Chapitre 1 : Notions d'algèbre.

1.1 Introduction

Les codes cycliques sont étroitement liés à l'algèbre linéaire et à l'arithmétique des polynômes sur un corps fini. On va présenter dans ce chapitre quelques notions et concepts algébriques associées aux codes cycliques et qui seront utilisées tout au long des chapitres qui suivent.

1. Les corps fini : Les codes cycliques sont construits sur des corps finis, les éléments d'un corps fini peuvent être utilisés pour représenter les coefficients des polynômes dans la construction des codes cycliques.
2. Les polynômes : Les codes cycliques sont définis en utilisant des polynômes, qui sont des expressions algébriques de la forme $a_0 + a_1X + a_2X^2 + ... + a_nX^n$, où les a_i sont les coefficients du polynôme et X est l'indéterminé. Les polynômes jouent un rôle central dans la conception des codes cycliques, car ils déterminent les propriétés du code.
3. La division polynomiale : La division polynomiale est une opération essentielle dans la construction des codes cycliques. Pour coder les données, on effectue une division polynomiale du polynôme à coder par le polynôme générateur. Le reste de cette division détermine si le mot appartient ou non au code cyclique correspondant.
4. Les polynômes générateurs et matrices génératrices : Un code cyclique est défini par un polynôme générateur ou une matrice génératrice y associée. Ce polynôme est choisi pour avoir des propriétés particulières, notamment la cyclicité qui rend la détection et la correction d'erreurs plus efficaces. Le polynôme générateur cyclique est utilisé pour générer le code cyclique à partir des données.
5. Les sommes de contrôle cycliques (CRC) : Les codes cycliques sont souvent utilisés pour la détection d'erreurs à l'aide de CRC. Les CRC sont des sommes de contrôle calculées à l'aide de polynômes pour vérifier l'intégrité des données transmises.
6. La matrices de contrôle de parité : Dans certains contextes, les codes cycliques peuvent être représentés sous forme matricielle à l'aide de matrices de contrôle de parité. Ces matrices permettent de détecter et de corriger les erreurs dans les données transmises.

En résumé, pour comprendre pleinement les codes cycliques, il est important d'avoir des connaissances en algèbre linéaire, en arithmétique des polynômes et en théorie des corps finis.

Ces concepts sont fondamentaux pour la conception, l'analyse et l'application des codes cycliques dans les systèmes de communication et de stockage de données.

1.2 Anneaux et anneau des polynômes

1.2.1 Anneaux

Définition 1.1.

Soit A un ensemble muni de deux lois internes (+) ,(.), *alors* $(A, +, .)$ est un **anneau**, si et seulement s'il vérifie les conditions suivantes:

1. $(A, +)$ est un groupe abélien (d'élément neutre 0_A où 0 par la loi (+), dit **élément nul**.
2. La loi (.) associative et distributive sur la loi (+).
3. A admet un élément neutre noté 1_A ou 1 par la loi (.)

- Dans certaines définitions, la condition (3) n'est pas nécessaire. Dans ce cas, on dit que A est un **anneau unitaire**.
- Si la loi (.) est commutative alors A est dit **anneau commutatif**.

Définition 1.2.

Soit A un anneau, un élément $x \in A-\{0\}$ est dit **diviseur de zéro**, s'il existe un élément $y \in A-\{0\}$ tel que $x.y = 0$ ou $y.x = 0$. Un anneau A est dit **anneau intègre**, s'il n'admet pas de diviseurs de zéro.

Exemple 1.1.

Les anneaux $(\mathbb{Z}, +, .)$, $(\mathbb{R}, +, .)$ et $(\mathbb{R}[X], +, .)$ sont des anneaux commutatifs intègres.

$(\mathbb{Z}/6\mathbb{Z}, +, .)$ et $(F(\mathbb{R}, \mathbb{R}) , +, .)$ sont des anneaux non intègres.

Définition 1.3.

1. Un élément $a \in A-\{0\}$ est dit **inversible** (ou **unité**) dans A, s'il existe un élément $b \in A-\{0\}$ tel que $a.b = b.a = 1$.
2. L'ensemble des unités de A est noté $\mathcal{U}(A)$ ou A^*. i.e. $\mathcal{U}(A)= \{a \in A, a \text{ inversible}\}$.

Proposition 1.1.

$(\mathcal{U}(A), .)$ est un groupe multiplicatif, dit **groupe des unités** de A.

On a : $\mathcal{U}(\mathbb{Z})=\{1, -1\}$, $\mathcal{U}(\mathbb{R}[X])=\mathbb{R}-\{0\}$.

Définition 1.4.

1. $(\mathbb{K}, +, .)$ est un **corps** si, et seulement si, $(\mathbb{K}, +, .)$ est un anneau unitaire dans lequel tout élément non nul est inversible. Autrement dit $\mathbb{K}$ est un corps si, et seulement si $\mathcal{U}(K)= \mathbb{K}-\{0\}$.
2. Un corps $\mathbb{K}$ est dit **corps commutatif,** si la loi (.) est commutative.
3. Un corps $\mathbb{K}$ est dit **corps fini**, si son cardinal entant qu'ensemble est fini.

Définition 1.5.

1. Soit $(A, +, .)$ un anneau, $I \subset A$ est dit **idéal** de A si et seulement si, I vérifie :

a. $I \leq (A, +)$.

b. Pour tous $x \in I$, $a \in A$: $xa \in I$ et $ax \in I$.

