Master 2. Mathematiques Fondamentale et Discrète.
Module : Théorie des codes correcteurs d'erreurs 2.

Chapitre 1: Notions d'algèbre.

I.1 Anneau des polynômes.

Définition 1.1. Soit A un anneau commutatif. Un **polynôme** sur A est une suite $P=(a_i)_{i\in\mathbb{N}}$ d'éléments de A (dits **coefficients**) qui sont nuls sauf un nombre fini. On note $A[X]=\{ P=(a_i)_{i\in\mathbb{N}} / a_i\in A\}$ l'ensemble des polynômes sur A, où X=(0, 1, 0, …,0..) est dite **l'indéterminé**. Si on muni A[X] par les lois d'addition (+) et multiplication (.) définies par :
$(a_i)_{i\in\mathbb{N}}+(b_i)_{i\in\mathbb{N}}=(a_i+b_i)_{i\in\mathbb{N}}$ et $(a_i)_{i\in\mathbb{N}}.(b_i)_{i\in\mathbb{N}}=(\sum_{j=0}^{i} a_j b_{i-j})_{i\in\mathbb{N}}$, alors on aura la proposition suivante :

Proposition et définition 1.2.
(A[X], +, .) est un anneau commutatif dit **anneau des polynômes** d'indéterminé X. D'éléments neutres 0=(0, 0, …., 0…) pour la loi (+) dit **polynôme nul** et (1, 0, 0, …, 0, …) pour la loi (.).

Remarque: On a pour tout entier n, X^n= (0, 0,…,0, 1, 0, ….) ou 1 se trouve en position n+1, et tout polynôme $P=(a_i)_{i\in\mathbb{N}}$ s'écrit $P = \sum_{i\geq 0} a_i X^i$ et comme cette somme est fini alors il existe un entier n tel que $a_n\neq 0$, et $P = \sum_{i=0}^{n} a_i X^i$. L'entier n est appelé le **degré** du polynôme P noté **d°(p),** Par convention d°(0)=-∝. Le coefficient a_n est dit le **coefficient dominant**, si a_n=1 on dit que P est un **polynôme unitaire**.

Exemple: Les polynômes de degré nul sont de la forme P=a / a∈A-{0} dit **polynômes constants**. Les polynômes de degré 1 sont de la forme P=ax+b / a∈A-{0} et b∈A, ceux de degré 2 sont de la forme $P=aX^2+bX+c$ / a∈A-{0} et b,c∈A.

Proposition 1.3.
A[X] est un anneau intègre si et seulement si A est un anneau intègre.

Proposition 1.4. Division Euclidienne.
Si A est un anneau commutatif intègre alors, ∀A∈ **A**[X] et ∀B∈ A[X]-{0} de coefficient dominant inversible alors :
∃(Q, R)∈𝕂[X]×𝕂[X]: A=BQ+R / R=0 ou d°(R) < d°(B)

Proposition 1.5. Division Euclidienne
Si 𝕂 est un corps commutatif alors l'anneau 𝕂[X] est un anneau commutatif Euclidien.

Conséquence 1.6.
Si 𝕂 est un corps commutatif alors 𝕂[X] est un anneau principal.

Remarque :
Si I est un idéal de 𝕂[X] alors il est principal engendré par tout polynôme non nul de I de degré minimum, et le polynôme unitaire P engendrant I est dit « **le générateur** » de I et on a:
I=(P) ={ PQ / Q∈ 𝕂[X]}, les éléments de I sont dits les multiples de P.

Exemple :
Soit I={P∈ℝ[X] : P(1)=0} I est un idéal de ℝ[X] et on a: P∈I ⇔P(1)=0⇔P=(X-1)Q / Q∈ℝ[X])⇔P∈(P_1=X-1).
donc I=(P_1=X-1) l'idéal engendré par le polynôme P_1=X-1.

1.2 Racines d'un polynôme et l'anneau quotient 𝕂[X]/(P).

Définition 1.7.
1) Un élément α de l'anneau A est dit **racine** du polynôme $P = \sum_{i=0}^{n} a_i X^i$∈A[X] si et seulement si $P(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0$ (le zéro de A).
2) α est dite **racine multiple** de P **d'ordre** k si $P=(X-\alpha)^k Q$ et $Q(\alpha)\neq 0$. Si k=1, α est dite **racine simple**.

Exemple : $P=(X-1)^2(X+1)\in\mathbb{R}[X]$ admet 1 comme racine double et (-1) comme racine simple.

Proposition 1.8.
Si α est une racine d'ordre k d'un polynôme P de 𝕂[X] alors α est racine d'ordre k-1 de son dérivé P`.

Proposition 1.9.
Si 𝕂 est un corps commutatif et I un idéal de 𝕂[X] de générateur un polynôme P Alors 𝕂[X]/(P) est un anneau commutatif d'élément neutre $\bar{0}$ =I par l'addition et $\bar{1}$ =1+I par la multiplication, dit **anneau quotient** de 𝕂[X] par l'idéal I=(P).

Conséquence 1.10.
Si P∈ 𝕂[X] est un polynôme **irréductible** alors l'anneau quotient 𝕂[X]/(P) est un corps commutatif.

Exercice: Soit 𝕂 un corps commutatif. L'ensemble $\mathbb{K}_{n-1}[X]$= {P∈ 𝕂[X] tel que d°(P) ≤ n-1} est une sous-algèbre de 𝕂[X].

1.3 Corps finis.

1.3.1 Construction des corps finis.

Proposition 1.11. : Si p est un entier premier et P un polynôme irréductible sur F_p de degré n alors le corps $F_p[X]/(P)$ est un corps commutatif fini isomorphe à $(F_p)_{n-1}[X]$ (l'anneau des polynômes sur F_p de degré ≤ à n-1) et de cardinal p^n.

Preuve: Soit l'application ϕ de $F_p[X]$ dans $(F_p)_{n-1}[X]$, A⟼ϕ(A)=R tel que R est le reste de la division Euclidienne de A par P. ϕ est un morphisme d'anneaux surjective car : Imϕ={ϕ(A) / A∈F_p[X]}= {R / R∈F_p[X] et d°(R)≤n-1}= $(F_p)_{n-1}$[X].
On a A=QP+R avec R=0 ou d°(R) ≤ n-1 et Kerϕ={A∈F_p[X] / ϕ(A)=0}={A∈F_p[X] / R=0}
Kerϕ={ PQ / Q∈F_p[X] }=(P) l'idéal engendré par le polynôme P. selon le premier théorème d'isomorphisme alors:
$F_p[X]/(P) \cong (F_p)_{n-1}[X] \cong (F_p)^n$ et donc $Card(F_p[X]/(P))= p^n$.

