# Elements mathématiques pour le codage

## 0. Rappels L'anneau des polynômes $(\boldsymbol{K}[\boldsymbol{X}],+,.)$

**On se contentera de rappeler que l'ensemble K[X] , muni de l'addition et de la multiplication est un anneau (cf algèbre appliquée au cryptage); on y connait la division euclidienne des polynômes, qui permet de définir la divisiblité d'un polynôme par un autre; puis le pgcd de deux polynômes A(X) et B(X) qui est le polynôme unitaire de plus haut degré qui les divise tous les deux.**

**Exercice 1. Effectuer la division euclidienne de** $X^6-X^4+X^2+1$ **par** $\mathbf{X}^3+\mathbf{X}^2+\mathbf{X}+1$

**Exemple 1. Calculs polynomiaux avec maxima**

**L 'addition de polynômes P:(x^3+x^2+2*x)+(x^4+3*x+5);**

**La multiplication de polynômes: P:(x^3+x^2+2*x)*(x^4+3*x+5); expand(P);**

**La division euclidienne de polynômes P:divide(x^5+x^2+2*x,x^4+3*x+5) donnera le quotient, suivi du reste.**

**gcd(P,Q) donne le pgcd des deux polynômes P et Q**

**Théorème 2.**

**Dans K[X], comme dans $\mathbb{Z}$, on connaît l'identité de Bezout:**

**Si A(X) et B(X) sont deux polynômes et si D(X) désigne leur pgcd il existe deux polynômes (U(X)),V(X)) tels que A(X)U(X)+B(X)V(X)=D(X)**

**La manière efficace de trouver U(X) et V(X) est l'algorithme d'Euclide étendu (cf algèbre appliquée au cryptage).**

| | | |
|---|---|---|
| $r$ | $u$ | $v$ |
| $r_0=a$ | $u_0=1$ | $v_0=0$ |
| $r_1=b$ | $u_1=0$ | $v_1=1$ |
| $\ldots$ | $\ldots$ | $\ldots$ |
| $r_{k-1}$ | $u_{k-1}$ | $v_{k-1}$ |
| $r_k$ | $u_k$ | $v_k$ |
| $r_{k+1}=r_{k-1}-(r_{k-1}:r_k)r_k$ | $u_{k+1}=u_{k-1}-(r_{k-1}:r_k)u_k$ | $v_{k+1}=v_{k-1}-(r_{k-1}:r_k)v_k$ |
| $\ldots$ | $\ldots$ | $\ldots$ |
| $r_n=a\wedge b$ | $u$ | $v$ |
| $0$ | $\text{on } s'\text{en fiche}$ | $\text{de même}$ |

**Exercice 2.**

**a. Montrer que** $X^2+X+1\wedge X+1=1$

**b. Déterminer deux polynômes U(X) et V(X) tels que** $(X^2+X+1)U(X)+(X+1)V(X)=1$

**b. Déterminer** $D(X)=X^3+3X^2+3X+1\wedge X^2-1$

**c. Déterminer deux polynômes U(X) et V(X) tels que** $(X^3+3X^2+3X+1)U(X)+(X^2-1)V(X)=D(X)$

**Solution.**

| | | | | | |
|---|---|---|---|---|---|
| | $r$ | $u$ | $v$ | $q$ |
| | $X^3+3X^2+3X+1$ | 1 | 0 | |
| **b.** | $X^2-1$ | 0 | 1 | |
| | $4X+4$ | 1 | $-X-3$ | $X+3$ |
| | 0 | | | $X/4-1/4$ |

