient $\mathbb{Z}$ qui est $\mathbb{Q}$ ($\mathbb{Q}$ est le plus petit corps de caractéristique 0).
- De même dans un corps de caractéristique p, $p.1 = 0$ de tel sorte que $\mathbb{Z}/p\mathbb{Z}$ est sous corps premier de tout corps de caractéristique p.

{théorème d'isomorphisme}

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad\varphi\quad} & \mathbb{K} \\ & \searrow \quad \nearrow \bar{\varphi} & \\ & \text{Z— ker } \varphi & \end{array}$$

$\overline{\varphi}$ est injective (1^{er} théorème d'isomorphisme), $ker(\varphi) = p\mathbb{Z}$ p premier, donc $\mathbb{Z}/p\mathbb{Z}$ est contenu dans $\mathbb{K}$.

2 Extension de corps, Corps de décomposition, Clôture algébrique

2.1 Proposition : Division euclidienne

Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau euclidien :
$\forall A, B, \exists!(Q, R)$ tel que :
$A = BQ + R$ avec $deg(R) < deg(B)$ ou $R = 0$.

2.2 Définition et Proposition : Extension de corps

Soient $\mathbb{K}, \mathbb{L}$ deux corps. S'il existe un homomorphisme d'anneau unitaire ϕ : $\mathbb{K} \longrightarrow \mathbb{L}$, alors il est injectif et est appelé plongement de $\mathbb{K}$ dans $\mathbb{L}$.
On dit que $\mathbb{L}$ est une extension de $\mathbb{K}$.

2.3 Proposition :

Si $\mathbb{K} \subset \mathbb{L}$,$\mathbb{K}$ et $\mathbb{L}$ sont des corps, alors on peut munir $\mathbb{L}$ d'une structure de $\mathbb{K}$-espace vectoriel.
Preuve : $\mathbb{L}$ est un corps donc un groupe additif, de plus on munit $\mathbb{L}$ de la multiplication externe par :

$$\begin{cases} \mathbb{K} \times \mathbb{L} \longrightarrow \mathbb{L} \\ (\lambda, x) \longmapsto \lambda.x \end{cases}$$

vérifiant : $\forall\ (x, y) \in \mathbb{L}^2$, $\forall (\lambda, \mu) \in \mathbb{K}^2$, on a :
- $1.x = x$ où 1 est l'élément neutre pour la multiplication de $\mathbb{K}$.
- $(\lambda + \mu).x = \lambda.x + \mu.x$
- $\lambda.(x + y) = \lambda.x + \mu.y$
- $\lambda.(\mu.x) = (\lambda\mu).x$

Donc $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.

2.4 Définition : Extension finie, degré d'extension

Si $\mathbb{K} \subset \mathbb{L}$, on dit que $\mathbb{L}$ est une extension finie de $\mathbb{K}$ si la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel est finie. Cette dimension est appelé degré d'extension de $\mathbb{L}$ et se note $[\mathbb{L} : \mathbb{K}]$.

2.5 Définition : Corps de décomposition

Soit $P \in \mathbb{K}[X]$ un polynôme non constant, un corps de décomposition de P est une extension $\mathbb{L}$ tel que :
— P est scindé dans $\mathbb{L}[X]$:
$P(X) = c(X - \xi_1)...(X - \xi_d), c, \xi_1, ..., \xi_d \in \mathbb{L}$.
— $\mathbb{L} = \mathbb{K}[\xi_1, ..., \xi_d]$.

2.6 Proposition : Prolongement d'isomorphisme

Soit $P = \sum a_i X^i \in \mathbb{K}[X]$,un polynôme irréductible avec $a_i \in \mathbb{K}$.
Soit $P^\sigma = \sum \sigma(a_i) X^i \in \mathbb{K}'[X]$. Soit $\sigma : \mathbb{K} \longrightarrow \mathbb{K}'$ un isomorphisme de corps. Alors P^σ est irréductible. Si α, α' sont des racines de P, P^σ dans des extensions de $\mathbb{K}, \mathbb{K}'$, alors σ se prolonge en un isomorphisme $\mathbb{K}_(\alpha) \simeq \mathbb{K}'(\alpha')$ qui envoie α sur α'.
Preuve :
$\forall P \in \mathbb{K}[X]$, on a :
$\sigma(P) = \sigma(a_0 + a_1 X + ... + a_n X^n) = \sigma(a_0) + \sigma(a_1)X + ... + \sigma(a_n)X^n$
Il est clair que σ est un morphisme d'anneau :
$\forall P, P' \in \mathbb{K}$,

— $\sigma(P + P') = \sigma((a_0 + a'_0) + (a_1 + a'_1)X + ... + (a_n + a'_n)X^n)$
$= \sigma(a_0 + a'_0) + \sigma(a_1 + a'_1)X + ... + \sigma(a_n + a'_n)X^n$
$=(\sigma(a_0) + \sigma(a_1)X + ... + \sigma(a_n)X^n) + (\sigma(a'_0) + \sigma(a'_1)X + ... + \sigma(a'_n)X^n)$
$= \sigma(P) + \sigma(P')$
— $\sigma(PP') = \sigma(P)\sigma(P')$
— $\sigma(1) = 1$
σ est injective, car si on a :
$\sigma(a_0 + a_1 X + ... + a_n X^n) = 0$
Alors $\sigma(a_i) = 0$ pour $i = \{1, ..., n\}$. Il en résulte $a_i = 0$ pour $i = \{1, ..., n\}$ et $P = 0$.
Comme $\mathbb{K}'$ est finie, alors σ est bijective.

2.7 Définition : Corps de rupture

Soit P un polynôme sur le corps $\mathbb{K}$, irréductible sur $\mathbb{K}$. On appelle corps de rupture de P sur $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :
— Dans $\mathbb{L}$, P admet une racine
— $\mathbb{L}$ est engendré par $\mathbb{K}$ et α : $\mathbb{L} = \mathbb{K}(\alpha)$.
On a $\mathbb{K}[X]/(P) = \mathbb{L}$. Comme P est irreductible, (P) est maximal dans $\mathbb{K}[X]$ et donc $\mathbb{L}$ est bien un corps.

Existence du corps de rupture :

Dans un corps à $q = 2^2$ éléments :
Soit le polynôme $P = 1 + X + X^2 \in \mathbb{F}_2[X]$. P est irréductible dans $\mathbb{F}_2[X]$, car

sinon P admet un facteur de degré 1 et donc une racine dans $\mathbb{F}_2$.
Or $P(0) = 1 = P(1) = 1 + 1 + 1$, donc P n'a pas de racine et donc P est irréductible dans $\mathbb{F}_2$.
Comme P est irréductible, son corps de rupture est donné par :
$\mathbb{F}_2[X]/(1 + X + X^2)$.

2.8 Proposition : Existence et unicité du corps de décomposition

Tout polynôme non nul P $\mathbb{K}[X]$ possède un corps de décomposition, unique à isomorphisme près.

Preuve :

Existence :
On procède par récurrence sur le degré de P pour montrer l'existence $n = degP$.
Initialisation : Si $n = 1$, alors $P = aX + b = a(X - \frac{b}{a})$ et $\mathbb{K}$ est un corps de décomposition de P.
Hérédité : $n = 2$. supposons que l'hypothèse de récurrence vrai pour tout corps et tout polynôme de degré $< n$, et soit $P \in \mathbb{K}[X]$ de degré ¡ n. Soit S un facteur irréductible de P et soit $k_1 = k(\alpha)$ un corps de rupture de S.Alors dans $k_1[X]$, on a $P = (X - \alpha)Q$, où $Q \in k_1[X]$(division euclidienne dans $k_1[X]$) de degré $n - 1$. Par hypothèse de récurrence, il existe une extension $\mathbb{L}$ dans laquelle Q a des racines $\alpha_1, ..., \alpha_n$ et telle que $K = k_1(\alpha_1, ..., \alpha_n)$. Alors $\alpha_1, ..., \alpha_n$ sont des racines de P dans $\mathbb{K}$ et $\mathbb{L}$ est engendré sur $\mathbb{K}$ par ces éléments. Q admet un corps de décomposition $k_1(\alpha_2, ..., \alpha_{n-1}) = k(\alpha)(\alpha_2, ..., \alpha_{n-1}) = k(\alpha_1, ..., \alpha_{n-1})$.

Unicité du corps de décomposition :

Soit $P \in \mathbb{K}[X]$. Soit $\mathbb{E} \supseteq \mathbb{K}$ un corps ou P est scindé : $P = c(X - \alpha_1)...(X - \alpha_n)$.
Soit $\mathbb{E}' \supseteq \mathbb{K}$ un corps ou P^σ est scindé : $P = c'(X - \alpha'_1)...(X - \alpha'_n)$. On veut montrer que $B = \mathbb{K}(\alpha_1, ..., \alpha_n) \simeq \mathbb{K}(\alpha'_1, ..., \alpha'_n)$.
On applique le résultat de prolongement de la proposition (2.6) par récurrence sur n.
n=1 : Id : $\mathbb{K} \longrightarrow \mathbb{K}$, on prolonge à $\mathbb{K}(\alpha_1) \longrightarrow \mathbb{K}(\alpha'_1)$.
Hérédité : On suppose qu'il existe un entier tel que :
$\sigma : \mathbb{K}(\alpha_1, ..., \alpha_{n-1}) \longrightarrow \mathbb{K}(\alpha'_1, ..., \alpha'_n)$ est vraie.
On applique la proposition (2.6)
$B \simeq B'$.

2.9 Définition et Proposition : Corps algébriquement clos

Soit $\mathbb{K}$ un corps. Les propriétés suivantes sont équivalentes :
— Tout polynôme $P(X) \in \mathbb{K}$[X] non constant a au moins une racine dans $\mathbb{K}$.
— Les seuls polynômes irréductible de $\mathbb{K}$[X] sont les ceux de degré 1.
— Tout polynôme P(X) $\in \mathbb{K}$[X] non constant est scindé.

Si ces conditions sont vérifiées, alors $\mathbb{K}$ est algébriquement clos.