Proposition 1.12.
Si $\mathbb{K}$ est un corps fini alors la caractéristique de $\mathbb{K}$ est un entier premier p et $\mathbb{K}$ admet un sous-corps isomorphe à F_p dit **sous-corps premier** de $\mathbb{K}$ et le cardinal de $\mathbb{K}$ est de la forme p^n.
Preuve : Comme $\mathbb{K}$ est un corps alors c'est un anneau intègre donc car($\mathbb{K}$)=0 ou car($\mathbb{K}$)=p premier, si on suppose car($\mathbb{K}$)=0 alors $\mathbb{K}$ est infini absurde car $\mathbb{K}$ est fini.
L'application $f: \mathbb{Z} \longrightarrow \mathbb{K}, k \longmapsto f(k) = k.1_{\mathbb{K}}$, est un morphisme d'anneaux de noyau Kerf=p$\mathbb{Z}$ et $F_p = \mathbb{Z}/p\mathbb{Z} \cong f(\mathbb{Z})$ or $f(\mathbb{Z})$ est un sous-corps de $\mathbb{K}$, donc on peut considérer F_p comme un sous-corps de $\mathbb{K}$ dit **sous-corps premier** de $\mathbb{K}$ et donc le corps $\mathbb{K}$ est considéré comme espace vectoriel sur F_p et si $\dim_{\mathbf{F_p}}\mathbb{K} = n$ alors $\mathbb{K} \cong {F_p}^n$ et card($\mathbb{K}$)=p^n.
Propriétés 1.13.
Soit p est la caractéristique d'un corps commutatif fini $\mathbb{K}$ alors :
1) p est le plus petit entier non nul vérifiant $p.1_{\mathbf{A}} = 0$.
2) $\forall x \in \mathbb{K}: \; p.x = 0,$
3) $\forall x, y \in \mathbb{K} : (x+y)^p = x^p + y^p$ et $(xy)^p = x^p + y^p$,
4) $\forall i \in \mathbb{N}, \forall x, y \in \mathbb{K} : (x+y)^{p^i} = x^{p^i} + y^{p^i}$,
Proposition 1.14.
Si $\mathbb{K}$ est un corps commutatif fini de caractéristique p et de cardinal p^n alors :
($\mathbb{K}^*=\mathbb{K}-\{0\}, .$) est un groupe cyclique d'ordre p^n-1 et $\forall\, x \in \mathbb{K} : x^{p^n} = x$.
Preuve:
1) $\mathbb{K}^*=U(\mathbb{K})$ est un groupe cyclique multiplicatif de cardinal p^n-1. Donc $\forall\, x \in \mathbb{K}^* : x^{p^n-1} = 1$ en multipliant par x on trouve $\forall\, x \in \mathbb{K}^* : x^{p^n} = x$ et comme cette égalité est vrai pour x=0 alors on trouve $\forall\, x \in \mathbb{K} : x^{p^n} = x$.
Définition 1.15. Racine primitive d'un corps fini.
Si $\mathbb{K}$ est un corps commutatif fini de cardinal p^n , alors tout générateur α du groupe cyclique $\mathbb{K}^*$ est appelé **racine primitive** (ou **élément primitif**) de $\mathbb{K}$ et $\mathbb{K}=\{0, \alpha^i / 0 \leq i \leq p^n-2\}$.
Proposition et **définition 1.16.**
Soit $\mathbb{K}$ un corps commutatif fini de car($\mathbb{K}$)=p premier et $\beta \in \mathbb{K}$. L'ensemble $I_\beta=\{P \in F_p[X] / P(\beta)=0\}$ est un idéal (principal) de $F_p[X]$. Son générateur noté M_β est appelé **polynôme minimal** de β sur F_p (ou dans $F_p[X]$).
Remarque:
Si α est une racine primitive de $\mathbb{K}$ alors le polynôme minimal M_α est appelé **polynôme primitif** de $\mathbb{K}$
Propriétés de M_β 1.17.
1) M_β est un polynôme unitaire de $F_p[X]$ qui s'annule en β.
2) Si $P \in I_\beta$ (i.e. $P(\beta) = 0$) alors M_β divise P.
3) M_β est un polynôme irréductible (premier) sur F_p.
Preuve: 1) et 2) découlent de la définition de M_β. Pour 3) soit P, $Q \in F_p[X]$: $PQ \in I \Leftrightarrow (PQ)(\beta)=0 \Leftrightarrow P(\beta)Q(\beta)=0$ et comme $F_p[X]$ est intègre alors $P(\beta)=0$ ou $Q(\beta)=0 \Rightarrow P \in I_\beta$ ou $Q \in I_\beta$ d'où I_β est premier donc d'après la proposition II.1.8.2 et M_β est premier (irréductible).
Exemple :
Soit $\mathbb{K}$ un corps commutatif fini tel que car($\mathbb{K}$)=3 et $\beta=1 \in \mathbb{K}$
$I_1=\{P \in F_3[X] / P(1)=0\}=\{ (X-1)Q / Q \in F_3[X] \}=<(X-1)>$ et $M_1=X-1$ est le polynôme minimal de $\beta=1$ sur F_3.
Proposition 1.18.
Soit $\beta \in \mathbb{K}$, l'application $\phi : F_p[X] \longrightarrow \mathbb{K}$, $P \longmapsto \phi(P)=P(\beta)$.
ϕ est un morphisme d'anneaux de noyau I_β et le corps $F_p[X]/ I_\beta$ est isomorphe à Im(ϕ).
Preuve:
Kerϕ=$\{ P \in F_p[X] / P(\beta)=0\}=I_\beta=(M_\beta)$ et donc d'après le premier théorème d'isomorphisme on a :
$F_p[X]/ \text{Ker}\phi \cong \text{Im}(\phi) \Rightarrow F_p[X]/ I_\beta \cong \text{Im}(\phi)=\{P(\beta)/P \in F_p[X]\}$ qu'on note $\mathbf{F_p[\beta].}$
Le corps $\mathbf{F_p[X]/ (M_\beta)}$ **est isomorphe à $\mathbf{F_p[\beta]}$** ensemble des polynômes d'indéterminé β sur F_p dit **extension** de F_p par β.
Remarque (exercice) : $F_p[\beta]$ est le plus petit sous-corps de $\mathbb{K}$ contenant β et F_p.
Proposition 1.19.
Si $d°(M_\beta)=n$ alors $F_p[\beta]$ est un espace vectoriel sur F_p de dimension n et admet $B=\{1,\beta^2, \ldots, \beta^{n-1}\}$ comme base.
Proposition 1.20.
Si α est une racine primitive d'un corps commutatif fini $\mathbb{K}$ alors: $\mathbb{K} \cong F_p[X]/(M_\alpha)$ où M_α est le polynôme primitif de $\mathbb{K}$.
Preuve: il suffit de montrer que $F_p[\alpha] = \mathbb{K}$. On a $\alpha \in \mathbb{K}$ alors si $P=\sum_{i\geq 0} a_i X^i \in F_p[X]$ alors $P(\alpha)=\sum_{i\geq 0} a_i \alpha^i \in \mathbb{K}$ d'où $F_p[\alpha] \subset \mathbb{K}$.
Si $x \in \mathbb{K} \Rightarrow x=0$ ou $x \in \mathbb{K}^* \Rightarrow x=0$ ou $x=\alpha^i / 0< i \leq p^n-2$ et dans les deux cas $x \in F_p[\alpha]$