2. Si A est commutatif, la condition 2. devient : Pour tous $x \in I$, $a \in A$: $ax \in I$.

Exemple 1.2. Soient A est un anneau commutatif et $a \in A$.

1. *{0} et A* sont des idéaux de A, dits **idéaux triviaux**.
2. L'ensemble $I=\{ax / x \in A\}$ est un idéal de A, dit **idéal principal** de générateur a, noté $<a>$ *ou* aA.
3. $I=n\mathbb{Z} = <n>=\{nk / k \in \mathbb{Z}\}$, ensemble des multiples de n dans $\mathbb{Z}$ est un idéal principal de $\mathbb{Z}$.

Définition 1.6.

1. Un idéal I de A est dit **idéal maximal**, si et seulement si, pour tout idéal J de A tel que $I \subset J$ alors $J=I$ ou $J=A$.
2. Un idéal I de A est dit **idéal premier**, si et seulement si, pour tous $x, y \in A$ tel que $xy \in I$ alors $x \in I$ ou $y \in I$.

Définition 1.7.

Un anneau commutatif et intègre A est dit **anneau principal**, si tout idéal de A est un idéal principal.

Exemple 1.3.

1. L'anneau $\mathbb{Z}$ des entiers relatifs est un anneau principal.
2. Soit $\mathbb{K}$ un corps, l'anneau $\mathbb{K}[X]$ des polynômes sur $\mathbb{K}$, est un anneau principal.

1.2.2 Morphisme d'anneaux, anneaux quotients et anneau Euclidiens.

Définition 1.8.

1. Soient $(A, +, .)$, $(A', +, .)$ deux anneaux, d'éléments neutres, respectivement, 1_A et $1_{A'}$ par la loi (.). Une application f de A dans A' est dite **morphisme d'anneaux**, si et seulement si, pour tous $x, y \in A$ on a :
   a. $f(x+y) = f(x) + f(y)$.
   b. $f(x.y) = f(x).f(y)$.
   c. $f(1_A) = 1_{A'}$.
2. Le **noyau** du morphisme d'anneaux f, noté $Kerf$, est définit par :
$$Kerf = \{x \in A, f(x) = 0_A\} \subset A.$$
3. L'**image** du morphisme d'anneaux f, noté Imf, est définit par :
$$Imf = \{ f(x), x \in A\} \subset A'.$$

Proposition 1.2.

Soient A, A' deux anneaux et f un morphisme d'anneaux de A dans A', on a alors :

1. $Kerf$ est un idéal de A.
2. Imf est un sous-anneau de A'.
3. f injective, si et seulement si, $Kerf = \{0_A\}$.
4. f surjective, si et seulement si, $Imf = A'$.

Théorème 1.1. (Premier théorème d'isomorphismes d'anneaux)

Soient A, A' deux anneaux et f un morphisme d'anneaux de A dans A', on a alors :
$$A/Kerf \cong Imf.$$

Définition 1.9.

Soit A un anneau commutatif et considérons l'application :

$$f : \mathbb{Z} \to A$$
$$k \mapsto f(k) = k.1 = \begin{cases} 1+1+\cdots+1 & \text{si} \quad k > 0 \\ 0 & \text{si} \quad k = 0 \\ -1-1-\cdots-1 & \text{si} \quad k < 0 \end{cases}$$

f est un morphisme d'anneaux et donc $Kerf$ est un idéal de $(\mathbb{Z}, +)$, d'où $\exists\, n \in \mathbb{N}$ tel que $Kerf = n\mathbb{Z}$. L'entier est n est appelé la **caractéristique** de A, noté $car(A)$

Remarque 1.1.

1. Si f est injectif (donc n=0), A est dit anneau de **caractéristique nulle**.
2. Si f n'est pas injectif ($n\neq0$), on dit que A est de caractéristique n et on écrit car(A)=n.
3. S'il existe, n est le plus petit entier positif non-nul vérifiant : $n.1_A=0_A$, si non $n=0$.

Proposition 1.3.

Soit (A, +, .) un anneau, I un idéal de A, comme I est un sous-groupe normal dans le groupe (A, +), alors le groupe (A/I, +) est un groupe abélien, tel que la loi (+) est définie par : $\bar{x}+\bar{y}=\overline{x+y}$.

La loi (.) dans A est compatible avec la relation d'équivalence R définie par :

$x\ R\ y$ si, et seulement si, $x-y\in I$. On définit donc dans A/I la loi (.) par : $\bar{x}\ .\ \bar{y}=\overline{x.y}$.

et (A/I, +, .) est un anneau, dit **anneau quotient** de A par I.

Exemple 1.4.

Soit A= ($\mathbb{Z}$, +, .), I=$n\mathbb{Z}$ avec $n\in\mathbb{N}^*$, alors ($\mathbb{Z}/n\mathbb{Z}$, +, .) est l'anneau quotient de $\mathbb{Z}$ par $n\mathbb{Z}$ tel

que : pour tout $x, y\in\mathbb{Z}$: $\bar{x}+\bar{y}=\overline{x+y}\Leftrightarrow(x+n\mathbb{Z})+(y+n\mathbb{Z})=(x+y)+n\mathbb{Z}$.

$\bar{x}\ .\ \bar{y}=\overline{x.y}\ \Leftrightarrow(x+n\mathbb{Z})\ .\ (y+n\mathbb{Z})=(x.y)+n\mathbb{Z}$.

Proposition 1.4.