2.10 Définition : élément algébrique

Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$ et $\xi \in \mathbb{L}$. On dit que ξ est algébrique sur $\mathbb{K}$ s'il existe un polynôme non nul $P \in \mathbb{K}$ avec $P(\xi) = 0$.

2.11 Définition : Polynôme minimal

Si ξ est algébrique sur $\mathbb{K}$, alors il existe un unique polynôme irréductible sur $\mathbb{K}$ tel que : $P_\xi(\xi) = 0$. On l'appelle polynôme minimal sur $\mathbb{K}$.

2.12 Définition : Extension algébrique

Soit $\mathbb{L}$ un extension de $\mathbb{K}$. On dit que $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$ si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

2.13 Définition : Clôture algébrique

Soient $\mathbb{K}$ un corps et $\overline{\mathbb{K}}$ une extension de $\mathbb{K}$. On dit que $\overline{\mathbb{K}}$ est une clôture algébrique de $\mathbb{K}$ si $\overline{\mathbb{K}}$ est algébriquement clos et est une extension algébrique de $\mathbb{K}$.

2.14 Théorème :

Soient $\mathbb{L}$ une extension du corps $\mathbb{K}$ et $\xi \in \mathbb{L}$. Les propriétés suivantes sont équivalentes :

1. ξ est algébrique sur $\mathbb{K}$
2. $\mathbb{K}[\xi]$ est un espace vectoriel de dimension finie sur K
3. $\mathbb{K}[\xi]$ est un sous-corps de $\mathbb{L}$

$$\varphi : \begin{cases} \mathbb{K}[X] \longrightarrow \mathbb{K}[\xi] \subset \mathbb{L} \\ \text{P(X)} \longmapsto P(\xi) \end{cases}$$

De plus, si ces propriétés sont vérifiées, alors $\{1,\xi,...,\xi^{deg(\xi-1)}\}$ est une base de l'espace vectoriel. $\mathbb{K}[\xi]$ sur $\mathbb{K}$ et $[\mathbb{K}[\xi] : \mathbb{K}\,]$=deg$(P_\xi)$

Preuve :
1)⇒2) : Soit $x \in \mathbb{K}[\xi]$. Il existe $P(X) \in \mathbb{K}[X]$ avec $P(\xi) = x$. Soient $Q[X]$ et $R[X]$ le reste de la division et le quotient de la division euclidienne de $P(X)$ par $P_\xi(X)$.
On a : $x = P(\xi) = Q(\xi)P(\xi) + R(\xi) = R(\xi)$
De plus, $R = 0$ ou deg$(R) \leq$ deg $(P_\xi) = d$ et on peut donc écrire :
R(X) $= a_0 + a_1 + ... + a_{d-1}X^{d-1}$ avec $a_0, ..., a_{d-1} \in \mathbb{K}$ et x $= a_0\xi + ... + a_{d-1}\xi^{d-1}$.
Ainsi, x est une combinaison linéaire a coefficients dans $\mathbb{K}$ des éléments $\{1, \xi, ..., \xi^{d-1}\}$ et $\{1, \xi, ..., \xi^{d-1}\}$ est un système générateur de $\mathbb{K}[\xi]$. Supposons que ξ est algébrique

de degré d. Si $a_0, a_1, ..., a_{d-1} \in \mathbb{K}$ vérifient $a_0 + a_1\xi + ... + a_{d-1}\xi^{d-1}$, alors le polynôme $P(X) = a_0 + ... + a_{d-1}X^{d-1}$ admet ξ pour racine et il est donc un multiple du polynôme minimal P_ξ.
Comme $deg(P_\xi) =$ et que $deg(P) < 0$
On a $P(X) = 0$,
Donc $a_0 = a_1 = ... = a_{d-1} = 0$,
Donc 1, $\xi, ..., \xi^{d-1}$ est une base de $\mathbb{K}[\xi]$.
2)⇒3) : Supposons que $\mathbb{K}[\xi]$ est un espace vectoriel de dimension finie sur $\mathbb{K}$, énonçons le lemme suivant avant de démontrer la propriété

Lemme Soit A un sous-anneau de $\mathbb{L}$ contenant $\mathbb{K}$. Si A est un espace vectoriel de dimension finie sur $\mathbb{K}$ alors A est un corps.

Preuve : Soit $a \in A$, $a \neq 0$. On va montrer qu'alors a est inversible :
Pour tout x $\in A$, on a : $ax \in A$. On considère l'application $f_a : x \longmapsto ax$ de A dans A qui est linéaire. Donc, $\forall\ x, y \in A$ alors :
$f_a(\lambda x + \mu y) = a(\lambda x + \mu y) = \lambda f_a(x) + \mu f_a(y)$, avec $\lambda, \mu \in \mathbb{K}$
On montre que f_a est injective :
$f_a(x) = 0 \Longleftrightarrow ax = 0$, or A est un anneau integre en tant que sous-anneau du corps $\mathbb{L}$, donc $x = 0$. Donc f_a est injective, donc bijective car $\dim(A)$ est finie.
Donc il existe $x \in A$ tel que $ax = f_a(x) = 1$, donc $x = a^{-1} \in A$.
Donc A est un corps.
Par le Lemme on a **2)** $\Longrightarrow$ **3)**
3) $\Longrightarrow$ **1) :** Si $\xi = 0$ alors $\xi \in \mathbb{K}$ est algébrique. Supposons que $\xi \neq 0$.
Comme $\xi \in \mathbb{K}[\xi]$ un corps donc $\xi^{-1} \in \mathbb{K}[\xi]$ et il existe Q $\in \mathbb{K}[X]$ tel que
$\xi^{-1} =$ Q[ξ]
Posons P(X) = XQ(X) - 1 $\in \mathbb{K}[X]$
P(X) $\neq 0$ et ξ est une racine de P(X).
Donc ξ est algébrique sur $\mathbb{K}$.

2.15 Théorème :

Tout extension finie est algébrique.

Preuve :
Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension de $\mathbb{K}$ et $\xi \in \mathbb{L}$
On a : $\mathbb{K}[\xi]$ est un espace vectoriel fini de $\mathbb{K}$ (car $\xi \in \mathbb{L}$ est une extension finie)
Donc par le théorème on a : ξ est algébrique.
Donc $\mathbb{L}$ est une extension algébrique.

3 Indicatrice d'Euler

3.1 Définition :

Soit un entier $n > 1$.
On appelle indicatrice d'Euler de n l'entier $\varphi(n)$ défini par :
$\varphi(n) = \text{card } \{1 \leq k \leq \text{n tel que } k \wedge\ n = 1\}$ ou $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Calcul :

1. Soit un entier $n > 1$.
   On appelle indicatrice d'Euler de n l'entier $\varphi(n)$ défini par :
   $\varphi(n) = \text{card } \{1 \leq k \leq \text{n tel que } k \wedge\ n = 1\}$ ou $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.
   Calcul :
   (a) Si p premier on a :
   $\varphi(p) = \text{card } \{1 \leq k \leq p : k \wedge p = 1\} = p - 1$
   Pour $\alpha \geq 1$ on a :

$$\begin{aligned}\varphi(p^\alpha) &= card\{1 \leq k \leq p^\alpha; k \wedge p^\alpha = 1\} \\ &= card\{1 \leq k \leq p^\alpha; pk\} \\ &= p^\alpha - card\{1 \leq k \leq p^\alpha; p|k\} \\ &= p^\alpha - card\{pl; 1 \leq pl \leq p^\alpha\}.\end{aligned}$$

   Donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

   (b) si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m) \times \varphi(n)$.

   Théorème Chinois : Soient $m, n \in \mathbb{N}^*$ et $m \wedge n = 1$ alors :
   $\mathbb{Z}|n\mathbb{Z} \times \mathbb{Z}|m\mathbb{Z} \cong \mathbb{Z}|nm\mathbb{Z}$
   Donc $((\mathbb{Z}|n\mathbb{Z} \times \mathbb{Z}|m\mathbb{Z})^*, \times) \cong ((\mathbb{Z}|nm\mathbb{Z})^*, \times)$
   Donc on a $(\mathbb{Z}|n\mathbb{Z})^* \times (\mathbb{Z}|m\mathbb{Z})^* \cong (\mathbb{Z}|nm\mathbb{Z})^*$
   Donc $|(\mathbb{Z}|n\mathbb{Z})^* \times (\mathbb{Z}|m\mathbb{Z})^*| = |(\mathbb{Z}|nm\mathbb{Z})^*, \times)|$.
   Donc $\varphi(n)\varphi(m) = \varphi(nm)$.
   (c) Si $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$ avec $p_i \wedge p_j = 1$ en utilisant 1 et 2 par récurrence sur r on a :
   $\varphi(n) = \prod_{i=1}^{n} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.

3.2 Proposition : Cardinal de $(\mathbb{Z}/d\mathbb{Z})^*$

On a : $\varphi(d) = |(\mathbb{Z}/d\mathbb{Z})^*| = card\{$élément d'ordre d de (Z/dZ)$^*\}$.

3.3 Théorème : Formule de Möbius

Soit un entier $n > 1$. Soit $\varphi(n)$ est d'indicatrice d'Euler de n. On a :
$n = \sum_{d/n} \varphi(d)$

Preuve :
Soit $\overline{x} = \frac{\overline{n}}{d} \in \mathbb{Z}/n\mathbb{Z}$, on a $d\overline{x} = \overline{n} = \overline{0}$, donc si on pose $k = o(n)$, on a $k|d$.
On a $k\overline{x} = \overline{0} = \overline{n}$
donc $\exists\ k'$ tel que $kx = k'n$
donc $\frac{kn}{d} = k'n$
donc $k = k'd$,
donc $d|k$.
Donc $d = k$.
Donc $\overline{x}$ est d'ordre d.
Donc $< \overline{x} >$ est un groupe cyclique d'ordre d qui est donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$.
Il admet donc exactement $\varphi(d)$ générateurs qui sont donc des éléments d'ordre d.
Soit $\overline{y}$ un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$, alors $d\overline{y} = \overline{0}$, donc $\exists\ k'$ tel que :
$dy = k'n$
donc $y = k'\frac{n}{d} = k'x$
donc $y \in < x >$.
Donc les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les éléments d'ordre d de $< x >$, il y en a donc exactement $\varphi(d)$.
Donc en utilisant $\mathbb{Z}/n\mathbb{Z} = \bigsqcup\{x \in \mathbb{Z}/n\mathbb{Z},\ o(x) = d\}$.
On a donc $n = \sum \varphi(d)$.