Théorème de Wadderburn 1.21. Tout corps fini $\mathbb{K}$ est un corps commutatif.

Conclusion :
Tout corps fini $\mathbb{K}$ est isomorphe au corps quotient de l'anneau des polynômes sur son sous-corps premier par l'idéal engendré par le polynôme primitif de $\mathbb{K}$.

1.3.2 Existence des corps finis.

Pour p un entier premier et $n\in\mathbb{N}^*$, posons-nous les questions suivantes :

1) Si P est un polynôme unitaire et irréductible sur F_p existe-il un corps fini $\mathbb{K}$ et une racine primitive α de $\mathbb{K}$ tel que $P=M_\alpha$.
2) Existe-il un un polynôme unitaire et irréductible de degré n sur F_p.
3) Existe-il un corps fini $\mathbb{K}$ de cardinal p^n.

Remarque : Si L est un corps commutatif quelconque et $\mathbb{K}$ un sous-corps de L, en remplaçant $\mathbb{K}$ par L et F_p par $\mathbb{K}$ on peut généraliser la définition de I_β pour $\beta\in L$, et le polynôme minimal M_β de β sur $\mathbb{K}$ et ses propriétés comme dans le cas précédent.

Théorème 1.22.

Soit $\mathbb{K}$ un corps commutatif et $P\in\mathbb{K}[X]$ irréductible, unitaire et non constant alors
Il existe une extension L de $\mathbb{K}$ et $\alpha\in L$ tel que $P=M_\alpha$.

Preuve: il suffit de prendre $L=\mathbb{K}[X]/(P)$ qui est un corps commutatif et l'application
$f : \mathbb{K} \longrightarrow \mathbb{K}[X]/(P)$, $x \longmapsto f(x) = \bar{x}$ est un morphisme de corps injective donc $\mathbb{K}$ est isomorphe à $f(\mathbb{K})$ qui est un sous-corps de $\mathbb{K}[X]/(P)$ d'où L est un sur-corps de $\mathbb{K}$ et $\alpha=\bar{X}\in L$, si $P=\sum_{i=0}^{n} a_i X^i$ alors $P(\alpha)=\sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i \bar{X}^i = \sum_{i=0}^{n} a_i \overline{X^i}$
$=\overline{\sum_{i=0}^{n} a_i X^i} = \bar{P} = 0$. Donc P vérifie les propriétés dans III.2.1.7 alors $P==M_\alpha$.

Définition 1.23.

Une extension L d'un corps commutatif $\mathbb{K}$ est dite **corps de rupture** d'un polynôme P sur $\mathbb{K}$**,** si $P\in\mathbb{K}[X]$ et P admet au moins une racine $\alpha\in L$.

Exemple :

1) Si $P=aX+b\in\mathbb{K}[X]$ de degré 1, alors $\mathbb{K}$ est un corps de rupture de P et $\alpha=-ba^{-1}$ est une racine de P.
2) $P=X^2+1\in\mathbb{R}[X]$, alors le corps $L=\mathbb{C}$ est un corps de rupture de P sur $\mathbb{R}$ car $\alpha=i$ est une racine de P dans $\mathbb{C}$.

Proposition 1.24.

Si $\mathbb{K}$ est un corps commutatif et $P\in\mathbb{K}[X]$ avec $d°(P)\geq 1$ alors P admet un corps de rupture L sur $\mathbb{K}$.

Définition 1.25.

Une extension L d'un corps commutatif $\mathbb{K}$ est dite **corps de décomposition** d'un polynôme P sur $\mathbb{K}$ de degré n, si $P\in\mathbb{K}[X]$ et $P = a(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$ où $\alpha_i\in L$, $a\in\mathbb{K}$, (P est dit est **scindé** dans L).

Exemple :

1) Si $P=aX+b\in\mathbb{K}[X]$ de degré 1, alors $\mathbb{K}$ est un corps de décomposition de P car $P=a(X-ba^{-1})$
2) $P=X^2+1\in\mathbb{R}[X]$, alors le corps $L=\mathbb{C}$ est un corps de décomposition de P sur $\mathbb{R}$ car $P=(X-i)(X+i)$ tel que $\alpha_1=i$ et $\alpha_1=-i$ les racines de P dans $\mathbb{C}$.

Proposition 1.26.

Si $\mathbb{K}$ est un corps commutatif et $P\in\mathbb{K}[X]$ avec $d°(P)\geq 1$ alors P admet un corps de décomposition L sur $\mathbb{K}$.

Théorème 1.27.

Si p un entier premier et $n\in\mathbb{N}^*$, alors il existe un corps fini $\mathbb{K}$ de cardinal p^n et un polynôme irréductible $P\in F_p[X]$ et $d°(P)=n$.