**donc** $D(X)=X^3+3X^2+3X+1\wedge X^2-1=$**X+1**

**c.** $(X^3+3X^2+3X+1)1+(X^2-1)(-X-3)=4X+4$

**d'où** $(X^3+3X^2+3X+1)1/4+(X^2-1)(-X/4-3/4)=X+1$

# 1. Corps premiers F$p$

**Définition 3.** ***si p est premier on désigne par $F_p$ l'anneau $(\mathbb{Z}/p\mathbb{Z},+,.)$.***

**Théorème 4.** ***Soit p un entier premier***

***1) L'anneau $(\mathbb{Z}/p\mathbb{Z},+,.)$ possède p éléments.***

***2)*** $\forall x\in\mathbb{Z}, x\wedge p=1\Longrightarrow\exists u\in\mathbb{Z}, \mathrm{ux}\equiv 1[p]$

***c'est à dire: 2')*** $\forall\bar{x}\in(\mathbb{Z}/p\mathbb{Z})^*, \exists\bar{u}\in(\mathbb{Z}/p\mathbb{Z})^*, \bar{x}\,.\bar{u}=\bar{1}$.

***(ce qui permet de conclure que $((\mathbb{Z}/p\mathbb{Z})^*$,.) est un groupe).***

**Théorème 5.** ***petit théorème de Fermat***

***Soit p un entier premier*** $\forall\bar{x}\in(\mathbb{Z}/p\mathbb{Z})^*, \bar{x}^{\,p-1}=\bar{1}$.

**Théorème 6.** ***Quel que soit l'entier premier p le groupe $((\mathbb{Z}/p\mathbb{Z})^*$,.) est cyclique, c'est à dire***

***1) il existe*** $\bar{\alpha}\in(\mathbb{Z}/p\mathbb{Z})^*$ ***tel que*** $\forall\bar{x}\in(\mathbb{Z}/p\mathbb{Z})^*, \exists k\in\{0,...,p-1\}, \bar{x}=\bar{\alpha}^k$.

***2) il existe*** $\bar{\alpha}\in(\mathbb{Z}/p\mathbb{Z})^*$ ***d'ordre p-1***

***3)*** $F_p=\{\bar{0},\bar{\alpha},\bar{\alpha}^2,....,\bar{\alpha}^{p-1}\}$

**Exemple 7. Un cas simple $((\mathbb{Z}/7\mathbb{Z})^*$,.)**

**il a 6 éléments:** $\{\bar{1},\bar{2},\bar{3},\bar{4},\overline{5,\bar{6}}\}$,

$\bar{3}^1=\bar{3}$,$\bar{3}^2=\bar{2}$, $\bar{3}^3=\bar{6}$, $\bar{3}^4=\bar{4}$, $\bar{3}^5=\bar{5}$,$\bar{3}^6=\bar{1}$, **donc $\bar{3}$ est un générateur du groupe $((\mathbb{Z}/p\mathbb{Z})^*$,.).**

**Définition 8.** ***Corps***

***Un corps est un anneau (A,+,.) où , de plus, tout élément autre que 0 est inversible.***

**Exemple 9.** $\mathbb{Q},\mathbb{R},\mathbb{C}$

**$\mathbb{Z}/n\mathbb{Z}$ lorsque n est premier**

**mais pas $\mathbb{Z}/n\mathbb{Z}$ lorsque n n'est pas premier.**

**Exercice 3.**

**1) Déterminer tous les générateurs du groupe $((\mathbb{Z}/11\mathbb{Z})^*$,.)**

**2) Donner une bonne raison pour expliquer que l'ensemble $((\mathbb{Z}/38\mathbb{Z},+,.)$ n'est pas un corps.**

**Solution.**

**1)** $\bar{1}$ **n'engendre que lui-même**

**les puissances de** $\bar{2}$ **:** $\bar{2}$, $\bar{4}$, $\bar{8}$, $\bar{5}$, $\overline{10}$, $\bar{9}$, $\bar{7}$, $\bar{3}$, $\bar{6}$, $\bar{1}$ **donc** $\bar{2}$ **est un générateur**

**les puissances de** $\bar{3}$ **:** $\bar{3}$, $\bar{9}$, $\bar{5}$, $\bar{4}$, $\bar{1}$ **donc** $\bar{3}$ **n'est pas un générateur**