Soit A un anneau et I un idéal de A, alors :

1. A/I est un corps, si et seulement si, I est un idéal maximal.
2. A/I est un anneau intègre, si et seulement si, I est un idéal premier.

Proposition 1.5.

1. Un élément a de A est dit **premier** si, est seulement si $<a>$ est un idéal premier.
2. $<a>$ est un idéal premier si, et seulement si, $A/<a>$ est un anneau intègre.
3. Un élément a de A est **irréductible** si, et seulement si $<a>$ est un idéal maximal.
4. $<a>$ est un idéal maximal si, et seulement si $A/<a>$ est un corps.

Définition 1.10.

Soit A un anneau commutatif intègre, A est dit **anneau Euclidien,** s'il existe une application $\varphi : A\text{-}\{0\}\rightarrow\mathbb{N}\text{-}\{0\}$ appelée **Stathme** vérifiant :

1. Pour tout $x, y \in A$ tel que $y \neq 0_A$, $\exists!\ q, r \in A \quad x=yq + r$ avec $r=0$ ou $\varphi(r) < \varphi(y)$.
2. Pour tout $x, y \in A-\{0\}$ ($\exists\ z \in A$ tel que $x=yz$) $\Rightarrow \varphi(r) \leq \varphi(y)$.

L'opération de trouver q et r est dite **Division Euclidienne** de x par y, q est dit le **quotient** et r est dit le **reste** de cette division.

Remarque 1.2.

1) Si le reste $r=0$, alors $x=yq$, on dit que y **divise** x ou y est un **diviseur** de x ou encore que x est un **multiple** de y.
2) Deux éléments a et b de A sont dits **associés,** si a divise b et b divise a , c'est-à-dire s'il existe c et d dans A tels que $a=bc$ et $b=ad$. Cela revient encore à dire qu'il existe u élément de A inversible tel que $a=bu$.

Proposition 1.6.

Tout anneau Euclidien est un anneau principal.

Preuve.

Soit I un idéal non nul de A et soit $a \in I$ avec $a \neq 0$ tel que $\varphi(a)$ minimal dans $\varphi(A-\{0\}) \subset \mathbb{N}$).

[Rappelons que tout ensemble non vide de $\mathbb{N}$ possède un élément minimal.] Soit maintenant

$x \in I$. En effectuant la Division Euclidienne de x par a, on peut écrire $x = aq + r$ avec $r = 0$ ou bien $\varphi(r) < \varphi(a)$. Il est clair que $r=x-aq \in I$. Si on suppose $\varphi(r) < \varphi(a)$ alors $\varphi(r)$ sera l'élément minimal dans $\varphi(r)$, ce qui est absurde, et on a donc nécessairement $r = 0$ et d'où $x = aq \in < a >$ et donc $I=< a >$ principal.

Exemple 1.4.

1. $\mathbb{Z}$ est un anneau Euclidien avec le Sthatme φ est définie par: $x \in \mathbb{Z}$: $\varphi(x)=|x|$
2. Si $\mathbb{K}$ $\mathbb{R}[X]$ est un anneau Euclidien avec le Sthatme φ est définie par: $P \in \mathbb{R}[X]$:

   $\varphi(P)=\deg(P)$.

1.2.3 Polynômes et Anneau des polynômes.

Définition 1.11.

Soit A un anneau commutatif. Un **polynôme** sur A est une suite $P=(a_i)_{i \in \mathbb{N}}$ d'éléments de A, qui sont tous nuls sauf un nombre fini, ces éléments sont dits **coefficients** de P.

c.à.d. $\exists\, n \in \mathbb{N}$: $a_n \neq 0$ et pour tout $i > n$: $a_n = 0$. L'entier n est dit le **degré** de P, noté deg(P).

Par convention d°(0) = -∞. Le coefficient a_n est dit le **coefficient dominant**. Si $a_n = 1$, le polynôme P *est* dit **polynôme unitaire** ou **normalisé.**

On note $A[X] = \{ P = (a_i)_{i \in \mathbb{N}} / a_i \in A \}$, l'ensemble des polynômes sur A, où $X = (0, 1, 0, \ldots, 0..)$ est

dite **l'indéterminé**. On muni $A[X]$ par les lois d'addition (+) et multiplication (.) définies par : $(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} = (a_i + b_i)_{i\in\mathbb{N}}$, $(a_i)_{i\in\mathbb{N}} . (b_i)_{i\in\mathbb{N}} = (c_i)_{i\in\mathbb{N}}$, avec $c_i = \sum_{j=0}^{i} a_j\, b_{i-j}$

Remarque 1.2.

On a $X^1 = X$, $X^2 = X.X$, (0, 0,1, …,0, 0, …) et pour tout entier i, $X^i = (0, 0, \ldots, 0, 1, 0, \ldots)$ où 1 se trouve en position $i+1$, et par convention $X^0 = (1, 0, 0, \ldots, 0, \ldots)$, et tout polynôme $P = (a_i)_{i\in\mathbb{N}}$ s'écrit sous la forme $P = \sum_{i\in\mathbb{N}} a_i\, X^i$.

Proposition 1.7.

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

Exemple 1.5.

1. Les polynômes de degré nul sont de la forme $P = a$ / $a \in A$-{0} dit **polynômes constants**.
2. Les polynômes de degré1 sont de la forme $P = aX + b$ / $a \in A$-{0} et $b \in A$.
3. Les polynômes de degré 2 sont de la forme $P = aX^2 + bX + c$ / $a \in A$-{0} *et* $b, c \in A$.