Preuve: Soit $P_1= X^{p^n} - X\in F_p[X]$ et $\mathbb{K}_1$ le corps de décomposition de P_1 sur F_p alors toutes les racines de P_1 sont différentes en effet on a $P_1=XP_2$ tel que $P_2= X^{p^n-1}-1$ est de degré p^n-1, on a sa dérivé $P_2'= - X^{p^n-1}$ n'admet qu'une seule racine qui n'est pas racine de P_2 donc toutes les racines de P_2 sont différentes et l'ensemble
$\mathbb{K} =\{x\in\mathbb{K}_1,\ x^{p^n} - x = 0\}$ des racines de P_1est un corps car il est stable par l'addition et la multiplication et contient F_p et de $card(\mathbb{K})= p^n$. Si α est une racine primitive du corps $\mathbb{K}$ alors il suffit de prendre $P= M_\alpha$ le polynôme minimal associé à α alors P est un polynôme irréductible, unitaire et d'après Proposition 1.11. et Proposition 1.10, $\mathbb{K}\cong F_p[X]/\langle M_\alpha\rangle$ donc $card(\mathbb{K}) = card(F_p[X]/\langle M_\alpha\rangle$ d'où $p^n = p^{d°(P)} \Rightarrow d°(P)=n$.

Théorème 1.28. Deux corps finis $\mathbb{K}$ et $\mathbb{K}$` de même cardinal sont isomorphes.

Conséquence 1.29. Si $\mathbb{K}$ est un corps de cardinal p^n où p un entier premier et $n\in\mathbb{N}^*$ et s'il existe $P\in F_p[X]$ irréductible avec $d°(P)=n$ alors $\mathbb{K}\cong F_p[X]/\langle P\rangle$.

En effet : on a $card(F_p[X]/\langle P\rangle)= p^{d°(P)}= p^n = card(\mathbb{K})$ donc $\mathbb{K}\cong F_p[X]/(P)$.

Conclusion :
Le corps fini $\mathbb{K}$ de cardinal $q=p^n$ tel que p entier premier et $n\in\mathbb{N}^*$ est dit **corps de Galois**
Noté $F_q =F_{p^n}$.Pour décrire le corps de Galois F_q(de cardinal $q=p^n$) il suffit de connaitre une racine primitive α de F_q et son polynôme minimal M_α(dit polynôme primitif) tel que $d°(M_\alpha)=n$ et $\mathbf{F_q\cong F_p[\alpha]=\{0, 1, \alpha, \alpha^2,\ldots,\alpha^{p^n-2}\}.}$

Exemple 1 :

Description du corps de Galois $\mathbb{K} =F_9$, on a $card(F_9)=9=3^2$ donc $p=car(F_9)= 3$ et $n=2$
On a besoin d'un polynôme irréductible P de degré n=2 sur le corps $F_3=\{0, 1, 2\}$.
Soit $P=X^2+X+2\in F_3[X]$ comme $P(0)=2\neq 0$, $P(1)=1\neq 0$, $P(2)=2\neq 0$ alors P est irréductible sur F_3, et il existe une racine primitive α de F_9, de polynôme minimal $M_\alpha=P$.
On a $F_9\cong F_3[\alpha]=\{0, 1, \alpha, \alpha^2,\alpha^3, \alpha^4, \alpha^5, \alpha^6,\alpha^7\}$
$M_\alpha(\alpha)=0 \Rightarrow\alpha^2+\alpha+2=0 \Rightarrow\alpha^2 = -\alpha-2=2\alpha+1 \Rightarrow\alpha^3 = 2\alpha^2+\alpha=2\alpha+2 \Rightarrow\alpha^4 =2$,
$\alpha^5 = 2\alpha$, $\alpha^6 = \alpha+1$, $\alpha^7= \alpha$. En fin $F_9=\{0, 1, 2, \alpha, 2\alpha, \alpha+1, \alpha+2, 2\alpha+1, 2\alpha+2\}$.

Exemple 2: Décrire le corps de Galois de cardinal q=16 (F_{16}).

1.3.3 Racines nième de l'unité.

Définition 1.30. Soit n un entier non nul et $\mathbb{K}$ un corps, on appel **racine nième de l'unité** sur $\mathbb{K}$ tout élément α de $\mathbb{K}$ racine du polynôme $X^n-1 \in \mathbb{K}[X]$, c'est aussi l'ordre de α dans le groupe $\mathbb{K}^*$.
On note $G_n(\mathbb{K})$ l'ensemble des racines nièmes de l'unité dans $\mathbb{K}$ c.à.d. $G_n(\mathbb{K}) = \{x \in \mathbb{K} - \{0\} : x^n - 1 = 0\}$

Exemple.

1- Les racines troisième de l'unité sur $\mathbb{C}$ sont $\alpha_1=1$, $\alpha_2= \frac{1}{2} + \frac{1}{2}i$, $\alpha_3= \frac{1}{2} - \frac{1}{2}i$ et sur $\mathbb{R}$ ou $\mathbb{Q}$ c'est $\alpha=1$.

2- Les racines quatrièmes de l'unité sur $\mathbb{R}$ sont $\alpha_1=1$, $\alpha_2= -1$.

Rappelons le théorème suivant concernant les groupes cycliques :

Théorème 1.31. Si G est un groupe cyclique d'ordre n et $H = \{x \in G, x^k = 1\}$ l'ensemble des racines d'ordre k de l'unité alors H est un sous-groupe (cyclique) de G d'ordre $d = \mathrm{PGCD}(n, k)$.

Théorème 1.32. Groupe des racines nième de l'unité

Soit $K=F_q$ le corps de Galois de cardinal $q=p^r$ tel que $r \in \mathbb{N}^*$ et de caractéristique p premier.
L'ensemble $G_n(\mathbb{K}) = \{x \in \mathbb{K} - \{0\} : x^n - 1 = 0\}$ est un sous-groupe cyclique d'ordre $d = \mathrm{PGCD}(p^r - 1, n)$ dit **groupe des racines nièmes de l'unité** sur F_p et on a $G_n(\mathbb{K})=G_d(\mathbb{K})$.

Preuve : il suffit d'appliquer le théorème ci-dessus pour $G= K^*=F_q-\{0\}$ et $H=G_n(\mathbb{K})$

1.3.4 Corps des racines nièmes de l'unité sur F_p.

Soit p un entier premier et $n \in \mathbb{N}^*$ et cherchons un corps de décomposition $\mathbb{K}$ de X^n-1 sur F_p
c-à-d. un sur-corps $\mathbb{K}$ du corps premier F_p tel que X^n-1 se décompose en produit de polynômes premiers (pas nécessairement tous différents), i.e. $X^n-1=\prod_{i=1}^{n}(X - \beta_i)$ tel que $\beta_i \in \mathbb{K}$.

