→ Construction des codes cycliques : Soit $\sigma = (1\ 2\ \dots\ n)$

Déf : Un code $\mathcal{C}$ est cyclique si $\forall m = (m_0 \dots m_{n-1}) \in \mathcal{C}$, $\sigma(m) \in \mathcal{C}$.

On identifie m avec $m(X) = m_0 + \dots + m_{n-1} X^{n-1} \in \mathbb{F}_q(X)$.

Alors $\mathcal{C}$ cyclique ⇔ $\mathcal{C}(X)$ idéal de $\mathbb{F}_q[X]/(X^n-1) \simeq \mathbb{F}_{q^n}$

Donc l'ensemble des codes cycliques est en bijection avec les diviseurs unitaires de X^n-1 dans $\mathbb{F}_q[X]$

→ Factorisation de X^n-1 dans $\mathbb{F}_q[X]$ (lorsque $q \wedge n = 1$)

• $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$. Contrairement à ce qui se passe sur $\mathbb{Q}$, sur $\mathbb{F}_p$ les polynômes cyclotomiques ne sont pas irréductibles ! :

Prop : (il faut $q \wedge n = 1$) $\bar{n} = \bar{o}(q)$ dans $(\mathbb{Z}/n\mathbb{Z}^*, \times)$. Alors Φ_n se décompose en produit de polynômes irréductibles de degré $\bar{n}$ tous distincts. dans $\mathbb{F}_q[X]$

• Lemme 1 : $X^n - 1$ n'a que des facteurs simples dans $\mathbb{F}_q(X)$.

Si $X^n - 1 = Q^2 R$, alors en dérivant : $n X^{n-1} = Q(2Q'R + QR')$

et $n = nXX^{n-1} - nX^n + n = Q(X(2Q'R + QR') - nQR)$

Donc Q constant, car $n \neq 0$ dans $\mathbb{F}_q$ - Vérifié + simple : on montre que X^n-1 a racines simples (*)

Donc en particulier les Φ_d sont tous à racines simples dans $\mathbb{F}_q(X)$.

• Lemme 2 : Les racines de $\prod_{d \mid n} \Phi_n$ sont les racines n-ièmes de 1 :

Par récurrence en utilisant $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$, les racines étant racines d'exactement 1 Φ_d

Preuve de la prop : (*) Ce n'est pas tout à fait équivalent, car on pourrait avoir un facteur multiple sans racines, mais ici c'est suffisant

→ $(X^n-1)' = nX^{n-1}$, racine $\neq 0$ car $n \wedge p = 1$. Donc (0 pas racine de X^n-1),

X^n-1 racines simples car sinon il y aurait une racine en commun avec $(X^n-1)'$

Preuve de la prop: $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$.

$n \mid q^n - 1$ donc $\mathbb{F}_{q^n}^* \simeq \mathbb{Z}/(q^n-1)\mathbb{Z}$ admet un élément α d'ordre n (car il est cyclique).

Soit $I = \{$classes de premiers avec n dans $\mathbb{Z}/n\mathbb{Z}\}$. $\#I = \varphi(n) = \deg \Phi_n$.

$= \{\alpha^{i_1}, \dots, \alpha^{i_{\varphi(n)}}\}$

Chacun des α^i est d'ordre n, donc $\Phi_n(X) = \prod_{i \in I} X - \alpha^i$. (*)

On considère la multiplication par q sur I. $\forall i \in I$, $q^n i = i$ [n]. Comme $n \mid q^n - 1$, $q^n \equiv 1$ [n], donc $\forall i \in I$, $q^n i = i$.

De + Par ailleurs, $i \wedge n = 1$ et $g(q) = n$ donc $i, iq, \dots, iq^{n-1}$ sont dans des classes distinctes dans $\mathbb{Z}/n\mathbb{Z}$.

On construit ainsi des classes toutes à n éléments qui partitionnent I.

En reprenant (*), cela donne une décomposition de Φ_n en produit par polynômes de degré n.

Reste à voir que ces polynômes (notons P_Σ pour le polynôme associé à la classe Σ) sont à coeffs dans $\mathbb{F}_q$. Tout découle du Frobenius via la proposition suivante:

Prop: $g_\Sigma \in \mathbb{F}_q(X) \iff \Sigma$ stable par mult par q mod n.

Preuve: "$\Rightarrow$" $g_\Sigma \in \mathbb{F}_q(X) \Rightarrow$ chaque coeff de g_Σ stable par Frob et par linéarité, $g_\Sigma(X^q) = (g_\Sigma(X))^q$, donc $\{$racines de $g_\Sigma\}$ stable par Frob

i.e. Σ stable par $\times q$ (suffit de l'écrire)

"$\Leftarrow$" Σ stable par $\times q \Rightarrow g_\Sigma(X^q) = g_\Sigma(X)^q$ i.e. tous les coeffs de g_Σ sont égaux à leur puissance q-ième, donc sont des racines de $X^q - X \in$ exactement les éléments de $\mathbb{F}_q$

or $X^q - X$ admet au q racines dans un corps. Yoyo !

(Conséquemment on a montré que le corps de décomposition de Φ_n sur $\mathbb{F}_q$ est $\mathbb{F}_{q^n}$.