Proposition 1.8.

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

Preuve Laissé comme exercice.

Remarque 1.3.

Soit $A = \mathbb{K}$ un corps commutatif. On dit qu'un polynôme P de $\mathbb{K}[X]$ est **irréductible** s'il est non constant, et si ses seuls diviseurs sont les polynômes constants et les polynômes qui lui sont **associés**, c'est-à-dire les polynômes de la forme λP, avec $\lambda \in \mathbb{K}^*$.

Proposition 1.9.

Si $A=\mathbb{K}$ est un corps commutatif, alors l'anneau $\mathbb{K}[X]$ est un anneau commutatif intègre Euclidien. Son Stathme est l'application :

$$\varphi : \mathbb{K}[X]\text{-}\{0\} \to \mathbb{N}\text{-}\{0\}$$
$$P \to \varphi(P)= d°(P).$$

Conséquence 1.1.

Si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est un anneau principal.

Remarque 1.4.

Si I est un idéal de $\mathbb{K}[X]$, alors il est principal, engendré par tout polynôme non nul de I, de degré minimum. Le polynôme unitaire P engendrant I est dit **le générateur** de I et on a:

$$I=<P> =\{ PQ / Q\in \mathbb{K}[X]\}.$$

Les éléments de I sont les multiples de P.

Exemple 1.6.

Soit $I=\{P\in\mathbb{R}[X]: P(1)=0\}$, alors I est un idéal de $\mathbb{R}[X]$ et on a:

$P\in I \Leftrightarrow P(1)=0\Leftrightarrow(\exists\ Q\in\mathbb{R}[X] : P=(X\text{-}1)Q)\Leftrightarrow P\in <P_1=X\text{-}1>$, donc $I=<X\text{-}1>$ l'idéal engendré par le polynôme $P_1=X\text{-}1$.

1.2.4 Racines d'un polynôme et l'anneau quotient $\mathbb{K}[X]/(P)$

Définition 1.12.

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

Exemple 1.7.

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

Proposition 1.10.

1. Si α est une racine d'ordre k d'un polynôme $P\in\mathbb{K}[X]$, alors α est une racine d'ordre k-1 de son polynôme dérivé P'.
2. Si $P(\alpha)=0$ et $P'(\alpha)\neq 0$, alors α est une racine simple de P.

Proposition 1.12.

Si $\mathbb{K}$ est un corps commutatif et I un idéal de $\mathbb{K}[X]$ de générateur un polynôme P, alors l'anneau quotient $\mathbb{K}[X]/I=<P>$ est un anneau commutatif, d'éléments neutres $\bar{0}=I$ par l'addition et $\bar{1}=1+I$ par la multiplication. L'anneau $\mathbb{K}[X]/<P>$ est dit **anneau quotient** de $\mathbb{K}[X]$ par l'idéal $I=<P>$.

Conséquence 1.2.

Si $P\in\mathbb{K}[X]$ est un polynôme irréductible, alors l'anneau quotient $\mathbb{K}[X]/<P>$ est un corps commutatif.

Exercice 1.1.

Soit $\mathbb{K}$ un corps commutatif, alors $(\mathbb{K}[X], +, ., \times)$ est une $\mathbb{K}$-algèbre, et l'ensemble $\mathbb{K}_{n-1}[X]=\{P\in\mathbb{K}[X]$ tel que $d°(P)\leq n-1\}$ est une $\mathbb{K}$-sous-algèbre de $\mathbb{K}[X]$.

Rappelons que $(\times)$ est la loi externe définie par : $\lambda\in\mathbb{K}$, $P=\sum_{i=0}^{n} a_i X^i\in \mathbb{K}[X]$:

$$\lambda\times P=\sum_{i=0}^{n}(\lambda a_i) X^i.$$

1.3 Construction et existence des corps finis.

1.3.1 Construction des corps finis

Proposition 1.12.

Si p est un entier premier et P un polynôme irréductible sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ de degré n, alors le corps $\mathbb{F}_p[X]/(P)$ est uncorps commutatif fini isomorphe à $(\mathbb{F}_p)_{n-1}[X]$ (l'anneau des polynômes sur $\mathbb{F}_p$ de degré inferieur ou égal à n-1) et de cardinal p^n.

Preuve.

Soit l'application f définie par :

$$f : \mathbb{F}_p[X] \to (\mathbb{F}_p)_{n-1}[X],$$
$$A \longmapsto f(A)=R$$

tel que R est le reste de la division Euclidienne de A par P.

f ainsi définie est un morphisme d'anneaux surjective car:

$Imf=\{f(A) / A\in\mathbb{F}_p[X]\}=\{R / R\in\mathbb{F}_p[X]$ et $d°(R)\leq n-1\}=(\mathbb{F}_p)_{n-1}[X]$.

On a : $A=QP+R$ avec $R=0$ ou $d°(R)\leq n-1$ et le noyau de f est donné par :

$Kerf=\{A\in\mathbb{F}_p[X] / f(A)=0\}=\{A\in\mathbb{F}_p[X] / R=0\}=\{ PQ / Q\in\mathbb{F}_p[X] \}=<P>$, l'idéal engendré par le polynôme P. Selon le premier théorème d'isomorphisme: $\mathbb{F}_p[X]/<P>\cong(\mathbb{F}_p)_{n-1}[X]$ or $(\mathbb{F}_p)_{n-1}[X]$ est un espace vectoriel de dimension n sur $\mathbb{F}_p$, donc $(\mathbb{F}_p)_{n-1}[X]\cong(\mathbb{F}_p)^n$ et d'où $card(\mathbb{F}_p[X]/(P))=card((\mathbb{F}_p)^n)=p^n$.