Remarque : On peut écrire l'entier n sous forme $n=Np^m$ où $N \wedge p=1$et $m \in \mathbb{N}$ on a 2 cas :

1) **$n \wedge p=1$** (n premier avec p) donc m=0et N=n.
2) **n n'est pas premier avec p** dans ce cas $n=Np^m$ et $m \neq 0$ et $N \wedge p=1$. Ce cas peut être envoyer au premier cas. C-à-d. que la décomposition de X^n-1avec n n'est pas premier avec p se déduit de celle de X^N-1 avec N premier avec p car on a :

$X^n - 1 = X^{N.p^m} - 1 = X^{N.p^m} - 1^{p^m} = (X^N - 1)^{p^m}$.

$X^n - 1 = 0 \Leftrightarrow (X^N - 1)^{p^m} = 0 \Leftrightarrow X^N - 1 = 0$ et $G_n(\mathbb{K}) = G_N(\mathbb{K})$.

Proposition et définition 1.33. Construction du corps des racines nièmes de l'unité :

Soit p un entier premier et $n \in \mathbb{N}$, il existe un unique (le plus petit) corps de décomposition de X^n-1 sur F_p , c'est le corps $\mathbb{K} = F_{p^r}$ où r est le plus petit entier non nul tel que N divise p^r-1 ce corps est dit **corps des racines nièmes de l'unité** sur F_p.
Et on a :

$X^n - 1 = \prod_{i=0}^{N-1}(X - \beta^i)^{p^m}$ avec $\beta=\alpha^s$ tel que $s = \frac{p^r-1}{N}$ ou α est une racine primitive de $\mathbb{K}$.

Preuve:

1) **si n premier avec p.** En effectuant la division Euclidienne de p par n on trouve :
$p = q.n + p_1$ avec $0 < p_1 < n \implies p \equiv p_1[n]$ on a $p \wedge n=1$ donc $p_1 \wedge n=1$ et $p_1 < n$
donc $\overline{p_1}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et soit r est l'ordre de $\overline{p_1}$ donc r est le plus petit entier non nul tel que $p_1{}^r \equiv 1[n]$ et comme $p \equiv p_1[n]$ alors $p^r \equiv 1[n] \Rightarrow p^r - 1 \equiv 0[n]$
d'où r est le plus petit entier non nul tel que n divise $p^r - 1$.
Soit $\mathbb{K}=F_{p^r}$ le corps de Galois où r est l'entier définie ci-dessus. Selon le théorème III.2.3.2 ci-dessus le groupe cyclique $G_n(\mathbb{K})$ est d'ordre $d = \mathrm{PGCD}(p^r - 1, n)=n$ car dans ce cas n divise $p^r - 1$.
Si $\beta \in K^*$ est un générateur de $G_n(\mathbb{K})$ alors $G_n(\mathbb{K}) = \langle\beta\rangle = \{1, \beta, \beta^2, \dots, \beta^{n-1}\}$ constitué de n racines distinctes de X^n-1 et X^n-1qui se décompose donc par :
$X^n - 1 = \prod_{i=0}^{n-1}(X - \beta^i)$ et donc $\mathbb{K} =F_{p^r}$ est un corps de décomposition de X^n-1 sur F_p.

Remarque : Si α est une racine primitive de $\mathbb{K}$(générateur de $\mathbb{K}^*$) alors d'après les propriétés des groupes cycliques on peut prendre β (générateur de $G_n(\mathbb{K}) = \langle\beta\rangle$) de la forme $\beta=\alpha^s$ tel que $s = \frac{p^r-1}{n}$.
Le corps $\mathbb{K}=F_{p^r}$ est le plus petit corps de décomposition de x^n-1 sur F_p.

En effet :

- Si $L =F_{p^v}$ est un autre corps de décomposition de X^n-1 sur F_p alors n divise $p^v - 1$ comme r est le plus petit entier non nul tel que n divise $p^r - 1$ alors par division Euclidienne de v par r on trouve : v=rq+t tel que $0 \leq t < r$, t=0 si non on aura :
$p^v \equiv 1[n] \wedge p^r \equiv 1[n] \Rightarrow p^v \equiv 1[n] \wedge p^{-qr} \equiv 1[n] \Rightarrow p^t = p^{v-qr} \equiv 1[n]$
Ce qui montre que t est le plus petit entier non nul tel que n divise $p^t - 1$ ce qui est bsurde,
donc t=0 et v=rq d'où r divise v et donc $\mathbb{K} =F_{p^r}$ est un sous-corps de $L =F_{p^v}$.
Donc chaque corps de décomposition L de X^n-1est un sur-corps de $\mathbb{K}$.
- Si L est un sur-corps de $K=F_{p^r}$alors L est automatiquement un corps de décomposition de de X^n-1 sur F_p.
D'où $\mathbb{K}=F_{p^r}$ est le plus petit corps de décomposition de X^n-1 sur F_p.

2) si n n'est pas premier avec p.

Soient $n=Np^m$ et $m \neq 0$ tel que $N \wedge p=1$ et r le plus petit entier non nul tel que N divise p^r-1
alors le corps $\mathbb{K} =F_{p^r}$ est le corps de décomposition de X^N-1et donc celui de X^n-1 qui se décompose par :

$X^N - 1 = \prod_{i=0}^{n-1}(X - \beta^i) \Rightarrow X^n - 1 = \prod_{i=0}^{n-1}(X - \beta^i)^{p^m}$ avec β est un générateur du groupe $G_n(\mathbb{K})$ et $\beta=\alpha^s$ tel que $s = \frac{p^r-1}{N}$ et α est une racine primitive de $\mathbb{K}$.