4 Polynôme cyclotomique dans $\mathbb{C}$

4.1 Définition : racine primitive de l'unité

Pour un entier naturel non nul n donné. On appelle racine n-ième de l'unité toute solution de l'équation $X^n - 1 = 0$.
Une racine n-ième de l'unité est dite primitive quand elle est d'ordre exactement n.
Soit $n \in \mathbb{N}^*$. En général dans $\mathbb{K}$, on note P_n l'ensemble des racines primitives n-ième de l'unité :

$$\begin{aligned} P_n &= \{x \in \mathbb{K}^*, ordre(x) = n\} \\ &= \{x \in \mathbb{K}^*, x^n = 1 et x^m \neq 1 \forall, m < n\}. \\ &= \{e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n, k \wedge n = 1\} \end{aligned}$$

4.2 Définition : Polynôme cyclotomique dans $\mathbb{C}$:

Soit $n \in \mathbb{N}^*$. On appelle n-ième polynôme cyclotomique les polynômes dans $\mathbb{C}$
$\Phi_n(X) = \prod_{\xi \in P_n} (X - \xi) = \prod_{k \in \mathbb{Z}/n\mathbb{Z}, k \wedge n = 1} (X - e^{\frac{2ik\pi}{n}})$

4.3 Lemme de Gauss :

Le contenu d'un polynôme P est le pgcd de ses coefficients. On note $c(P)$
Dans $\mathbb{R}[X]$, soient P et Q deux polynômes à une variable à coefficients dans $\mathbb{R}[X]$. Alors
$c(P.Q) = c(P).c(Q)$.
Preuve : On peut écrire :

$$P[X] = a_0 + ... + a_n X^n, a_i \in \mathbb{R}$$
$$Q[X] = b_0 + ... + b_n X^n, b_j \in \mathbb{R}$$

Soit $a' = c(P)$ et $b' = c(Q)$
On a $a' \times b' = c(P) \times c(Q)$
On a $PQ = \prod_{i,j=(0...n)} a_i b_j X^{i+j}$
Donc $c(PQ) = a' \times b' = c(P) \times c(Q)$

4.4 Lemme :

Si P,Q deux polynômes, il ne sont pas premier entre eux dans $\mathbb{C}[X]$. On a aussi qu'il ne sont pas premier entre eux dans $\mathbb{Q}[X]$.

Preuve :
Soit $P, Q \in \mathbb{Q}[X]$, si P et Q sont premier entre eux dans $\mathbb{Q}[X]$, ils sont aussi premier entre eux dans $\mathbb{C}[X]$. Par Bezout, il existe u,v $\in \mathbb{Q}[X]$ tel que $uP+vQ = 1$, donc u,v $\in \mathbb{C}[X]$. Donc P(X) et Q(X) sont premier entre eux dans $\mathbb{C}[X]$ par le théorème de bezout.

4.5 Théorème de la division euclidienne des polynômes :

Soit $\mathbb{K}$ un corps commutatif.
Soient A et B deux polynômes à coefficients dans $\mathbb{K}$, avec B non nul, il existe un unique coupe (Q,R) tel que A = BQ + R et deg(R)>deg(B)

4.6 Proposition : Φ_n unitaire et irréductible

Φ_n est un polynôme unitaire à coefficient entier, de degré $\varphi(n)$. De plus il est irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$ On a : X^n - 1 = $\prod_{d/n} \Phi_d(X)$

Preuve :
On note $\mathbb{U}_n = \{e^{\frac{2ik\pi}{n}}\} = \dot{\cup}_{d|n} P_d = \dot{\cup}_{d|n} \{ \xi : d^o(\xi) = d\}$

On voit que $\mathbb{U}_n =< e^{\frac{2i\pi}{n}} >$.
Donc $\mathbb{U}_n$ est cyclique et $|\mathbb{U}_n| = n = |\{1, e^{\frac{2i\pi}{n}}, ..., e^{\frac{2i(n-1)\pi}{n}}\}|$

1. On va montre que degré de Φ_n égal $\varphi(n)$:
   Par définition 4.2 :
   On a : degré de Φ_n égal cardinal de P_n
   Donc degré de Φ_n égal nombre de k tel que :
   $$\bar{k} \in \mathbb{Z}|n\mathbb{Z} \text{ et } k \wedge n = 1$$
   Donc $d^o(\Phi_n) = card\{1 \leq k \leq n, k \wedge n = 1\}$ et Φ_n est unitaire (car Φ_n est produit des polynômes unitaires)

2. Montrons maintenat que $\Phi_n \in \mathbb{Z}[X]$

a. D'abord, on va montre que : $X^n - 1 = \prod_{d|n} \Phi_d(X)$

i) On montre $X^n - 1$ disvise $\prod_{d|n} \Phi_d(X)$

Soit $P = X^n - 1 \in \mathbb{C}[X]$ donc $P' = nX^{n-1}$
On a $P + \frac{X}{n}P' = X^n - 1 - \frac{X}{n}(nX^{n-1}) = -1$
On a la seul racine de P' est 0 mais $P(0) = -1$
Donc P n'a que de racine simple.
Donc on peut écrit : $P(X) = \prod_{i=1}^{n}(X - \alpha_i)$ avec $\alpha_i \neq \alpha_j$

Soit a un racine n_{ieme} de l'unité.
Donc a $\in \mathbb{U}_n =< e^{\frac{2i\pi}{n}} >$ donc $a^n = 1$
Supposons que d'order a est d ($d \in \mathbb{N}^*$)
On a $a^d = 1$ donc $d|n$
Cette égalité faite de a est une racine d_{ieme} de l'unité donc $a \in \mathbb{U}_d$.
Comme d'order de a égal $|\mathbb{U}_d|$ et $\mathbb{U}_d$ est cyclique.
Donc $\Phi_d(a) = 0$.
Donc a est une racine du produit $\prod_{d|n} \Phi_d(X)$
Donc $X^n - 1$ disvise $\prod_{d|n} \Phi_d(X)$

ii) On va cherche degré de $\prod_{d|n} \Phi_d(X)$.

On a
$$\begin{aligned} deg(\prod_{d|n} \Phi_d(X)) &= \sum_{d|n} deg(\Phi_d(X)) \\ &= \sum_{d|n} \varphi(d) \\ &= n \end{aligned}$$

Donc $\exists c \in \mathbb{C}$ telle que $X^n - 1 = c \times \prod_{d|n} \Phi_d(X)$
Or nos deux polynôme sont unitaire donc $c = 1$
Donc $X^n - 1 = c \times \prod_{d|n} \Phi_d(X)$

b. On va montre que $\Phi_n \in \mathbb{Z}[X]$
Par recurrence sur $n \in \mathbb{N}^*$:
Pour $n = 1$ on a : $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ unitaire.
Suppposons que résultat vrai jusqu'au rang $(n-1)$ et montrons le au rang n.
Par hypothèse de récurrence on a : $\forall d \neq n : \Phi_d \in \mathbb{Z}[X]$
Par ailleur on a : $X^n - 1 = \Phi_n \times \prod_{d|n, d\neq n} \Phi_d$
Comme $\prod_{d|n,d\neq n} \Phi_d$ est unitaire.
On peut faire le division euclidienne dans $\mathbb{Z}[X]$, on a donc :

$$X^n - 1 = \prod_{d|n,d\neq n} \Phi_d \times Q + R$$

avec $Q, R \in \mathbb{Z}[X]$ et $deg(R) < deg(\prod_{d|n,d\neq n} \Phi_d)$
Or c'est le même division que dans $\mathbb{C}[X]$.
Donc $Q = \Phi_n$ et $R = 0$. Ainsi, comme $Q \in \mathbb{Z}[X]$ et unitaire.
Donc on a $\Phi_n \in \mathbb{Z}[X]$.

3. Montrons maintenant que les polynômes cyclotimique sont irréductibles
Soit α la premier de racine primitive n_{ieme} d'unité.
C'est à dire $\alpha = e^{\frac{2i\pi}{n}}$ et $\alpha^p (p \wedge n = 1)$ est racine primitive n_{ieme} d'unité.
On note $F_1[X]$ est le polynôme minimal de α.
est note $F_p[X]$ est le polynôme minimal de α^p.

a. Montrons que $F_1[X]$ et $F_p[X]$ sont dans $\mathbb{Z}[X]$ et divisent Φ_n :

On utilise le caractere factoriel de $\mathbb{Z}[X]$.
On peut écrire : $\Phi_n = \prod_i A_i^{\alpha_i}$
Où les (A_i) sont irréductibles sur $\mathbb{Z}$ et unitaire (car Φ_n est unitaire)
On a : $\Phi_n(\alpha) = \Phi_n(\alpha^p) = 0$ car ce sont des racines n_{ieme} de l'unite.
Donc il existe i_0 et i_1 telle que :

$$A_{i_0}(\alpha) \text{ et } A_{i_1}(\alpha^p) = 0$$

Or comme les polynômes A_{i_0}, A_{i_1} est irréductible unitaire dans $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, on a :
$F_1 = A_{i_0} \in \mathbb{Z}[X]$ et $F_p = A_{i_1} \in \mathbb{Z}[X]$. Par definition de A_i donc : $F_1 | \Phi_n$ et $F_p | \Phi_n$ dans $\mathbb{Z}[X]$.

b. Monstrons que $F_1 = F_p$

Par l'absurde, on suppose que $F_1 \neq F_p$.
On sait que F_1, F_p irréductible dans $\mathbb{Z}[X]$.
On a donc :

$$F_1 F_p | \Phi_n \text{ dans } \mathbb{Z}[X].$$

et $F_p(\alpha^p) = 0$.
Donc α est une solution de $F_P(X^p)$.