Proposition 1.13.

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 $\mathbb{F}_p$ dit **sous-corps premier** de $\mathbb{K}$ et le cardinal de $\mathbb{K}$ est de la forme p^n avec $n \in \mathbb{N}$.

Preuve.

Comme $\mathbb{K}$ est un corps, alors $\mathbb{K}$ est un anneau intègre, donc car($\mathbb{K}$)=0 ou car(A)=p premier. Si on suppose car($\mathbb{K}$)=0, alors $\mathbb{K}$ est infini, ce qui est absurde car $\mathbb{K}$ est fini.

L'application $f:\mathbb{Z} \longrightarrow \mathbb{K}, k \mapsto f(k) = k.1_{\mathbb{K}}$, est un morphisme d'anneaux de noyau $Kerf=p\mathbb{Z}$ et $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z} \cong f(\mathbb{Z})$ or $f(\mathbb{Z})$ est un sous-corps de $\mathbb{K}$, donc $\mathbb{K}$ est considéré comme un espace vectoriel sur $\mathbb{F}_p$ de dimension fini car $\mathbb{K}$ est un corps fini . Si $\dim_{\mathbb{F}_p}\mathbb{K} = n$ alors $\mathbb{K} \cong \mathbb{F}_p^n$ et donc card($\mathbb{K}$)=p^n.

Proposition 1.14.

Soit p est la caractéristique d'un corps commutatif fini $\mathbb{K}$ alors :

1. p est le plus petit entier non nul vérifiant $p.1_{\mathbb{K}} = 0$.
2. Pour tout $x \in \mathbb{K}$: $p.x = 0$,
3. Pour tout $x, y \in \mathbb{K}$: $(x+y)^p = x^p + y^p$ et $(x.y)^p = x^p.y^p$.
4. Pour tout $i \in \mathbb{N}, x, y \in \mathbb{K}$: $(x+y)^{p^i} = x^{p^i} + y^{p^i}$ et $(x.y)^{p^i} = x^{p^i}.y^{p^i}$.

Proposition 1.15.

Si $\mathbb{K}$ est un corps commutatif fini de caractéristique p et de cardinal p^n alors :

1. ($\mathbb{K}^* = \mathbb{K}$-{0}, .) est un groupe cyclique d'ordre p^n-1
2. Pour tout $x \in \mathbb{K}$: $x^{p^n} = x$.

Preuve.

$\mathbb{K}^* = \mathcal{U}(\mathbb{K})$ est un groupe cyclique multiplicatif de cardinal p^n-1. Donc pour tout $x \in \mathbb{K}^*$: $x^{p^n-1} = 1$, en multipliant par x, on trouve que pour tout $x \in \mathbb{K}^*$: $x^{p^n} = x$ et comme cette égalité est vrai pour $x = 0$, alors pour tout $x \in \mathbb{K}$: $x^{p^n} = x$.

Définition 1.13.

Soit $\mathbb{K}$ un corps fini de caractéristique un entier premier p et $\beta \in \mathbb{K}$. Le **polynôme minimale** de β noté M_β est le polynôme générateur de l'idéal (principal) I_β définie par:

$$I_\beta = \{P \in \mathbb{F}_p[X] : P(\beta)=0\}.$$

Proposition 1.16.

Le polynôme minimale M_β vérifie les propriétés suivantes :

1. M_β est un polynôme unitaire de $\mathbb{F}_p[X]$ 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 $\mathbb{F}_p$.

Preuve.

1) et 2) découlent de la définition de M_β.

Pour 3) soit $P, Q \in \mathbb{F}_p[X]$: $PQ \in I \Leftrightarrow (PQ)(\beta)=0 \Rightarrow P(\beta)Q(\beta)=0$ et comme $\mathbb{F}_p[X]$ 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 M_β est premier (irréductible) sur $\mathbb{F}_p$.

Proposition 1.17.

Si $\mathbb{K}$ est un corps commutatif fini, alors $(\mathbb{K}^*, .)$ est un groupe cyclique, et tout générateur α de $\mathbb{K}^*$ est dit **racine primitive** (ou **élément primitif**) de $\mathbb{K}$ et $\mathbb{K}=\{0, \alpha^i / 0 \leq i \leq p^n-2\}$.

Le polynôme minimal associé à cette racine α est dit **polynôme primitif** de $\mathbb{K}$, qu'on note M_α qui a les mêmes propriétés de la Proposition 1.16.

Proposition 1.18.

Soit $\mathbb{K}$ un corps commutatif fini et $\beta \in \mathbb{K}$, alors l'application

$$f : \mathbb{F}_p[X] \to \mathbb{K},$$
$$P \mapsto f(P)=P(\beta),$$

est un morphisme d'anneaux de noyau I_β et le corps $\mathbb{F}_p[X]/I_\beta$ est isomorphe à $Im(f)$.

Preuve.