Exemple :
Déterminer $\mathbb{K}$ le corps des racines 15-imes de l'unité sur F_2 et décomposer X^{30}-1 sur F_2. N=15 et p=2 . Le corps concerné est $K=F_2^r$ tel que r est le plus petit entier non nul tel que N=15 divise 2^r-1 on trouve r= 4 et donc $K= F_2^4=F_{16}$.
$(X^{15}-1)=\prod_{i=0}^{14}(X-\beta^i) = (X-1)(X-\beta)\dots(X-\beta^{14})$ et $X^{30}-1=(X^{15}-1)^2=\prod_{i=0}^{14}(X-\beta^i)^2 = (X-1)^2(X-\beta)^2\dots(X-\beta^{14})^2$ et $\beta=\alpha^s=\alpha$ est une racine primitive 15-ieme de l'unité où α est une racine primitive de $\mathbb{K}$**.**

1.3.5 Décomposition de X^n-1 en produit de polynômes irréductibles sur F_p.

Soit $\mathbb{K} = F_{p^r}$ corps des racines nièmes de l'unité sur F_p et $G_n(\mathbb{K}) = \{x \in \mathbb{K}^*: x^n - 1 = 0\}$

Définition 1.34. Racines nièmes primitives de l'unité.
On appel **racine nième primitive de l'unité** tout générateur β du groupe cyclique $G_n(\mathbb{K})$.L'ensemble de ces racines nième primitive de l'unité est noté $\mathbf{P_n(\mathbb{K})}$ et donc :$P_n(\mathbb{K})=\{\beta\in G_n(\mathbb{K}) / \beta \text{ engendre } G_n(\mathbb{K})\}$.

Définition 1.35. Polynômes cyclotomiques :
Soit $\mathbb{K} = F_{p^r}$ corps des racines nièmes de l'unité sur F_p.
On appelle **Polynôme cyclotomique** d'indice n, le polynôme noté $\emptyset_n(X) \in F_p[X]$ dont ses racines sont les racines nièmes primitives de l'unité dans $\mathbb{K}$. i.e. $\emptyset_n(X) = \prod_{\varepsilon\in P_n(\mathbb{K})}(X-\varepsilon)$**.**

Définition 1.36. Fonction indicatrice d'Euler :
On appelle **Fonction indicatrice d'Euler** la fonction:

$\varphi: \mathbb{N} \longrightarrow \mathbb{N}$

$n \longmapsto \varphi(n) = \text{card}\{i \in \mathbb{N}: i < n \text{ et } i \wedge n = 1\}$

Exemple : pour n=6, $\varphi(6) = \text{card}\{1,5\} = 2$.
Rappelons le théorème suivant concernant les générateurs d'un groupe cyclique :
Théorème 1.37. Si G est un groupe cyclique d'ordre n engendré par g, alors :
$(g^k \text{ engendre } G) \Leftrightarrow 1 \le k \le n-1 \wedge k \wedge n = 1.$
L'ensemble des générateurs de G est : $P = \{g^k, 1 \le k \le n-1 \wedge k \wedge n = 1\}$et $\text{Card}(P) = \varphi(n)$

Proposition 1.38.
Soient $n\in\mathbb{N}^*$ et $\mathbb{K}= F_{p^r}$ corps des racines nièmes de l'unité sur F_p .
Si β est une racine primitive nième de l'unité, Alors l'ensemble de tous les générateurs de $G_n(\mathbb{K})$ (les racine primitives nièmes de l'unité) est : $P_n(\mathbb{K}) = \{\beta^j / 1 \le j \le n-1 \text{ et } j \wedge n = 1\}$ et $\text{card}(P_n(\mathbb{K})) = \varphi(n)$.

Proposition 1.39.
Soient $n\in\mathbb{N}^*$ et $\mathbb{K} = F_{p^r}$ le corps des racines nièmes de l'unité sur F_p. Si β est une racine primitive nième de l'unité alors Le polynôme cyclotomique $\emptyset_n(X)$ s'écrit : $\emptyset_n(x) = \prod_{\substack{1\le j\le n-1\\ j\wedge n=1}}(x-\beta^j)$et $d^\circ(\emptyset_n(X)) = \varphi(n)$.

preuve :
$\emptyset_n(x) = \prod_{\varepsilon\in P_n(K)}(X-\varepsilon)$et ε est de la forme $\varepsilon=\beta^j$ tel que $1 \le j \le n-1$et $j \wedge n = 1$
Donc $\emptyset_n(x) = \prod_{\substack{1\le j\le n-1\\ j\wedge n=1}}(x-\beta^j)$et pour le degré on a :

$$d^\circ(\emptyset_n(X)) = d^\circ\left(\prod_{\substack{1\le j\le n-1\\ j\wedge n=1}}(X-\beta^j)\right) = \sum_{\substack{1\le j\le n-1\\ j\wedge n=1}} d^\circ(x-\beta^j) = \sum_{\substack{1\le j\le n-1\\ j\wedge n=1}} 1 = |P_n(K)| = \varphi(n).$$

Proposition 1.40.
Soient $n\in\mathbb{N}^*$ et p premier tel que n premier avec p et $\mathbb{K} = F_{p^r}$ corps des racines nièmes de l'unité sur F_p.
Alors le polynôme X^n-1 se décompose par : $X^n - 1 = \prod_{d/n} \emptyset_d(x)$**.**

Preuve :
Comme $n\wedge p=1$ alors si β est une racine primitive nième de l'unité le groupe $G_n(\mathbb{K}) = \{1, \beta, \dots, \beta^{n-1}\}$ est de cardinal n. si d divise n on note $P_d(K)$ l'ensemble des racines primitive d'ordre d de l'unité. Il est évident que $P_d(\mathbb{K}) \subset G_n(\mathbb{K})$ et la famille $\{P_d(\mathbb{K})\}_{d/n}$ forme une partition de $G_n(\mathbb{K})$ (exercice) et on a
$X^n - 1 = \prod_{\varepsilon\in G_n(K)}(X-\varepsilon) = \prod_{d/n}\left(\prod_{\varepsilon\in P_d(K)}(X-\varepsilon)\right)$ or $\left(\prod_{\varepsilon\in P_d(K)}(X-\varepsilon)\right)$ n'est que le polynôme cyclotomique $\emptyset_d(x)$ d'où $X^n - 1 = \prod_{d/n}\emptyset_d(x)$.

Conséquence 1.41. Si n n'est pas premier avec p alors $n=N.p^m$avec $N\wedge p=1$ et $x^n - 1 = \prod_{d/n}[\emptyset_d(x)]^{p^m}$.