Donc $F_1|F_p(X^p)$ dans $\mathbb{Z}[X]$.

Posons $\bar{\mathbb{P}}[X]$ est une apptication :

$$\begin{cases} \mathbb{Z}[X] \longrightarrow \mathbb{Z}|p\mathbb{Z} \\ \mathbb{P}[X] \longmapsto \bar{\mathbb{P}}[X] \end{cases}$$

On en déduire que $\bar{F_1}(X)|\bar{F_p}(X^p) = \bar{F_p}(X)^p$.
Ceci étant, soit $\bar{\mathbb{P}} \in \mathbb{Z}|n\mathbb{Z}[X]$ un facteur irréductible de $\bar{F_1}$ dans $\mathbb{Z}|n\mathbb{Z}[X]$.
On a : $\bar{\mathbb{P}}|\bar{F_p}(X^p)$ donc $\bar{\mathbb{P}}|\bar{F_p}(X)$
Par conséquent si $p \neq 1$ on voir que $\bar{\mathbb{P}}^2|\bar{\Phi_n} = \bar{F_1}...\bar{F_n}$.
Puis $\bar{\mathbb{P}}^2|\overline{X^n - 1}$ dans $\mathbb{Z}|p\mathbb{Z}[X]$. (1)
Donc existe $B \in F_p(X)$ tq $\overline{X^n - 1} = \mathbb{P}^2 B$
En dérivant, on trouve :

$$\overline{nX^{n-1}} = \mathbb{P} \times (2\mathbb{P}'B + \mathbb{P}B')$$

Ainsi on a : $\bar{\mathbb{P}}|\overline{nX^{n-1}}$ dans $\mathbb{Z}|n\mathbb{Z}[X]$. (2)
Par (1) et (2) on a :

$$\bar{\mathbb{P}}|\overline{nX^n} \text{ et } \bar{\mathbb{P}}|\overline{nX^n - n}$$

Donc $\bar{\mathbb{P}}|\bar{n}$ avec $n \neq 0$ et $p \wedge n = 1$. Donc $\mathbb{P}$ est une constant. Donc $F_1 = F_p$

c. Montrons que tous racines n_{ieme} primitives l'unité sont racines de F_1.

On note P_n est l'ensemble des racines primitives n_{ieme} de l'unité.

$$P_n = \{e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n-1, k \wedge n = 1\}$$

Soit $\alpha_i \in P_n$ et $i \wedge n = 1$, $0 \leq i \leq n-1$

- si $i = p$ premier :
  On a $F_p = F_1$ donc $F_p(\alpha^p) = F_1(\alpha^p) = 0$ (par b)
  Donc α^p est racine de $F_1(X)$
- si $i = p_1 p_2 ... p_s$ avec p_j premier. Donc par récurrence sur s on a :
  Pour $s = 1$ on a $F_1(\alpha^{p_1}) = 0$ (car point avant)
  Supposons le résultat vrai au rang $s-1$. Et montrons le au rang s :
  Comme $i \wedge n = 1$ on a $p_1, ..., p_{s-1} \wedge n = 1$.
  Donc d'après l'hypothèse de recurrence : $F_1(\alpha^{p_1 \cdots p_{s-1}}) = 0$
  Or $p_s \wedge n = 1$
  Donc :

$$F_1[(\alpha^{p_1 \cdots p_{s-1}})^{p_s}] = F_1(\alpha^i) = 0$$

  Or α^i est racine de F_1.

Donc tout les éléments de P_n sont donc des racines de F_1, ce qui prouve que $\Phi_n = F_1$.

Donc Φ_n est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.

5 Corps Finis :

5.1 Théorème : Corps fini à p^r éléments

Soit $\mathbb{K}$ un corps fini, alors il existe un nombre premier p et un entier r tel que card($\mathbb{K}$) = p^r
Preuve : Soit $\mathbb{K}$ un corps fini, alors d'après la proposition (1.2) , la caractéristique de $\mathbb{K}$ est un nombre premier p. Donc $\mathbb{F}_p \subset \mathbb{K}$, donc $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel, sa dimension est finie car $\mathbb{K}$ est fini et r = [$\mathbb{K}$: $\mathbb{F}_p$].
Soit $\pi : \mathbb{F}_p \longrightarrow \mathbb{K}$ $(n_1, ..., n_r) \longmapsto \sum n_i\ e_i$
Il existe donc une base $(e_1, ..., e_n)$ dans $\mathbb{K}$ sur $\mathbb{F}_p$, de tel sorte que π est surjective : y = $\sum n_i e_i = \phi(n_1, ..., n_r)$. π est d'autre part injective, ker(π) = $0_{\mathbb{K}}$.
π est donc bijective et card($\mathbb{K}$) = q = p^r

5.2 Proposition :

Pour $\mathbb{K}$ un corps fini, ($\mathbb{K}^*$, x) est cyclique

Preuve :
On a montré le résultat du théorème suivant :
Pour un entier n$\geq$ 1, On a : n = $\sum\limits_{d/n} \varphi(d)$
Posons $n = q-1$, soit d un diviseur de n. Il suffit de montrer qu'il existe $x \in \mathbb{F}_q^*$ qui est d'ordre $q-1$. H : $< x > \simeq \mathbb{Z}/\mathrm{d}\mathbb{Z}$ où $x \in \mathbb{F}_{\mathbb{q}}{}^*$.
Soit $x \in \mathbb{F}_q^*$ d'ordre d où $d|n$.Soit y un élément d alors $y^d = 1$. De plus le polynôme $y^d - 1$ a au plus d racines dans $\mathbb{F}_{\mathbb{q}}$, or le polynôme $X^d - 1$ a aussi au plus d racines qui sont donc les d éléments.. Or $H \simeq \mathbb{Z}/d\mathbb{Z}$ donc tout élément d'ordre d est dans H. Par conséquent, le nombre $N(d)$ d'éléments d'ordre d de $\mathbb{F}_{\mathbb{q}}{}^*$ vaut 0 ou $\varphi(d)$, donc N(d) $\leq \varphi(d)$. Or tout élément de $\mathbb{F}_{\mathbb{q}}{}^*$ a pour ordre un diviseur de n donc n = | $\mathbb{F}_{\mathbb{q}}{}^*$ | = $\sum\limits_{d/n}$ N(d)=$\sum\limits_{d|n} \varphi(d)$
Par la proposition (3.2), on en déduit N(d) = $\varphi(d)$ pour tout d, d'où N(n) = $\varphi(n) > 0$ donc $\mathbb{F}_{\mathbb{q}}{}^*$ contient un élément d'ordre n donc est cyclique.

Proposition :

Polynôme cyclotomique de $\mathbb{F}_q$.
On sait que $\exists\alpha$ tel que $\mathbb{F}_q^* =< \alpha >$ et on sait que :

$$X^{q-1} - 1 = \prod_{x \in \mathbb{F}_q^*} (X - x) = \prod_{i=0}^{q-2} (X - \alpha^i)$$

Donc $\Phi(X) = \prod\limits_{i=0}^{q-2} (X - \alpha^i)$ avec α^i est racine primitive n_{ieme} dans $\mathbb{F}_q$.

Exemples de construction :

— **Corps à q = 2^2 éléments :**
Soit le polynôme $P = 1+X+X^2 \in \mathbb{F}_2[X]$. P est irréductible dans $\mathbb{F}_2$, car sinon P admet un facteur de degré 1 et donc une racine dans $\mathbb{F}_2$.
Or $P(0) = 1 = P(1) = 1+1+1$, donc P n'a pas de racine et donc P est irréductible dans $\mathbb{F}_2$.
Comme P est irréductible, son corps de rupture est donné par $\mathbb{F}_2[X]/(1+X+X^2)$.
Soit $\pi : \mathbb{F}_2[X] \longrightarrow \mathbb{F}_2[X]/(1+X+X^2)$ la projection canonique.
En posant $\alpha = \pi(X)$, on a : $\alpha^2+\alpha+1 = 0$
Donc $\alpha^2 = \alpha+1$, le corps de rupture de P est $\mathbb{F}_2[\alpha]$ car :
$(\alpha^2)^2+\alpha^2+1 = (\alpha+1)(\alpha+1)+\alpha^2+1$
$(\alpha^2)^2+\alpha^2+1) = 1+\alpha^2+\alpha^2+1 = 0$
α^2 est aussi une racine de P appartenant a $\mathbb{F}_2[\alpha]$, c'est un corps de décomposition.
Par construction $\mathbb{K}$ est un espace vectoriel de dimension 2 sur $\mathbb{F}_2$ et $1, \alpha$ en est une base
Les éléments sont donc $\{0, 1, \alpha, 1+\alpha\}$ (seules combinaisons linéaire de 1 et α à coefficients dans $\mathbb{F}_2$).

— **Corps à q = 3^2 éléments :**
Soit $P = X^2+X+2 \in \mathbb{F}_3[X]$.
On a $P(0) = P(2) = 2$ et $P(1) = 1$
Donc P est un polynome unitaire irreductiible de degre 2 a coefficients dans $\mathbb{F}_3$, son corps de rupture est donnée par : $\mathbb{F}_3[X]/(X^2+X+2)$
Soit $\pi : \mathbb{F}_3[X] \longrightarrow \mathbb{F}_3[X]/(X^2+X+2)$ la surjection canonique.
En posant $\alpha = \pi(X)$, on a $\alpha^2+\alpha+1 = 0$
Donc $\alpha^2 = 2\alpha+1$, on a :
$\alpha^3 = \alpha^2.\alpha = (2\alpha+1)\alpha = \alpha+2\alpha^2 = \alpha+\alpha+2 = 2\alpha+2$
$\alpha^4 = \alpha^3.\alpha = (2\alpha+2)\alpha = 2\alpha^2+2\alpha = \alpha+2+2\alpha = 2.$
Par le theoreme de Lagrange, $\alpha^8 = 1$.
Donc α est un generateur du groupe multiplicatif et :
$\mathbb{F}_9 = \{1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\} = <\alpha>$.