**les puissances de** $\bar{4}$ **:** $\bar{4}$, $\bar{5}$, $\bar{9}$, $\bar{3}$, $\bar{1}$ **donc** $\bar{4}$ **n'est pas un générateur**

**les puissances de** $\bar{5}$ **:** $\bar{5}$, $\bar{3}$, $\bar{4}$, $\bar{9}$, $\bar{1}$, **donc** $\bar{5}$ **n'est pas un générateur**

**les puissances de** $\bar{6}$ **:** $\bar{6}$, $\bar{3}$, $\bar{7}$, $\bar{9}$, $\overline{10}$, $\bar{5}$, $\bar{8}$, $\bar{4}$, $\bar{2}$, $\bar{1}$ **donc** $\bar{6}$ **est un générateur**

**les puissances de** $\bar{7}$ **:** $\bar{7}$, $\bar{5}$, $\bar{2}$, $\bar{3}$, $\overline{10}$, $\bar{4}$, $\bar{6}$, $\bar{9}$, $\bar{8}$, $\bar{1}$ **donc** $\bar{7}$ **est un générateur**

**etc...**

**Remarque 10.**

**Pour la suite nous travaillerons eseentiellement avec les corps** $F_2$ **et** $F_3$**.**

$\mathbf{F_2}$ **deux éléments 0 et 1: 0+0=0, 0+1=1+0=1; 0*0=0, 1*1=1**

$\mathbf{F_3}$ **trois éléments 0,-1 et 1:**

**0+0=0, 0+1=1+0=1,0+(-1)=(-1)+0=-1; 1+(-1)=(-1)+1 mais attention 1+1=-1; (-1)+(-1)=1 !!! (-1)*(-1)=1**

**0*0=0, 1*1=1,(-1)*0=0*(-1)=0, (-1)*1=1*(-1)=-1,**

# 2. Corps construit par quotient de l'anneau des polynômes

**Nous allons fabriquer de nouveaux corps en suivant le même schéma que pour fabriquer** $\mathbb{Z}/n\mathbb{Z}$**.**

**Définition 11.** ***L'ensemble des polynômes à coefficients dans $F_p$ ( p est un entier premier)***

***On désigne par $F_p[X]$ l'ensemble des polynômes à coefficients dans $F_p$***

**Définition 12.** ***Un polynôme P(X), de degré d $\geqslant$1, à coefficients dans $F_p$ sera dit irréductible lorsqu'il n'est divisible par aucun polynôme non constant de degré strictement inférieur.***

**Exemple 13.**

**Les polynômes de degré un sont toujours irréductbles**

**Soit p=3 et le corps $F_3$ que l'on peut écrire $\{0,1,-1\}$ (ou $\{0,1,2\}$), recherchons les polynômes irréductibles de degré deux.**

**1. Liste des polynômes de degré deux:**

$X^2, -X^2, X^2+X, -X^2+X, X^2-X, -X^2-X, \text{etc....}$ **il y en a 3*3*3=27**

**2. Les polynômes $X^2+1, X^2+X-1, X^2-X-1$ sont irréductibles:**

**Ecrivons** $X^2+1=(\mathrm{aX}+b)(\mathrm{cX}+d)$ **ce qui exige** $\left\{\begin{array}{l}\mathrm{ac}=1\\ \mathrm{ad}+\mathrm{bc}=0\\ \mathrm{bd}=1\end{array}\right.$ **, d'où** $\left\{\begin{array}{l}a=c=1 \,\mathrm{ou}\, a=c=-1\\ \mathrm{ad}+\mathrm{bc}=0\\ b=d=1 \,\mathrm{ou}\, b=d=-1\end{array}\right.$