$Kerf=\{P \in \mathbb{F}_p[X] / P(\beta)=0\}=I_\beta=(M_\beta)$ et donc d'après le premier théorème d'isomorphisme on a : $\mathbb{F}_p[X]/Kerf \cong Im(f)$. On a $Kerf = I_\beta$ et $Im(f)=\{P(\beta)/P \in \mathbb{F}p[X]\}$ qu'on note $\mathbb{F}_p[\beta]$**.** Donc le corps quotient $\mathbb{F}_p[X]/< M_\beta >$ est isomorphe à $\mathbb{F}_p[\beta]$ **(**l'ensemble des expressions polynômiales d'indéterminé β sur $\mathbb{F}_p$) dit **extension** de $\mathbb{F}_p$ par β.

Remarque 1.5. (Exercice)

$\mathbb{F}_p[\beta]$ est le plus petit sous-corps de $\mathbb{K}$ contenant β et $\mathbb{F}_p$.

Proposition 1.19.

Si $d°(M_\beta)=n$ alors $\mathbb{F}_p[\beta]$ est un espace vectoriel sur $\mathbb{F}_p$ de dimension n et admet la famille $B=\{1, \beta, \beta^2, ..., \beta^{n-1}\}$ comme base.

Théorème 1.2. (Waderburn)

Tout corps fini $\mathbb{K}$ est commutatif.

Le théorème ci-dessous nous permet de construire un corps fini $\mathbb{K}$ dont sa caractéristique et son polynôme primitif sont connus.

Théorème 1.3.

Tout corps fini $\mathbb{K}$ de caractéristique un entier premier p et de racine primitive α, est isomorphe au corps quotient $\mathbb{F}_p[X]/< M_\alpha >$ tel que M_α est son polynôme primitif.

Preuve.

D'après la Proposition 1.19 en prenant $\beta=\alpha$ alors on trouve que $\mathbb{F}_p[X]/ I_\alpha = < M_\alpha>$ est isomorphe à $\mathbb{F}_p[\alpha]$ (ensembles des expressions polynomiales en α à coefficients dans $\mathbb{F}_p$). Montrons que $\mathbb{K}= \mathbb{F}_p[\alpha]$.

Il est clair que $\mathbb{F}_p[\alpha] \subset \mathbb{K}$. Soit $x\in\mathbb{K}$, si $x=0$ alors $x\in Imf=\mathbb{F}_p[\alpha]$. Soit $x\neq 0$ et $x \in \mathbb{K}^*=<\alpha>$, alors il existe $m\in\mathbb{N}^*$: $x=\alpha^m$ ce qui montre que x est un élément de $\mathbb{F}_p[\alpha]$, d'où $\mathbb{K} \subset \mathbb{F}_p[\alpha]$.

Enfin comme M_α est irréductible alors $\mathbb{F}_p[X]/<M_\alpha>$ est un corps isomorphe au corps $\mathbb{K}$.

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

Remarque 1.6.

Si L est un corps commutatif quelconque et $\mathbb{K}$ un sous-corps de L, en remplaçant $\mathbb{K}$ par L et $\mathbb{F}_p$ 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 1.4.

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 $f : \mathbb{K} \to \mathbb{K}[X]/<P>$, $x \mapsto f(x) = \bar{x}$, f est un morphisme de corps injectif, donc $\mathbb{K}$ est isomorphe à $f(\mathbb{K})$ qui est un sous-corps de $L= \mathbb{K}[X]/(P)$, d'où L est une extension de $\mathbb{K}$. *Si* $P=\sum_{i=0}^{i=n} a_i X^i$, alors $P(\alpha)=\sum_{i=0}^{i=n} a_i\alpha^i = \sum_{i=0}^{i=n} a_i\bar{X}^i = \overline{\sum_{\iota=0}^{\iota=n} a_\iota X^\iota} = \bar{P} = \bar{0}$, alors P vérifie la propriété 2. de la Proposition 1.17, donc $P= M_\alpha$.

Définition 1.14.

Une extension (ou sur-corps) L d'un corps commutatif $\mathbb{K}$ est dite **corps de rupture** d'un polynôme $P \in \mathbb{K}[X]$, si et seulement si, $\exists \alpha \in \mathbb{K}$, $a \in L$, tel que $P=\alpha(X-a)Q$, avec $Q \in \mathbb{K}[X]$.

Définition 1.15.

Une extension (ou sur-corps) L d'un corps commutatif $\mathbb{K}$ est dite **corps de décomposition** d'un polynôme $P \in \mathbb{K}[X]$, si et seulement si, $\exists \alpha \in \mathbb{K}$, $a_1, a_2, \ldots, a_n \in L$ tel que $P=\alpha \prod_{i=1}^{i=n}(X-a_i)$.

Proposition 1.20.

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

Théorème 1.5.

Si $n \in \mathbb{N}^*$ et p entier premier alors il existe un corps fini $\mathbb{K}$ de cardinal p^n et un polynôme irréductible P sur $\mathbb{F}_p$ de degré n.

Preuve.

Soit $P=X^{p^n}-X$ le polynôme de degré p^n sur $\mathbb{K}$ et soit $\mathbb{K}_1$ le corps de décomposition du polynôme $P_1=X^{p^n-1}-1$. Le polynôme dérivé de P_1 est $P_1'=-X^{p^n-2}$, qui n'admet que la racine nulle, qui n'est pas racine de P et donc toutes les p^n-1 racines de P_1 sont distinctes et différentes de 0, alors P admet p^n racines distinctes. Soit $\mathbb{K}$ l'ensemble des racines de P dans $\mathbb{K}_1$. Montrons que $\mathbb{K}=\{x \in \mathbb{K}_1 : x^{p^n}-x=0\}$ est un sous-corps de cardinal p^n du corps $\mathbb{K}_1$. Il suffit de montrer qu'il est stable par les deux lois (+) et (.).