5.3 Proposition :

Soit $\mathbb{K}$ un corps de caracteristique p, alors l'endomorphisme $\sigma : x \longmapsto x^p$ est un automorphisme de $\mathbb{K}$.
Preuve : On a :
— $\sigma(1) = 1$.
$\forall\ x, y \in \mathbb{K}$:
— $\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$.

— $\sigma(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{j}{p}\ x^j y^{p-j} = \binom{p}{p}x^p + \binom{p}{0}y^p + \sum_{j=1}^{p-1} \binom{p}{j}x^j y^{p-j}$
On sait que pour $1 \leq j \leq p-1$, $\binom{p}{j} = \frac{p!}{j(p-j)!}$

Donc $j!(p-j)!\binom{p}{j} = p! = p(p-1)!$
Donc $p|j!(p-j)!\binom{p}{j}$.
Or $1 \leq j \leq p-1 < 1$, donc $pgcd(p,j) = 1$ et $pgcd(p,j!) = 1$.
De même si $1 \leq j \leq p-1$ alors $1 \leq p-j \leq p-1$, donc comme précédemment, $pgcd(p,(p-j)!) = 1$
Enfin, on trouve $pgcd(p,(j!(p-j)!) = 1$.
Donc $p|\binom{p}{j}$, $\sum_{j=1}^{p-1} x^j y^{p-j} = 0$.
Donc $\sigma(x+y) = x^p + y^p = \sigma(x) + \sigma(y)$.
Ainsi σ est un homomorphisme d'anneaux.

5.4 Théorème : Existence et unicité d'un corps fini

Soit $q = p^r$, alors il existe un corps de cardinal q , unique à isomorphisme près. C'est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$. On le note $\mathbb{F}_q$.
Preuve :
Existence : Soit $\mathbb{K}$ le corps de décomposition sur $\mathbb{F}_p$ du polynôme $P = X^q - X$. Soit $\mathbb{K}'$ l'ensemble des racines dans $\mathbb{K}$ du polynôme $X^q - X$. On montre que $\mathbb{K}'$ est un corps :
— $1 \in \mathbb{K}'$
— $\forall x, y \in \mathbb{K}', y \neq 0 : (xy^{-1})^q = x^q(y^{-1})^q = x(y^q)^{-1} = xy^{-1} \in \mathbb{K}'$
— $\forall x, y \in \mathbb{K}' : (x+y)^q = x^q + y^q = x + y$ (Frobenius)
Par définition du corps de décomposition, $\mathbb{K} = \mathbb{K}'$.
Le polynôme dérivée de $P = X^q - X$ vaut $P' = qX^{q-1} - 1 = -1$, de tel sorte que P et P' sont premier entre eux, donc toutes les racines sont simples et il y a en donc q.
Finalement $\mathbb{K}$ est bien un corps de cardinal q.
Unicité : Si $\mathbb{F}$ est un corps a q éléments, $\mathbb{F}^*$ est un groupe d'ordre $q-1$. Donc tout $x \in \mathbb{F}$ est racine du polynôme $X^q - X$ à coefficients dans $\mathbb{F}_p$ sous corps premier de $\mathbb{F}$ (L'extension $\mathbb{F}_p \subset \mathbb{K}$ est algébrique).
Donc $\mathbb{F}$ est le corps de décomposition de $X^q - X$ que $\mathbb{F}_p$.
Par unicité du corps de décomposition (prop 2.8), on a le résultat.

5.5 Théorème : Wedderburn

Tout corps fini est commutatif.

Preuve :
1) Soit $\mathbb{K}$ un corps et Z son centre. Par la définition , Z est un sous corps de $\mathbb{K}$ commutatif et de cardinal $q \geq 2$ (car contient au moins 0 et 1). Par la proposition(2.3) , $\mathbb{K}$ est un Z-espace vectoriel, donc $\exists$ n $\in \mathbb{N}^*$ tel que $|\mathbb{K}| = q^n$.

2)Pour $n \geq 2$, on raisonne par l'absurde en supposant$\mathbb{K}$ non commutatif.
- On considère $\mathbb{K}^*$ (non abélien) d'ordre $q^n - 1$. $\mathbb{K}^*$ opère sur lui même par automorphisme intérieur.
Pour $x \in \mathbb{K}^*$, on note son orbite :

$$w(x) = \{axa^{-1}, a \in \mathbb{K}^*\}$$

et on pose :

$$\mathbb{K}_x = \{y \in \mathbb{K}, yx = xy\}$$

$\mathbb{K}_x$ est un sous corps de $\mathbb{K}$, le stabilisateur de x sous l'action de $\mathbb{K}^*$ sur $\mathbb{K}^*$ est $\mathbb{K}_x^*$. De plus, $\mathbb{K}_x$ est un Z-espace vectoriel, donc $|\mathbb{K}_x| = q^d$.
Comme de plus, $\mathbb{K}_x^*$ ¡ $\mathbb{K}^*$,par lagrange $q^d - 1 | q^n - 1$. En effectuant la division euclidienne : $\exists (q, r) \in \mathbb{N}^* \times \mathbb{N}$ tel que $n = dq + r$ et $r < d$ ou $r = 0$.
Comme $r < d, q^n + 1 < q^d - 1$ et don :
$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + ... + q^{n-qd}) + (q^r - 1)$
Donc $q^r - 1$ est bien le reste de la division euclidienne de $q^n - 1$ par $q^d - 1$
Comme $q^d - 1 | q^n - 1$, donc $q^r - 1 = 0 \iff r = 0$ et $d|n$, et donc $|w(x)| = \frac{|\mathbb{K}^*|}{|\mathbb{K}_x^*|} = \frac{q^n - 1}{q^d - 1}, d|n$.
3) On utilise la propriété vu en proposition (...) :
Pour $d \neq n$, on a $\phi_n(q) | \frac{q^n - 1}{q^d - 1}$.
4) On utilise l'équation aux classes :

$$|\mathbb{K}^*| = |Z^*| + \sum_{x \notin Z} |w(x)|$$

$x \notin Z \iff d \neq n$.
$\iff q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$
Or $|\phi_n(q)||q - 1$ (car $\phi_n(q)|q^n - 1$ et $\phi_n(q) | \frac{q^n - 1}{q^d - 1}$, d diviseur strict de n)
Donc $|\phi_n(q)| \leq q - 1$.
5) On conclut avec : $\phi_n(q) = (q - \xi_1)...(q - \xi_l)$ où $\xi_1, ..., \xi_l$ racines primitives n-ième de l'unité.
$|\xi_i| = 1$ et $\xi_i \neq 1$ (car $n \neq 1$)
Donc $|q - \xi_i| > q - 1$. $|\phi_n(q)| > (q - 1)^l \geq q - 1$, Contradiction.

6 Codes correcteurs :

Problème : La transmission (message) sur un canal de communication (tel que la lecture d'un CD, d'un code QR,...) est souvent sujette à des perturbations, pour éviter cela on introduit **les codes détecteurs** et **correcteurs d'erreurs.** Formellement, on code le message à envoyer afin de detecter et corriger les éventuelles erreurs. Le but est donc d'avoir le meilleur code afin de détecter et corriger toutes les erreurs (ou un maximum).
Queslques exemples : On introduit quelques facons de coder afin de faire apparaître les difficultés qu'on peut rencontrer. On suppose qu'on veut envoyer

une sequence de **4 bits**, comme on a à chaque fois 2 choix possible (**"0" et "1"**), on a au total $2^4 = 16$ sequences possibles.

1. **Première possibilité :** On ne code pas le message. Donc si une erreur survient durant la transmission, on ne peut pas la detecter, encore moins la corriger. Donc on doit coder notre message.
2. **Deuxième possibilité :** On introduit un bit d'erreur : c'est le bit de parité, c'est a dire la somme des bits modulo 2 (qui donne 0 si la somme est un nombre pair et 1 sinon). Si la séquence reçue contient une erreur, on pourra la detecter car la somme des bits sera différent du bit de parité. En revanche, il nous est impossible de la corriger car on a aucune information sur la position de l'erreur. De plus, s'il y a deux erreurs, on ne peut ni les détecter, ni les corriger.
   Exemple :
   message transmis : 01100
   message reçu : 01000, on a détecté l'erreur.
   mais si message reçu : 11000, on détecte rien alors qu'il y a 2 erreurs.
   Donc on doit améliorer notre code.
3. **Troisième exemple :** On envoie chaque bit n fois, c'est le code par répétition. On pourra détecter des erreurs dès l'instant que l'on sait que le nombre d'erreurs de la transmission est strictement inférieur à $\frac{n}{2}$.

$$\begin{cases} \mathbb{F}_q \longrightarrow \mathbb{F}_q^n \\ x \longmapsto (x, ...x) \end{cases}$$

   En fait on plonge ainsi nos bits dans un espace vectoriel plus grand et donc l'envoi du message est plus long.
4. **Quatrième exemple :** Le code de Hamming, Il est l'un des plus efficaces pour la détection et la correction d'erreurs. Il permet lors de la réception du message de détecter et de corriger une erreur sur 1 seul bit. Son principe est le suivant :
   Supposons que l'on veuille envoyer le message suivant :
   m=(1,0,1,1).

Pour ce faire on doit ajouter au message précédant d'autres informations, on ajoute pour cela des bits appelés **bits de contrôle ou de parité**, pour une séquence de 4 bits, il faut au moins 3 bits de contrôle.On a donc au total 7 bits que l'on numérote de 1 à 7 :

$\underset{m_4 m_3 m_2 k_3 m_1 k_2 k_1}{7\ 6\ 5\ 4\ 3\ 2\ 1}$ On place les bits de contrôle dans les positions qui sont une puissance de 2

où $(m_1, m_2, m_3, m_4) = (1, 1, 0, 1)$
Pour calculer les bits de contrôles, on procède ainsi :
k_1 = Parité$(m_1, m_2, m_4) = 1$
k_2=Parité$(m_1, m_3, m_4) = 0$

$k_3 = Parité(m_2, m_3, m_4) = 0$
Et donc le mot qui va etre envoyé via le canal de transmission est le suivant :$(1, 0, 1, 0, 1, 0, 1)$.