Preuve : il suffit d'après Proposition 1.40. de décomposer $X^N - 1 = \prod_{d/N}\emptyset_d(x)$.
Et on a $x^n - 1=(x^N - 1)^{p^m} \Rightarrow x^n - 1 = \prod_{d/n}[\emptyset_d(x)]^{p^m}$.

Proposition 1.42. Si $n\in\mathbb{N}^*$ et p premier tel que n premier avec p. Alors les polynômes cyclotomiques $\emptyset_n(x)$sont des polynômes unitaires à coefficients dans F_p.

Preuve :
On démontre par récurrence sur n.
Si n=1, $\emptyset_1(x)$=X-1 donc unitaire et $\emptyset_1(x)\in F_p[X]$. On suppose que pour tout m < n : $\emptyset_m(x)$ unitaire et $\emptyset_m(x)\in F_p[X]$.
On a :$X^n - 1 = \prod_{d/n}\emptyset_d(x) = \prod_{d/n, d\neq n}\emptyset_d(x).\ \emptyset_n(x)= P(x).\emptyset_n(x)$ avec $P(x) = \prod_{d/n, d\neq n}\emptyset_d(x)$on a : $\forall d/n$ alors d<n et donc $\emptyset_d(x)$ est unitaire $\emptyset_d(x)\in F_p[X]$ donc P(X) est unitaire et $P(X)\in F_p[X]$ et comme X^n-1$\in F_p[X]$ est unitaire alors $\emptyset_n(x)\in F_p[X]$ et unitaire.

1.3.6 Calcul direct des polynômes cyclotomiques.

Proposition 1.43.

Si p est un entier premier alors $\emptyset_p(x) = x^{p-1} + \ldots\ldots + x + 1$.

Preuve :

$x^p - 1 = \prod_{d/p} \emptyset_d(x) = \emptyset_1(x)\emptyset_p(x) = (x-1)\emptyset_p(x)$ donc $\emptyset_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Exemple :

$\emptyset_2(x) = x + 1$, $\emptyset_3(x) = x^2 + x + 1$, $\emptyset_5(x) = x^4 + x^3 + x^2 + x + 1$

Conséquence 1.44.

Si p un entier premier et $k \in \mathbb{N}^*$ alors : $\emptyset_{p^k}(x) = x^{(p-1)p^{k-1}} + x^{(p-2)p^{k-1}} + \ldots + x^{2p^{k-1}} + x^{p^{k-1}} + 1 = \frac{x^{p^k}-1}{x^{p^{k-1}}-1}$

Preuve:

$x^{p^k} - 1 = \prod_{d/p^k} \emptyset_d(x) = \emptyset_{p^k}(x) \prod_{d/p^{k-1}} \emptyset_d(x) \Rightarrow x^{p^k} - 1 = \emptyset_{p^k}(x)\left(x^{p^{k-1}} - 1\right) \Rightarrow \emptyset_{p^k}(x) = \frac{x^{p^k}-1}{x^{p^{k-1}}-1}$.

Remarque : $\emptyset_{p^k}(x) = \frac{x^{p^k}-1}{x^{p^{(k-1)}}-1} = \frac{\left(x^{p^{k-1}}\right)^p - 1}{x^{p^{k-1}}-1} = \emptyset_p\left(x^{p^{k-1}}\right)$.

Exemples :

$\emptyset_2(x) = x + 1$, $\emptyset_3(x) = x^2 + x + 1$, $\emptyset_5(x) = x^4 + x^3 + x^2 + x + 1$

$\emptyset_4(x) = \emptyset_{2^2}(x) = x^2 + 1$, $\emptyset_8(x) = \emptyset_{2^3}(x) = \frac{x^8-1}{x^4-1} = \emptyset_2(x^4) = x^4 + 1$.

Théorème 1.45.

Soit p entier premier et $n \in \mathbb{N}^*$,

1) si p divise n alors : $\emptyset_{np}(x) = \emptyset_n(x^p)$.

2) si p ne divise pas n alors : $\emptyset_{np^k}(x) = \frac{\emptyset_n(x^{p^k})}{\emptyset_n(x^{p^{k-1}})}$ et en particulier $\emptyset_{np}(x) = \frac{\emptyset_n(x^p)}{\emptyset_n(x)}$.

Exemples :

$\emptyset_{15}(x) = \emptyset_{3.5}(x) = \frac{\emptyset_3(x^5)}{\emptyset_3(x)} = \frac{x^{10}+x^5+1}{x^2+x+1} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$.

$\emptyset_{18}(x) = \emptyset_{2.3^2}(x) = \frac{\emptyset_2(x^{3^2})}{\emptyset_2(x^3)} = \frac{x^9+1}{x^3+1} = x^6 - x^3 + 1$ ou encore

$\emptyset_{18}(x) = \emptyset_{6.3}(x) = \emptyset_6(x^3) = \emptyset_{2.3}(x^3) = \frac{\emptyset_3((x^3)^2)}{\emptyset_3(x^3)} = \frac{x^{12}+x^6+1}{x^6+x^3+1} = x^6 - x^3 + 1$.

1.3.7 Décomposition de X^n-1 en polynômes irréductibles sur F_p.

Théorème 1.46.

Soient p premier, $n \in \mathbb{N}^*$ et $\mathbb{K} = F_{p^r}$ le corps des racines nièmes de l'unité sur F_p .

Alors $\emptyset_n(x)$ se décompose en produit de φ(n)/r polynômes irréductibles de degré r et à coefficients dans F_p.

Preuve :

Soit $\mathbb{K} = F_{p^r}$ le corps des racines nièmes de l'unité sur F_p.

Soit β une racine nieme primitive de l'unité et posons $I_n = \{i \in 1, n:\ i \wedge n = 1\}$ et on a: $p^r = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ et donc $\forall i \in I_n : p^r i = i$ dans $\mathbb{Z}/n\mathbb{Z}$ et comme i est premier avec n alors, les ensembles $J_i = \{i, pi, \ldots, p^{r-1}i\}$ où $i \wedge n = 1$ (dits **classes cyclotomiques**) sont de cardinal r et forment une partition à I_n c.à.d $I_n = \bigcup_{t=1}^{t=k} J_t$.