**d'où 1+1=2=-1 ou -1+ -1=-2=1 ce qui est impossible, donc il est irréductible dans $F_3[X]$.**

**et ce sont les seuls parmi les polynômes de degré 2 (au signe près).**

**Exercice 4.**

**1. Vérifier que $X^2+X-1$ est irréductible dans $F_3[X]$**

**2. Vérifier que $X^2+X$ n'est pas irréductible dans $F_3[X]$**

**Solution.**

**1. Si $X^2+X-1$ =(aX+b)(cX+d) alors** $\left\{\begin{array}{l}\mathrm{ac}=1\\ \mathrm{ad}+\mathrm{bc}=1\\ \mathrm{bd}=-1\end{array}\right.$ **d'où**

**a=c=1 ou a=c=-1**

**b=1 et d=-1 ou b=-1 et d=1**

**si a=c=1 et b=1,d=-1 alors ad+bc= 1*(-1)+1*(1)=0$\neq$1**

**si a=c=1 et b=-1,d=1 alors ad+bc=1*1+(-1)*1=0$\neq$1 aussi**

**si a=c=-1 et b=1,d=-1 alors ad+bc= (-1)*(-1)+1*(-1)=0$\neq$1**

**si a=c=-1 et b=-1,d=1 alors ad+bc=(-1)*1+(-1)*(-1)=0$\neq$1 aussi**

**d'où .......**

**2. X$^2$+X=X(X+1)**

**Définition 14.** ***Soit un corps premier $F_p$ et un polynôme P(X) à coefficients dans $F_p$, irréductible et de degré d;***

***On désigne par $F_p\,[X]/P(X)$ l'ensemble des classes de congruence de $F_p\,[X]$ modulo P(X).***

***1. Concrètement $F_p\,[X]/P(X)$ sera constitué par l'ensemble des polynômes à coefficients dans $F_p$ de degré strictement inférieur à d.***

***2. Les calculs dans $F_p[X]/P(X)$ se font « modulo P(X) », c'est à dire que la « somme » A(X)$\oplus$ B(X) ce sera le reste de la division de A(X)+B(X) par P(X); et le « produit » A(X)$\odot B(X)$ ce sera le reste de la division de A(X)B(X) par P(X).***

***On utilise une notation spéciale pour la classe de X (par exemple $\omega$)***

***et bien sûr la classe de P(X) c'est 0.***

**Exemple 15.**

**On considère le polynôme $X^2+1$ qui est irréductible dans $F_3[X]$ et l'ensemble $F_3\,[X]/(X^2+1)$**

**(pour alléger on désignera la classe de X par $\omega$)**

$(\omega+1)\odot(\omega-1)$=**la classe du reste de la division euclidienne de $X^2-1$ par $X^2+1$, c'est à dire 1**

$(\omega+1)\odot(\omega-1)$=**1**

**Exercice 5.**

**Dans** $F_3\,[X]/(X^2+1)$

1. **Calculer** -$\omega\odot(\omega+1)$
2. **Calculer** $(\omega-1)\odot(\omega-1)\odot(-\omega-1)$

**Solution.**

**1.** -$\omega\odot(\omega+1)$= **la classe de** $-X^2-X$; **la division euclidienne de** $-X^2-X$ **par** $(X^2+1)$ **donne**

$-X^2-X$=**-1**$(X^2+1)$+ **(-X+1)**

**donc** -$\omega\odot(\omega+1)$=$-\omega+1$

**2.** $(\omega-1)\odot(\omega-1)\odot(-\omega-1)$= **la classe de** $(X-1)(X-1)(-X-1)$;

**soit on multiplie et on réduit ensuite modulo** $X^2+1$

**c'est à dire** $(X-1)(X-1)(-X-1)$=**-X$^3$-1**

**puis -X$^3$-1=-X(X$^2$+1)+X-1**

**donc** $(\omega-1)\odot(\omega-1)\odot(-\omega-1)$=$\omega-1$

**soit on calcule pas à pas:**

$(\omega-1)\odot(\omega-1)$= **classe de** $(X-1)(X-1)$=$X^2-X+1$= **classe de -X**=$-\omega$