6.1 Codes linéaires :

6.1.1 Définition :

On réalise l'opération de codage.
$\mathbb{F}_q^k$ est un espace-vectoriel de dimension **k**.
$\mathbb{F}_q^n$ est un espace-vectoriel de dimension **n**.
Pour un mot de longueur k **:**$(x_1, x_2, ..., x_k), x_i \in \mathbb{F}_q$**, q=p**^{r} Il y a donc q^k mots de longueur k
Soit :

$$\varphi : \begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (x_1, ..., x_k) & \longmapsto & C \end{cases}$$

φ est linéaire et injective.
C $= \varphi(\mathbb{F}_q^k)$ est un sous-espace vectoriel de $\mathbb{F}_q^n$.
Comme φ injective $\mathbb{F}_q^k \sim \varphi(\mathbb{F}_q^k)$, donc C=$\varphi(\mathbb{F}_q^k)$ est un $\mathbb{F}_q$ - sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k.
Remarques : -Les mots de code de C sont envoyés et décodés à l'arrivée. -On travaillera dans la suite sur C un code linéaire de longueur n et de dimension k.

$$\text{m} \in \text{C} \xrightarrow{canal} \text{m'} \in \mathbb{F}_q^n$$

On réalise le décodage par le "principe du maximum de vraisemblance", c'est a dire que le mot décodé sera celui qui a le plus de composantes commune du mot reçu.

6.2 Définition : Distances de Hamming

Soient **m, m'** $\in \mathbb{F}_q^n$. On appelle **poids de m** et on le note **w(m)** le nombre de composantes on nulles de **m**. On appelle **distance de Hamming** entre **m** et **m'** et on le note **d(m,m')** l'entier **w(m-m')**, et on appelle **distance du code** l'entier :
d = min d(m,m') = $\min_{m \in C, m \neq 0}$ w(m)
Exemple : Dans $\mathbb{F}_2^4$
m = (1 0 1 1), m'=(1 0 0 1), m"=(1 1 0 0)

w(m - m') = 1	d(m,m') = 1
w(m - m") = 3	d(m,m") = 3
w(m' - m") = 3	d(m',m") =3

6.3 Lemme :

Distance de Hamming est une distance.

Preuve : On va montre 3 propriété suivante :

1. $d(m, m') = 0$ ssi $m = m'$
2. $d(m, m') = d(m', m)$
3. $d(m, m') \leq d(m, m") + d(m", m)$

6.4 Définition : t-correction

Soit t $\in \mathbb{N}$, on dit qu'un code C est **t-correcteur** s'il peut détecter et corriger au plus t erreurs.

6.5 Proposition : Correction d'erreurs

Soit **d** la distance du code **C**, alors :
— Si **d = 2t**, alors **C** est **(t-1)-correcteurs**.
— Si **d =2t**, alors **C** est **t-correcteurs**.
Preuve : Soit e est une erreur de poids < d. Si m $\in$ C est envoyé et m' = m+e est reçu avec w(m-m')=w(e)<d, alors m' $\notin$ C car sinon w(m'-m)<d avec m-m' $\in$ C, ce qui contredit la distance minimale du code. Donc on peut detecter l'erreur.
Si m' $\in \mathbb{F}_q^n$ peut s'écrire $m_1 + e_1$ et $m_2 + e_2$ avec $m_1, m_2 \in$ C et $w(e_1) < \frac{d}{2}$, $w(e_2) < \frac{d}{2}$ alors :
$w(m_1 - m_2) = w(e_1 - e_2)$
Comme distance de Hamming est une distance.
Donc on a :
$w(e_1 - e_2) = d(e_1, e_2) \leq d(e_1, 0) + d(e_2, 0) \leq w(e_1) + w(e_2)$
Or :
$w(m_1 - m_2) \leq w(e_1) + w(e_2)$ (Inegalité triangluraire)
$w(m_1 - m_2) < d$.
D'ou $m_1 = m_2$. On peut detecter et corriger une errerur de poids $< \frac{d}{2}$ et si $d = 2t$, le plus petit entier $< \frac{d}{2}$ est t-1, si $d = 2t + 1$ le plus petit entier est t.

6.6 Proposition : Borne du singleton

On a : **d $\leq$ n +1 - k**

Preuve :
Soit E le sous espace vectoriel de $\mathbb{F}_q^n$, constitué des mots dont les k-1 dernieres composantes sont nulles. Alors :
$\mathbb{F}_q^n = \{(x_1, ..., x_n), x_i \in \mathbb{F}_q\}$.
E = $\{(x_1, ..., x_{n-k+1}, 0, ..., 0)\}$, donc dim(E) = n-k+1.
On a : dim(C $\cap$ E) = dim(C) + dim(E) - dim(C $\cup$ E)

. = k + (n - k +1) - dim(Vect(C ∪ E)).
Or dim(Vect(C ∪ E)) ≤ n (car (C ∪ E) ∈ $\mathbb{F}_q^n$).
Donc dim(C ∩ E) ≥ 1. Il existe donc un element non nul m ∈ C qui de plus verifie w(m) < n + 1 - k.

6.7 Définition : type de code

$$\mathbb{F}_q^k \xrightarrow{\varphi} \mathbb{F}_q^n$$

C = $\varphi(\mathbb{F}_q^k)$ est de dimension k en tant que $\mathbb{F}_q$ sous-espace vectoriel de $\mathbb{F}_q^n$. On dit que C est **un code de type (n,k,d)** où **d** est la distance du code :
$\mathbf{d = \min_{m \in C} w(m)}$.

Revenons aux exemples vu au départ :

1. On ne code pas le mot envoyé, alors :

$$\varphi_1 : \left\{ \begin{array}{rcl} \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^n \\ (x_1, ..., x_n) & \longmapsto & (x_1, ..., x_n) \end{array} \right.$$

   $m \in C \iff m = (x_1, ..., x_n)$ et $d = 1$, car le plus petit poids d'un mot non nul est un mot dans lequel il n'y a qu'un seul 1. C'est donc un code de type **(n,n,1)**.

2. On ajoute un bit de parité, alors :

$$\varphi_2 : \left\{ \begin{array}{rcl} \mathbb{F}_2^{n-1} & \longrightarrow & \mathbb{F}_2^n \\ (x_1, ..., x_{n-1}) & \longmapsto & (x_1, ..., x_{n-1}, x_n) \end{array} \right.$$

   où $x_n = x_1 + ... + x_{n-1}[2]$
   Ici , le plus petit poids d'un mot non nul est un mot dans lequel il n'y a qu'un seul 1 parmi les n-1 premières composantes, donc $x_n = \sum_i x_i = 1$ et donc d = 2. C'est donc un code de type **(n,n-1,2)**.

3. On envoie chaque bit n fois, alors :

$$\varphi_3 : \left\{ \begin{array}{rcl} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^n \\ x & \longmapsto & (x, ..., x) \end{array} \right.$$

   On a pas le choix, on envoie 1 n fois et donc d=n. C'est un code de type **(n,1,n)**.

4. Considerons un quatrième exemple :

$$\phi : \left\{ \begin{array}{rcl} \mathbb{F}_2^4 & \longrightarrow & \mathbb{F}_2^7 \\ (a_0, a_1, a_2, a_3) & \longmapsto & a_0 m_0 + a_1 m_1 + a_2 m_2 + a_3 m_3 \end{array} \right.$$

   où :

$$\left\{ \begin{array}{l} m_0 = (1101000) \\ m_1 = (0110100) \\ m_2 = (0011010) \\ m_3 = (0001101) \end{array} \right.$$

On a : $a_0m_0 + a_1m_1 + a_2m_2 + a_3m_3 = (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2 + a_3, a_1 + a_3, a_2, a_3)$.
Regardons ce que vaut le poids du code quand pour tout k $\in$ I=$\{0, 1, 2, 3\}$, $a_k = 1$ et $a_i = 0$, $i \neq k$.

— Si $a_0 = 1$ et $a_1 = a_2 = a_3 = 0$,
$a_0m_0 + a_1m_1 + a_2m_2 + a_3m_3 = (1, 1, 0, 1, 0, 0, 0)$.
$w(m_i) = 3$.
— Si $a_1 = 1$ et $a_0 = a_2 = a_3 = 0$,
$a_0m_0 + a_1m_1 + a_2m_2 + a_3m_3 = (0, 1, 1, 0, 1, 0, 0)$.
$w(mi) = 3$
— Si $a_2 = 1$, $a_0 = a_1 = a_3 = 0$.
$a_0m_0 + a_1m_1 + a_2m_2 + a_3m_3 = (0, 0, 1, 1, 0, 1, 0)$.
$w(m_i) = 3$
— Si $a_3 = 1$ et $a_0 = a_1 = a_2 = 0$.
$a_0m_0 + a_1m_1 + a_2m_2 + a_3m_3 = (0, 0, 0, 1, 1, 0, 1)$.
$w(mi) = 3$

Donc $w(m) \geq 3$, mais comme $w(1, 0, 0, 0) = 3$, alors $w(m) = 3$.
De plus, on montre ϕ injectif : Soit $(a_0, a_1, a_2, a_3), (a'_0, a'_1, a'_2, a'_3) \in \mathbb{F}_2^4$ tel que :
$a_0m_0 + a_1m_1 + a_2m_2 + a_3m_3 = a'_0m_0 + a'_1m_1 + a'_2m_2 + a'_3m_3$.
Alors :

$$\begin{cases} \mathrm{a}_0 = a'_0 \\ \mathrm{a}_0 + a_1 = a'_0 + a'_1 \\ \mathrm{a}_1 + a_2 + a_3 = a'_1 + a'_2 + a'_3 \\ \mathrm{a}_1 + a_3 = a'_1 + a'_3 \\ \mathrm{a}_2 = a'_2 \\ \mathrm{a}_3 = a'_3 \end{cases}$$

$$\iff \begin{cases} \mathrm{a}_0 = a'_0 \\ \mathrm{a}_1 = a'_1 \\ \mathrm{a}_2 = a'_2 \\ \mathrm{a}_3 = a'_3 \end{cases}$$

Donc ϕ injectif. Donc $dim\phi(\mathbb{F}_2^4 = 4$, c'est un code de type **(7,4,3)**.
$\frac{d-1}{2} = 1$, il est **1-correcteur**.