En effet : si $x, y \in \mathbb{K}$ alors on a : $(x+y)^{p^n}=x^{p^n}+y^{p^n}=x+y$, donc $x+y \in \mathbb{K}$ et $(x.y)^{p^n}=x^{p^n}.y^{p^n}=x.y$, donc $x.y \in \mathbb{K}$, donc $\mathbb{K}$ est un corps de cardinal p^n et son polynôme primitif M_α est un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Proposition 1.21.

Tous les corps finis de caractéristique un entier premier p et de cardinal p^r , $r \in \mathbb{N}^*$, sont isomorphes. Cet unique corps fini à isomorphisme prés est dit **corps de Galois** noté $\mathbb{F}_q=\mathbb{F}_{p^r}$.

Remarque 1.6.

Pour décrire le corps de Galois $\mathbb{K}$ de caractéristique p sur le corps premier $\mathbb{F}_p$, il suffit de :

1- Soit connaitre un polynôme primitif de degré r sur $\mathbb{F}_p$ (i.e. le polynôme minimal M_α d'une racine primitive α de $\mathbb{K}$), et $\mathbb{F}_q=\mathbb{F}_p(\alpha)$ ou $\mathbb{F}_q \approx \mathbb{F}_p[X]/<M_\alpha>$.

2- Soit choisir un polynôme P de $\mathbb{F}_p[X]$, de degré r, irréductible sur $\mathbb{F}_p$ et $\mathbb{F}_q \approx \mathbb{F}_p[X]/<P>$

Exemple 1.7.

Construction d'un corps de Galois $\mathbb{K}=\mathbb{F}_9$, $q=9=3^2$ donc $p=car(\mathbb{K})=3$, $r=d°(M_\alpha)=2$,

$\mathbb{F}_9 = \{0\} \cup \mathbb{F}_9^* = \{0, \alpha^i, 0 \le i \le 7\} = \{0, 1, \alpha, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$. Soit M_α le polynôme primitif de $\mathbb{F}_9$ (le polynôme minimal associe à α), M_α est de degré n=2, irréductible et unitaire sur $\mathbb{F}_3$. On peut prendre le polynôme primitif $M_\alpha = X^2+X+2$ ou $M_\alpha = X^2+2X+2$.

1ere méthode. Prenons $M_\alpha = X^2+X+2$. On a $M_\alpha(\alpha)=0 \Leftrightarrow \alpha^2+\alpha+2=0 \Leftrightarrow \alpha^2=-\alpha-2=2\alpha+1$, $\alpha^3=2\alpha+2$, $\alpha^4=2$, $\alpha^5=2\alpha$, $\alpha^6=\alpha+2$, $\alpha^7=\alpha+1$, donc $\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$.

2eme méthode. Ou encore, considérons le polynôme $P = X^2+1$qui est irréductible de degré 2 sur $\mathbb{F}_3$.

Alors le corps $\mathbb{F}_9$ est isomorphe au corps quotient $\mathbb{F}_3[X]/<P> = \mathbb{F}_3[X]/<X^2+1>$

Donc $\mathbb{F}_9 = \{a\bar{X} + b / a, b \in \mathbb{F}_3\}$. Posons $\bar{X} = \beta$, alors $\mathbb{F}_9 = \{0, 1, 2, \beta, 2\beta, \beta+1, \beta+2, 2\beta+1, 2\beta+2\}$.

Exemple 1.8.

Construction d'un corps de Galois de cardinal $q = 8 = 2^3$ donc p=car(𝕂)=2,

$\mathbb{F}_8 = \{0\} \cup \mathbb{F}_8^* = \{0, \alpha^i, 0 \le i \le 6\} = \{0, 1, \alpha, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Soit M_α le polynôme primitif de $\mathbb{F}_8$ (le polynôme minimal associe à α), M_α est de degré r=3, irréductible et unitaire sur $\mathbb{F}_2$. On peut prendre le polynôme primitif $M_\alpha = X^3+X+1$ ou $M_\alpha = X^3+X^2+1$.

Prenons $M_\alpha = X^3+X+1$. On a $M_\alpha(\alpha)=0 \Leftrightarrow \alpha^3+\alpha+1=0 \Leftrightarrow \alpha^3=\alpha+1$, $\alpha^4=\alpha^2+\alpha$, $\alpha^5=\alpha^3+\alpha^2=\alpha^{2+}$ $\alpha+1$, $\alpha^6=\alpha^3+\alpha^2+\alpha$, $\alpha^7=1$, donc $\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1\ \alpha^2+\alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$.

Exemple 1.9.

(Exercice) Décrire le corps de Galois de cardinal q=16 ($\mathbb{F}_{16}$).

1.4 Groupe et corps des racines nièmes de l'unité et la décomposition du polynôme X^n -1

Dans ce paragraphe, on va définir et voir comment construire le plus petit corps qui contient tous les racines du polynôme X^n-1, pour n un entier non nul donné et qui nous permet de décomposer ce polynôme en produit de polynômes irréductibles sur $\mathbb{F}_p$.

1.4.1 Groupe des racines nièmes de l'unité

Définition 1.16.

Soit n un entier non nul et 𝕂 un corps commutatif, on appel **racine nième de l'unité** sur 𝕂, tout élément α de 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 𝕂 c.à.d.

$$G_n(\mathbb{K}) = \{x \in \mathbb{K} - \{0\} : x^n - 1 = 0\}$$

Exemple 1.9.