**puis** -$\omega\odot(-\omega-1)$= **classe de** $X^2+X$=**classe de X-1**=$\omega-1$

**Théorème 16.** ***Soit un corps premier $F_p$ et un polynôme P(X) à coefficients dans $F_p$, irréductible et de degré d;***

***On désigne par $F_p\,[X]/P(X)$ l'ensemble des classes de congruence de $F_p\,[X]$ modulo P(X).***

***1) Si on munit $F_p[X]/P(X)$ de l'addition modulo P(X) et de la multiplication modulo P(X) il devient un corps.***

***2) Par ailleurs $F_p[X]/P(X)$ est un $F_p$ espace vectoriel de base $\left(\bar{1}, \bar{X}, \overline{X^2}, \ldots., \overline{X^{d-1}}\right)$; par suite il possède $p^d$ éléments.***

***3) Il contient $F_p = \{\bar{0}, \bar{1}, \ldots., \overline{p-1}\}$.***

***On peut démontrer qu'il n'y a qu'un seul type de corps possédant $p^d$ éléments, on le notera $F_{p^d}$***

**Exemple 17.** $F_3[X]/(X^2+1) = \{0, 1, -1, \omega, -w, \omega+1, \omega-1, -\omega+1, -\omega-1\}$ **: 9 éléments**

**On l'appellera $\mathbf{F}_9$.**

**On cherche l'inverse de $\omega$ :**

**Pour cela on va déterminer U et V tels que** $\mathrm{XU}(X) + (X^2+1)V(X) = 1$**; appliquons l'algorithme d'Euclide enrichi**

| | $U$ | $V$ |
|---|---|---|
| $X^2+1$ | $1$ | $0$ |
| $X$ | $0$ | $1$ |
| $X^2+1-X\times X$ | $1$ | $-X$ |

**Donc** $(X^2+1)\times 1 - X\times X = 1.$

**C'est à dire 0**$\odot 1 - \omega\odot\omega$**=1**

**d'où** $-\omega\odot\omega = 1$ **donc** $\omega^{-1} = -\omega$**.**

**Exercice 6. On considère encore** $F_3[X]/(X^2+1) = \{0, 1, -1, \omega, -w, \omega+1, \omega-1, -\omega+1, -\omega-1\}$

**Déterminer l'inverse de** $-\omega-1$**.**

**Solution. On applique l'algorithme d'Euclide enrichi**

$X^2+1$=**(-X+1)(-X-1)-1**

| $q$ | $r$ | $U$ | $V$ |
|---|---|---|---|
| | $X^2+1$ | $1$ | $0$ |
| | $-X-1$ | $0$ | $1$ |
| $-X+1$ | $-1$ | $1$ | $X+1$ |

**d'où classe de 1**$(X^2+1)$ + **(X-1)(-X-1)=-1**

**et donc -1**$(X^2+1)$ + **(-X+1)(-X-1)=1**

**d'où l'inverse de** $-\omega-1$ **est** $-\omega+1$

**Problème 1.** On considère cette fois $F_3[X]$ et le polynôme $X^2+X-1$ qui est aussi irréductible (admis)

1. Donner la liste des 9 éléments de $F_3[X]/(X^2+X-1)$; on désignera la classe de X par $\theta$
2. Calculer $(\theta^2+1)\oplus(\theta-1)$
3. Calculer $(\theta^2+1)\odot(\theta-1)$

**Théorème 18.** *Calcul du produit de P(X) et Q(X) dans* $F_3[X]/(X^2+1)$ *avec maxima*

*On utilisera les deux procédures suivantes*

*multiplymodulo(P,Q,modulo):=block([U],U:second(divide(P*Q,modulo)),return(U))$*

*fabr(U):=block([a0,a1],a0:mod(coeff(U,x,0),3),a1:mod(coeff(U,x,1),3),,return(a0+a1*x))$*