7 Codes linéaires cycliques :

7.1 Définition :

Un code linéaire cyclique C $\subset \mathbb{F}_q^n$ est cyclique s'il est stable par permutation circulaire (ou shift à droite) :

$$\sigma : \begin{cases} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ (m_0, ..., , m_{n-1}) & \longmapsto & (m_{n-1}, m_0, ..., m_{n-2}) \end{cases}$$

On va identifier l'algebre $\mathbb{F}_q^n$ à l'algebre $\mathbb{F}_q[X]/(X^n-1)$ via l'application :

$$(m_0,...,m_{n-1}) \xrightarrow{\varphi} m_0 + m_1X + ... + m_{n-1}X^{n-1}$$

On verra cela plus en detail dans la proposition 7.3.

7.2 Proposition :

Un code linéaire est cyclique si et seulement si $\varphi(C)$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$.
Preuve :
$\Leftarrow$) On montre que si $\varphi(C)$ est un idéal alors C est un code cyclique.
Soit $m = (m_0, m_1, ..., m_{n-1})$ un mot et $m(X) = m_0 + m_1X + ... + m_{n-1}X^{n-1}$ le polynome associé à m.
En terme de polynome, un decalage à droite signifie :
$\sigma(m)(X) = m_{n-1} + m_0X + ... + m_{n-2}X^{n-1}$
$\sigma(m)(X) = m_{n-1} + X(m_0 + ... + m_{n-2}X^{n-2} + m_{n-1}X^{n-1} - m_{n-1}X^{n-1})$
$\sigma(m)(X) = m_{n-1} - m_{n-1}X^{n-1} + X(m_0 + m_1X + ... + m_{n-1}X^{n-1})$
$\sigma(m)(X) = m_{n-1}(1-X^n) + Xm(X)$
Donc $\sigma(m)(X) = Xm(X) mod(X^n-1)$
Comme $\varphi(C)$ est un idéal, $m(X) \in \varphi(C)$ et donc $Xm(X) \in \varphi(C)$.
Donc $\sigma(m) \in C$. Donc C est cyclique. $\Rightarrow$) Pour C un code cyclique, on montre :

— $\varphi(C)$ est une groupe pour l'adition.
— $\forall P \in \mathbb{F}_q[X], \forall Q \in \varphi(C), \overline{PQ} \in \varphi(C)$
Soit $m = (m_0, m_1, ..., m_{n-1})$ et $m' = (m_,0', m'_1, ..., m'_{n-1}) \in C$.
— $(0, ..., 0) \in C$
— $\varphi(m) - \varphi(m') = (m_0 - m'_0) + ... + (m_{n-1} - m'_{n-1})X^{n-1}$1i1in$\mathbb{F}_q[X]/(X^n-1)$.

Donc $\varphi(C)$ est un sous groupe.
Il reste à montrer que : $\forall P \in \mathbb{F}_q[X], \overline{P}\varphi(m) = \overline{P}m(X) \in \varphi(C)$ où
$\overline{P} = P \bmod(X^n-1)$, le reste de la division de P par X^n-1.
On a : $\forall k \leq n-1, \sigma^k(m)(X) = X^k m(X)$ (correspond à un décalage k fois à droite).
Donc $\forall k, X^k m(X) \in \varphi(C)$, donc $\forall \overline{P} \in \mathbb{F}_q[X]/(X^n-1), \overline{P}m(X) \in \varphi(C)$.
Donc $\varphi(C)$ est un idéal.

7.3 Proposition :

Tout idéal de $\mathbb{F}_q[X]/(X^n-1)$ est un idéal engendré par un polynôme unitaire qui divise X^n-1.

Preuve :

$$\mathbb{K}[X] \xrightarrow{\pi_q} \mathbb{K}[X]/Q$$

On a vu que pour $Q \in \mathbb{K}[X]$,l'endomorphisme de passage au quotient $\mathbb{K}[X] \longrightarrow \mathbb{K}[X]/(Q)$ induit une bijection entre l'ensemble des idéaux de $\mathbb{K}[X]/Q$ et l'ensemble des idéaux de $\mathbb{K}[X]$ qui contiennent Q.
On applique ce résultat ici, soit J un idéal de $\mathbb{F}_q[X]/(X^n-1)$, il existe un unique I contenant X^n-1 tel que $\pi_{X^n-1}(I) = J$.
$\varphi(C)$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, il existe un unique I contenant (X^n-1) tel que $\pi_q(I) = J$.
$\varphi(C)$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, il existe un unique I contenant X^{n-1} tel que $\prod_{X^n-1}(I) = \varphi(C)$.
Or $\mathbb{F}_q$ est un corps $\Rightarrow \mathbb{F}_q[X]$ principal. Donc $(I) = (P) \supset (X^n-1)$.
Donc $X^n - 1 \in (P)$.
$X^n - 1 = P \times R$ où $R \in \mathbb{F}_q[X]$, donc $(P)|X^n - 1$.

7.4 Définition :

L'unique générateur de l'idéal $\varphi(C)$ est appelé le générateur du code C.
D'après la proposition 7.4, ce générateur est un polynôme unitaire qui divise $X^n - 1$.

7.5 Proposition : Dimension de code

Étant donné un tel polynôme g, la dimension du code est dim(C) est k = n -deg(g(X)).

Preuve :
Soit $m \in C$, m(X) $= m_0 + m_1X + ... + m_n - 1X^(n-1)$.
$deg(m(X)) \leq (n-1)$, $m(X) \in < g(X) >$.
Donc on peut écrire : $m(X) = P(X).g(X) = \sum_{i=1}^{l}(b_iX^i)g = \sum_{i=1}^{l}(b_iX^ig)$.
$deg(m(X)) = l + deg(g) \leq (n-1)$.
Donc $l \leq n - 1 - deg(g)$
Donc C est l'ensemble $\{fg : f \in \mathbb{F}_q[X], deg(f) \leq n - 1 - deg(g)$.

Retour aux exemples :
Les trois exemples de la section 6.6, ainsi que l'exemple de **Hamming** sont tous cycliques.

1.
$$\varphi_1 : \begin{cases} \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^n \\ (x_1, ..., x_n) & \longmapsto & (x_1, ..., x_n) \end{cases}$$

Une permutation a droite donne :
$\sigma(x_1, ..., x_n) = (x_n, x_1, ..., x_{n-1})$

2.

$$\varphi_2 : \begin{cases} \mathbb{F}_2^{n-1} & \longrightarrow & \mathbb{F}_2^n \\ (x_1, ..., x_{n-1}) & \longmapsto & (x_1, ..., x_{n-1}, x_n) \end{cases}$$

Pour montrer la stabilité par le shift à droite on montre que :
$\sigma(x_1, ..., x_n) = (x_n, x_1 ..., x_{n-1})$ où x_{n-1} a la même parité que
$x_n + x_1 + ... + x_{n-2}$.
On peut conclure car l'addition est commutative. Donc le code est cyclique.
On montre que son polynome générateur est $1 + X$:

On sait que :
φ_2 est code du type (n, n-1, 2)
et par définition 7.5 on a : dim C est $n - 1 = n - deg(g(X))$ avec $g(X)$ est polynôme générateur du code C.
Donc $deg(g(X)) = 1$ Comme $g(X)$ divise $X^n - 1$ Donc $g(X) = X - 1 = X + 1$ dans $F_2[X]$

3.

$$\varphi_3 : \begin{cases} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^n \\ x & \longmapsto & (x, ..., x) \end{cases}$$

Ici, pas de problème, $\sigma(x, ..., x) = (x, ..., x)$ et le code est cyclique.
On montre que son polynome générateur vaut $1 + X + ... + X^{n-1}$

On a dim C = 1 donc $deg(g(X)) = n - 1$
Comme $g(X)$ divise $X^n - 1$
Donc $g(X) = X^{(n-1)} + X^{(n-2)} + ... + X + 1$

4.

$$\phi : \begin{cases} \mathbb{F}_2^4 & \longrightarrow & \mathbb{F}_2^7 \\ (a_0, a_1, a_2, a_3) & \longmapsto & a_0 m_0 + a_1 m_1 + a_2 m_2 + a_3 m_3 \end{cases}$$

où

$$\begin{cases} m_0 = (1101000) \\ m_1 = (0110100) \\ m_2 = (0011010) \\ m_3 = (0001101) \end{cases}$$

On a : dim C = 4 donc $deg(g) = 3$
Comme $g(X)$ divise $X^7 - 1$ et est irréductible dans $\mathbb{F}_2[X]$.(par 7.6)
On a

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

Maintenant on va montre que $X^3 + X + 1$ et $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_2$.

Comme $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ on peut voir $\bar{0}$ et $\bar{1}$ ne sont pas des solutions de $X^3 + X + 1$ ou $X^3 + X^2 + 1$.
Donc $X^3 + X + 1$ et $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_2$.
Donc $g(X) = X^3 + X^2 + 1$ ou $X^3 + X + 1$

7.6 Construction des codes cycliques linéaires :

On suppose désormais que n est premier avec q.

On a vu que construire un code sur $\mathbb{F}_q^n$, revient a trouver à trouver un polynôme unitaire g de $\mathbb{F}_q[X]$ qui de $X^n - 1$.
On va voir comment construire un tel polynôme.
Comme $n \wedge q = 1$, alors $\overline{q} \in (\mathbb{Z}|n\mathbb{Z})^*$. Soit $m = ordre(\overline{q})$ dans $(\mathbb{Z}|n\mathbb{Z})^*$.
On a :
$q^m \equiv 1$ (mod n), donc par Lagrange $n|(q^m - 1)$.
On sait (proposition 5.4) que $\mathbb{F}_{q^m}$ est un corps de décomposition de $X^{q^m} - X$.
Donc $\mathbb{F}_{q^m}$ est un corps décomposition de $X^{q^m-1} - 1$, $(\mathbb{F}_{q^m})^*, \times)$ est un groupe cyclique (prop 5.2), donc $\mathbb{F}_{q^m}^* =< \alpha >$. Donc on peut écrire :
$X^{q^m-1} - 1 = \prod_{i=0}^{q^m-2} (X - \alpha^i)$.
Or $n|(q^m - 1)$.
Donc $(X^n - 1)|(X^{q^m-1} - 1)$.
On utilise le résultat suivant :

Lemme :

Dans un corps quelconque $\mathbb{K}$, n divise n' implique $X^n - 1|X^{n'} - 1$.