$\emptyset_n(X) = \prod_{\varepsilon \in P_n(K)}(X - \varepsilon) = \prod_{j \wedge n = 1}(X - \beta^j) = \prod_{j \in I_n}(X - \beta^j) = \prod_{j \in \bigcup_{t=1}^{t=k} J_t}(X - \beta^j)$ avec $card(J_t) = r$ alors:

$\emptyset_n(X) = \prod_{j \in J_1}(X - \beta^j) \prod_{j \in J_2}(X - \beta^j) \ldots \prod_{j \in J_k}(X - \beta^j)$.

Si j_i est le représentant de la classe J_i, alors pour tout $i \in [1,k]$: $\prod_{j \in J_i}(X - \beta^j) = \prod_{l=0}^{r-1}\left(X - \beta^{j_i p^l}\right)$

Lemme 1.47.

Soit β est un élément d'un corps fini $\mathbb{K}$ de caractéristique p , et soit M_β le polynôme minimal de β de degré r alors :

1) Les éléments $\beta, \beta^p, \ldots, \beta^{p^{r-1}}$ (dits conjugués de β) sont distincts.
2) M_β s'écrit : $M_\beta = \prod_{l=0}^{r-1}\left(X - \beta^{p^l}\right)$ et $\forall l \in [1,r-1] : M_\beta = M_{\beta^{p^l}}$.

D'après le lemme ci-dessus : $\emptyset_n(x) = M_{\beta^{j_1}} M_{\beta^{j_2}} \ldots M_{\beta^{j_k}}$ qui est le produit de $k = \varphi(n)/r$ polynômes irréductibles, car on a: $d°(\emptyset_n(X)) = k\,d°(M_{\beta^{j_1}}) \Rightarrow \varphi(n) = k.r \Rightarrow k = \varphi(n)/r$.

Exemple :

Soit n=15 et p=2, le corps des racines 15-èmes de l'unité est $\mathbb{K} = F_{2^r}$ où r est le plus petit entier non nul tel que n=15 divise 2^r-1 on trouve que r=4, donc $\emptyset_{15}(x)$ se décompose en produit de φ (15)/r = 8/4 = 2 polynômes irréductibles de degré r=4

c.à.d. $\emptyset_{15}(X) = (X^4 + aX^3 + bX^2 + cX + 1)(X^4 + a'X^3 + b'X^2 + c'X + 1)$

$\emptyset_{15}(X) = \emptyset_{3.5}(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1$.

Après développement et identification on trouve : $a = b = b' = c' = 0$ et $c = a' = 1$

$\emptyset_{15}(X) = (X^4 + X + 1)(X^4 + X^3 + 1)$.

Conséquence 1.48.

Soient p premier, $n \in \mathbb{N}^*$ tel que $n \wedge p = 1$ et soit $\mathbb{K} = F_{p^r}$ le corps des racines nièmes de l'unité.

Si $\varphi(n)=r$ alors $\emptyset_n(x)$ est un polynôme irréductible.

Preuve : comme $\varphi(n)=r$ alors $k=1$ et $\emptyset_n(x)= M_\beta$ qui est un polynôme irréductibles

Exemple 1: soient $p=3$ et $n=5$. Le corps de décomposition de X^5-1 sur F_3

Est $\mathbb{K}= F_{3^r}$ où r est le plus petit entier non nul tel que $n=5$ divise 3^r-1 on trouve que $r=4$

on a $\varphi(5) = 4$ donc $\emptyset_5(X) = X^4 + X^3 + X^2 + X + 1$ est irréductible sur F_3.

Exemple 2: La décomposition de X^9-1 sur F_2 donne:

$X^9-1=\emptyset_1(X).\emptyset_3(X).\emptyset_9(X)$ = (X-1)(X^2+X+1) (X^6+X^3+1). L'ordre de p=2 dans $\mathbb{Z}/9\mathbb{Z}$ est r=6 donc le corps des racines 9-emes de l'unité est $\mathbb{K}= F_{2^6}$ et $\varphi(9)=6=r$ donc $\emptyset_9(X)$ est irréductible.

Théorème 1.49. (Décomposition de x^n-1 en produit de polynômes irréductibles).

Soient p premier, $n\in\mathbb{N}^*$ tel que $n\wedge p=1$. Alors le polynôme X^n-1 se décompose en produit de polynômes irréductibles sur F_p.

Preuve : il suffit d'appliquer la proposition 1.40 et sa Conséquence 1.41 et le Théorème 1.47

Et sa Conséquence 1.48.

Remarque : Si n n'est pas premier avec p alors $n=Np^m$ avec $N\wedge p=1$, on applique le théorème ci-dessus, en décomposant le polynôme X^N-1 et on en déduit la décomposition de X^n-1.

Exemple 1:

Décomposer le polynôme X^5-1 en polynômes irréductibles sur F_2. Soit $\mathbb{K}= F_{2^r}$ le corps des racines nièmes de l'unité sur F_2.

$n=5$ premier avec $p=2$. le plus petit entier non nul r tel que $n=5$ divise 2^r-1 est $r=4$ donc $\mathbb{K}= F_{2^4}$. $X^5-1= \prod_{d/5} \emptyset_d(x)=$ $\emptyset_1(x).\emptyset_5(x)= (X-1)\emptyset_5(x)$.

Décomposons $\emptyset_5(x)$ en produit de polynômes irréductibles sur F_2. On a $\varphi(5)=4=r$ et donc

$\emptyset_5(X) = X^4 + X^3 + X^2 + X + 1$ est irréductible sur F_2.

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

Exemple 2 :

Décomposer le polynôme X^{15}-1 sur F_3. $n=15$ et $p=3$, n n'est pas premier avec p et $n=Np^m$

Tel que $N=5$ premier avec $p=3$ et $m=1$, Soit $\mathbb{K}= F_{3^r}$ le corps des racines nièmes de l'unité sur F_3. le plus petit entier non nul r tel que $N=5$ divise 3^r-1 est $r=4$ donc $\mathbb{K}= F_{3^4}$.

$X^5-1= \prod_{d/5} \emptyset_d(x)= \emptyset_1(x).\emptyset_5(x)= (X-1)\emptyset_5(x)$ or $\emptyset_5(X) = X^4 + X^3 + X^2 + X + 1$

est irréductible sur F_3. Donc $X^{15}-1=(X^5-1)^3 =(X-1)^3(X^4 + X^3 + X^2 + X + 1)^3$.

Exemple 3 : TD

Décomposer les polynômes X^{15}-1 , X^9-1, X^{18}-1 sur F_2 et F_3 et F_5.