# Travaux dirigés

**Exercice 7.** On considère cette fois $F_3[X]$.

1. Vérifier que le polynôme $X^2+X-1$ qui est irréductible dans $F_3[X]$.
1. Donner la liste des 9 éléments de $F_3[X]/(X^2+X-1)$; on désignera la classe de X par $\theta$
2. On sait , d'après le cours, que $(F_3[X]/(X^2+X-1), \oplus, \odot)$ est un corps

a. Déterminer pour chaque élément non nul son inverse.

ces éléments s'écrivent aussi:0, $\theta$,$\theta^2,\theta^3,\theta^4,\theta^5,\theta^6,\theta^7,\theta^8$.

Ecrire chacun des éléments non nuls sous les deux formes: une puissance de $\theta$ et une combinaison linéaire de puissances de $\theta$ (y compris si nécessaire $\theta^0=1$).

3. Pour chaque élément non nul écrire son inverse sous la forme d'une combinaison linéaire de puissances de $\theta$ (y compris si nécessaire $\theta^0=1$).

**Exercice 8.** Même chose avec $X^2-X-1$

**Exercice 9.**

1) Déterminer un polynôme de degré 3 irréductible dans $F_3[X]$; on notera ce polynôme P(X)

2) Etude du corps $F_3[X]/P(X)$: son nombre d'éléments, les deux lois, les inverses.

**Exercice 10.** On considère désormais l'ensemble des matrices carrées, 2 lignes et 2 colonnes, à coefficients dans

K=$F_3[X]/(X^2+1)$ et on admet que les opérations, le déterminant, l'inverse, quand il existe, se calculent comme en première année, avec les matrices à coefficients réels.

1. Calculer $\begin{pmatrix} 1 & \omega \\ \omega & 1 \end{pmatrix}\begin{pmatrix} \omega & 1 \\ 1 & \omega \end{pmatrix}$ où $\omega$ désigne la classe de X.
2. Déterminer si la matrice A=$\begin{pmatrix} 1 & \omega \\ \omega & 1 \end{pmatrix}$ est inversible et, si oui, trouver son inverse.

---

?

**Exemple 19.** Reprenons $F_3$

**1) On considère le polynôme $X^2+1$ qui est irréductible dans $F_3[X]$**

**on obtient $F_9$ de la manière suivante**

$F_9=\{a+b\omega, a=0,1,2, b=0,1,2\}$ **avec des règles de calcul**

$a+b\omega$+$a'+b'\omega$=**(a+a')*mod(3)* + $\omega$(b+b') mod(3)**

$(a+b\omega)$ .$(a'+b'\omega)$=**c+d$\omega$, où on multiplie mod(3)) les polynômes $(a+\mathrm{b}X)$ +$(a'+b'X)$ dans $F_3\,[X]$ et on « réduit modulo $X^2+1$ » pour obtenir c+dX.**

**On peut aussi dire, qu'on agit comme dans $\mathbb{C}$, en posant $\omega^2=-1$.**

**2) Si on considère le polynôme $X^2+X-1$ on obtient $F_9$ de la manière suivante**

$F_9=\{a+b\theta, a=0,1,2, b=0,1,2\}$ **avec des règles de calcul**

$a+b\theta$+$a'+b'$=**(a+a')*mod(3)* + $\theta$(b+b') mod(3)**

$(a+b\theta)$.$(a'+b'\theta)$=**c+d$\theta$, où on multiplie mod(3)) les polynômes $(a+\mathrm{b}X)$+$(a'+b'X)$ dans $F_3\,[X]$ et on « réduit modulo $X^2+X-1$ » pour obtenir c+dX.**

**On peut aussi dire, qu'on agit comme dans $\mathbb{C}$, en posant $\theta^2=-\theta+1$.**

**Les deux constructions sont possibles et conduisent à des corps « identiques » (on dit isomorphes) :**

**l'élément $\omega$ dans le premier cas participe à créer le corps : $F_9$ est un $F_3$ espace vectoriel de base $(1,\omega)$**