Preuve :
Soit β une racine de $X^n - 1$ dans une clôture algébrique de $\mathbb{K}$. On a :
$\beta^n = 1$ $x' = ln$ donc $\beta^{x'} = (\beta^n)^l = 1$.
Donc β est aussi une racine de $X^{n'} - 1$.
Donc $X^n - 1$ divise $X^{n'} - 1$.
On sait que $(X^n - 1)|(X^{q^m-1} - 1)$.
Or $X^{q^m-1} - 1 = \prod_{i=0}^{q^m-1} (X - \alpha^i)$.
Or $(X^n - 1)|(X^{q^m-1} - 1)$ et $g|(X^n - 1)$.
Donc $g = \prod_{i \in \mathcal{I}} (X - \alpha^i)$
où $\mathcal{I}$ est une partie convenable de $\mathbb{Z}/n\mathbb{Z}$.

7.7 Proposition :

Soit $g(X) = \prod_{i \in \mathcal{I}} (X - \alpha^i)$ où $\mathbb{F}_{q^m}^* =< \alpha >$. $g \in \mathbb{F}_q[X]$ si et seulement si $\mathcal{I}$ est stable par multiplication par q (mod n).

Preuve :
Si $g \in \mathbb{F}_q[X]$, $g = \sum_{i=0}^{n-1} a_i X^i, a_i \in \mathbb{F}_q$.
Par Frobenius (Proposition 5.3) : $x \longmapsto x^p$ est un homomorphisme de corps. On a : $\mathbb{F}_q$ l'ensemble des éléments x tel que $x^q = x$.
$\forall a_i \in \mathbb{F}_q, a_i^q = a_i$. Pour toute racine β de $g(X)$, on a :
$g(\beta^q) = \sum_{i=0}^{n-1} a_i \beta^{qi} = \sum_{i=0}^{n-1} a_i^q \beta^{qi} = \sum_{i=0}^{n-1} (a_i \beta^i)^q = (g(\beta))^q$.
Donc $(g(\beta))^q = g(\beta^q)$.
Donc l'ensemble des racines de g sont stable par passage à la puissance $q^{ième}$.
Comme, $g(X) = \prod_{i \in \mathcal{I}} (X - \alpha^i)$, si α^i est une racine de g, alors α^{iq} est aussi une racine de g. Donc si $i \in \mathcal{I}$ alors $iq \in \mathcal{I}$.
Donc $\mathcal{I}$ stable par multiplication par q(mod n).

Réciproquement, si $\mathcal{I}$ est stable par multiplication par q(mod n), alors :

$$\begin{aligned} g(X^q) &= \prod_{i \in \mathcal{I}} (X^q - \alpha^i) \\ &= \prod_{i \in \mathcal{I}} (X^q - \alpha^{qi}) \\ &= \prod_{i \in \mathcal{I}} (X - \alpha^i)^q (Frobenius) \\ &= (g(X))^q \end{aligned}$$

Donc on a :
$\sum_{i=0}^{n-1} a_i X^{qi} = (\sum_{i=0}^{n-1} a_i X^i)^q = \sum_{i=0}^{n-1} a_i^q X^{qi}$.
Donc $a_i = a_i^q$
Donc a_i solution de $X^q - X$
Donc $a_i \in \mathbb{F}_q$.

7.8 Proposition :

S'il existe k,s $\in \mathbb{N}^*$ tels que $\mathcal{I}$ contienne **k+1,k+2,...,k+s**, alors la distance du code est $\geq$ **s+1**.

Preuve :
Supposons que $\mathcal{I} = \{i \in \mathbb{Z}/n\mathbb{Z}, \alpha^i \text{ racine de } g\}$ contienne $k+1, k+2, ..., k+s$.
Soit $m \in C$, alors $deg(m) \leq n-1$.
Or $g(X) \in C$ est un polynôme générateur du code C et $g(X) = \prod_{i \in \mathcal{I}} (X - \alpha^i)$, $\alpha^{k+1}, ..., \alpha^{k+s}$ sont des racines de g.

Donc $m(\alpha^n) = 0$ comme $g|n$, pour $l \in \{k+1, ..., k+s\}$.
Donc d la distance du code C, on a :
$d = \min_{m \in C, m \neq 0} w(m)$.
Par l'absurde, supposons $d \leq s$, donc $w(m) \leq s$ (ie m a au plus s coefficients non nul).
Posons $m(X) = \sum_{j=1}^{s} \lambda_j X^{nj}$ où $\lambda_j \neq 0, \lambda_j \in \mathbb{N}$ et $0 \leq n_1 < ... < n_s < n$.
Alors pour tout $1 \leq l \leq s$. $l = k + i$

$$\begin{aligned} m(\alpha^k) &= \sum \lambda_j (\alpha^l)^{nj} = 0 \\ &= \sum_{j=1}^{s} (\alpha^{k+i})^{nj} \\ &= \sum_{j=1}^{s} \lambda_i \alpha^{k+i} n_j \\ &= 0 \end{aligned}$$

Donc $\forall i : \sum_{j=1}^{s} \lambda_j (\alpha^{k+i})^{n_j} = 0$
$\lambda_1, ..., \lambda_s$ sont donc solutions du système :

$$\begin{vmatrix} \alpha^{(k+1)n_1} & \alpha^{(k+1)n_2} & \dots & \alpha^{(k+1)n_s} \\ \alpha^{(k+2)n_1} & \alpha^{(k+2)n_2} & \dots & \alpha^{(k+2)n_s} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(k+s)n_1} & \alpha^{(k+s)n_2} & \dots & \alpha^{(k+s)n_s} \end{vmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_s \end{bmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Soit D le déterminant de la matrice associe au système, on a :

$$D = \alpha^{(k+1)(n_1+...+n_s)} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{n_1} & \alpha^{n_2} & \cdots & \alpha^{n_s} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(s-1)n_1} & \alpha^{(s-1)n_2} & \dots & \alpha^{(s-1)n_s} \end{vmatrix}$$

Le déterminant de ce système est un déterminant de Vandermonde.
Donc $D = \alpha^{(k+1)(n_1+...+n_s)} \prod_{1 \leq j < i \leq s} (\alpha^{n_i} - \alpha^{n_j})$
Car α est une racine primitive $n^{ième}$ de l'unité, donc $\alpha \neq 0$ et $\alpha^{n_i} \neq \alpha^{n_j}, \forall i \neq j$.
Donc D non nul.
Donc le système homogène admet une unique solution $\alpha_1 = ... = \alpha_s = 0$.
Absurde $m \neq 0$. Donc $d \geq s + 1$.

Revenons sur l'exemple du code de Hamming :
Cas $q = 2$, $n = 7$:
Soit $j \in \mathbb{Z}|7\mathbb{Z}$, et $s > 0$ les plus petit entier tel que :

$$q^s \times j \equiv j(\text{mode}7)$$

On a $j \in \{\bar{0}, \bar{1}, ..., \bar{6}\}$: $2^s \times j \equiv j(\text{mod}7)$.
Donc $j \in \{\bar{0}, \bar{1}, \bar{3}\}$:

— Si $j = \bar{1}$ on a $s = 3$.

— Si $j = \bar{3}$ on a $s = 3$.

On a donc 3 classes cyclotomique sont $\{\bar{0}\}$, $\{\bar{1}, \bar{2}, \bar{4}\}$ et $\{\bar{3}, \bar{5}, \bar{6}\}$.
On a :$(q, n) = (2, 7) = 1$ et $q^3 \equiv 1(\text{mode}7)$
Donc $\mathbb{F}_{q^3} = \mathbb{F}_8$ est un corps décomposition de $X^{q^3-1} - 1 = X^7 - 1$.
Il clair que $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
Alors $\mathbb{F}_2[X]|(X^3 + X + 1)$ est une extension de degré 3 et $\mathbb{F}_2$.
Donc il est isomorphe à $\mathbb{F}_8$
Soit α est une racine primitive de $\mathbb{F}_8$.
Donc α est une racine de $X^3 + X + 1$, comme $\alpha^3 + \alpha + 1 = 0$. (*)
On peut écrire :

$$X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$$

où $X^7 - 1 = (X - 1) \times g_1(X) \times g_2(X)$ avec g_1 et g_2 sont irréductibles dans $\mathbb{F}_2[X]$.
Comme α est une racine primitive de $\mathbb{F}_8$, donc α est aussi une racine de $X^7 - 1$.
Donc $\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$. Par (*) on a $\alpha^6 + \alpha^5 + \alpha^3 = 1$.
On pose :

$$g_1(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4)$$
$$g_2(X) = (X - \alpha^3)(X - \alpha^5)(X - \alpha^6)$$

—

$$\begin{aligned} g_1(X) &= (X - \alpha)(X - \alpha^2)(X - \alpha^4) \\ &= X^3 - (\alpha^4 + \alpha^2 + \alpha)X^2 + (\alpha^6 + \alpha^5 + \alpha^3)X - \alpha^7 \\ &= X^3 + X - 1 \\ &= X^3 + X + 1(dans\mathbb{F}_2[X]) \end{aligned}$$

—

$$\begin{aligned} g_2(X) &= (X - \alpha^3)(X - \alpha^5)(X - \alpha^6) \\ &= X^3 - (\alpha^3 + \alpha^5 + \alpha^6)X^2 + (\alpha^4 + \alpha^2 + \alpha)X - \alpha^7 \\ &= X^3 - X^2 - 1 \\ &= X^3 + X^2 + 1(dans\mathbb{F}_2[X]) \end{aligned}$$