**l'élément $\theta$ dans le second cas participe à créer le corps : $F_9$ est un $F_3$ espace vectoriel de base $(1,\theta)$**

---

## 1.2 Corps construit par adjonction

**Définition 20.** ***Extension d'un corps***

***Lorsqu'un corps K contient un corps k on dit que K est une extension de K***

***C'est le cas pour $F_9$ qui est une extension de $F_3$.***

**Définition 21.** ***Construction d'une extension par adjonction d'un élément à un corps***

***Soit un corps k et un élément $\alpha\notin k$, racine d'un polynôme irréductible P(X)$\in k[X]$, l'ensemble $\{A(\alpha),\ A(X)\in k[X]\}$ est un corps, qui contient k et $\alpha$; on dit qu'il est construit par adjonction de $\alpha$.***

***C'est le cas pour $F_9$ qui est construit par adjonction de $\omega$ , ou de $\theta$, au choix.***

**Définition 22.** ***Polynôme minimal d'un élément sur un corps***

***Soit un corps k et un élément $\alpha\notin k$ qui est racine d'un polynôme (non nul !) de k[X], il existe un polynôme unitaire de plus bas degré parmi les polynômes de k[X] qui s'annulent en $\alpha$; celui est appelé polynôme minimal de $\alpha$ sur k; de par sa construction il est irréductible dans k[X].***

**Définition 23.** ***Element générateur du groupe K****

***Soit K un extension de k, un élément*** $\alpha \in K$ ***est dit générateur du groupe K* lorsque*** $\forall x \in \boldsymbol{K^*}, \exists t \in \mathbb{N}, x = \alpha^t$

**C'est le cas de $\theta$ pour $F_9$, puisque $F_9^* = \{\theta, \theta^2, ...., \theta^8 = 1\}$; $\theta$, à part être racine du polynôme $X^2 + X - 1$ est un générateur du groupe $F_9^*$.**

---

## 2. Les Corps $F_{2^r}$

**$F_2$ n'a que deux éléments 0,1; ce qui est adapté à l'ordinateur mais pauvre en possibilité de transmettre des informations; il nous faut en ensemble plus riche en possiblités, mais construit aussi sur le modèle de $F_2$, c'est à dire avec des 0 et des 1, nous allons appliquer la technique décrite au-dessus pour construire des extensions de $F_2$.**

**Théorème 24.** ***La factorisation des polynômes cyclotomiques dans*** $F_2[X]$

***Soit un entier impair n et r, le plus petit entier strictement positif tel que*** $2^r \equiv 1[n]$ ***alors le polynôme cyclotomique*** $\Phi_n(X)$ ***se factorise dans*** $F_2[X]$ ***en un produit de polynômes irréductibles, tous de degré r.***

**Théorème 25.**

***Pour tout entier strictement positif r, il existe un corps de cardinal*** $2^r$***, noté*** $F_{2^r}$***.***

***Ce corps contient*** $F_2$.

***Il est construit par adjonction à*** $F_2$ ***d'une racine n-ième primitive de l'unité, où*** $n = 2^r - 1$.

***Si on désigne cette racine par*** $\alpha$ ***cela signifie que*** $\alpha^n = 1$ ***et que*** $\forall t \in \{1, ..., n-1\}$***,*** $\alpha^t \neq 1$***, donc*** $\{\alpha, \alpha^2, ..., \alpha^{n-1}\}$ ***sont différents deux à deux; c'est à dire*** $F_{2^r} = \{0, \alpha, \alpha^2, ..., \alpha^{n-1}\}$***, ce qui permet d'avoir une table facile de multiplication dans*** $F_{2^r}$***.***

**Proposition 26.**

*Liste des premiers polynômes cyclotomiques et de leurs facteurs irréductibles dans* $F_2[X]$