1- Les racines troisième de l'unité sur ℂ sont $\alpha_1 = 1$, $\alpha_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\alpha_3 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$ et sur ℝ ou ℚ la

seule racine troisième de l'unité est la racine triviale α=1.

2- Les racines quatrièmes de l'unité sur $\mathbb{R}$ sont α_1=1, α_2= -1.

Rappelons le théorème suivant concernant les groupes cycliques :

Théorème 1.6.

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 = PGCD(n, k).

Théorème 1.7. Groupe des racines nième de l'unité

Soit $\mathbb{K} = \mathbb{F}_q$ 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=PGCD(p^r-1, n) dit **groupe des racines nièmes de l'unité** sur $\mathbb{F}_p$ et on a $G_n(\mathbb{K})=G_d(\mathbb{K})$.

Preuve.

Il suffit d'appliquer le théorème ci-dessus pour $G= \mathbb{K}^*= \mathbb{F}_q -\{0\}$ et $H=G_n(\mathbb{K})$

1.4.2 Corps des racines nièmes de l'unité sur $\mathbb{F}_p$

Soit *p* un entier premier et $n\in\mathbb{N}^*$ et cherchons un corps de décomposition $\mathbb{K}$ de X^n-1 sur $\mathbb{F}_p$

c-à-d. un sur-corps $\mathbb{K}$ du corps premier $\mathbb{F}_p$ tel que X^n-1 se décompose en produit de polynômes de premiers degré (pas nécessairement tous différents) c.à.d. $X^n-1=\prod_{i=1}^{i=n}(X-a_i)$.

Remarque 1.7.

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 $m=0$ et $N=n$.
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 ladécomposition de X^n-1 avec *n* n'est pas premier avec *p*, se déduit de celle de X^N-1 avec *N* premier avec *p*, en effet :

$X^n-1=0\Leftrightarrow X^{Np^m}-1=0\Leftrightarrow (X^n-1)^{p^m}=0\Leftrightarrow X^n-1=0$, et d'où $G_n(\mathbb{K})= G_N(\mathbb{K})$.

Théorème 1.8. (Construction du corps des racines nièmes de l'unité)

Soit *p* un entier premier et $n\neq\mathbb{N}$, il existe un unique (le plus petit) corps de décomposition de X^n-1 sur $\mathbb{F}_p$, c'est le corps $\mathbb{K}=\mathbb{F}_{p^r}$ 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 $\mathbb{F}_p$. Et on a :

$X^n-1=\prod_{i=1}^{i=n}\left(X-\beta^i\right)^{p^m}$, tel que $\beta=\alpha^s$, avec $s=\frac{p^r-1}{N}$ et α 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 $\mathbb{Z}/n\mathbb{Z}$. 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 $p^r \equiv 1[n]$ donc $p^r - 1 \equiv 0[n]$. En résumé r est le plus petit entier non nul tel que n divise $p^r - 1$. Considérons le corps $\mathbb{K}=\mathbb{F}_{p^r}$ où r est l'entier définie ci-dessus. Selon le Théorème 1.7. ci-dessus le groupe cyclique $G_n(\mathbb{K})$ est d'ordre $d = \text{PGCD}(p^r-1, n)=n$ (car on a : n divise p^r-1).

Si $\beta \in \mathbb{K}^*$ 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 $X^n - 1$ qui se décompose donc par :

$X^n - 1 = \prod_{i=1}^{i=n}(X - \beta^i)$ et donc $\mathbb{K}=\mathbb{F}_{p^r}$ est un corps de décomposition de $X^n - 1$ sur $\mathbb{F}_p$.

2. Si n n'est pas premier avec p. Soient $n=Np^m$ et $m \in 0$ tel que $N \wedge p=1$ et r le plus petit entier non nul tel que N divise p^r-1, alors le corps $\mathbb{K}=\mathbb{F}_{p^r}$ est le corps de décomposition de X^N-1 et donc celui de $X^n - 1$ qui se décompose par :

$$X^N - 1 = \prod_{i=0}^{i=N-1}(X - \beta^i) \Rightarrow X^n - 1 = (X^N - 1)^{p^m} = \prod_{i=0}^{i=N-1}(X - \beta^i)^{p^m}.$$

Si α est une racine primitive de $\mathbb{K}$ (c.à.d. générateur de $\mathbb{K}^*$) alors d'après les propriétés des groupes cycliques, on peut prendre β (générateur de $G(\mathbb{K})$) de la forme $\beta=\alpha^s$ tel que $s = \dfrac{p^r - 1}{n}$.

Exercice 1.2.

Le corps $\mathbb{K}=\mathbb{F}_{p^r}$ est le plus petit corps de décomposition de $X - 1$ sur $\mathbb{F}_p$.

En effet.

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

Exemple 1.10.

Déterminer $\mathbb{K}$ le corps des racines 15-imes de l'unité sur $\mathbb{F}_2$ et décomposer $X^{30}-1$ sur $\mathbb{F}_2$.

N=15 et p=2. Le corps concerné est $\mathbb{K}=\mathbb{F}_{2^r}$, tel que r est le plus petit entier non nul tel que N=15 divise 2^r -1, on trouve r= 4 et donc $\mathbb{K}=\mathbb{F}_{16}$.

$X^{15}-1=\prod_{i=0}^{i=14}(X-\beta^i)$ et $X^{30}-1=(X^{15}-1)^2=\prod_{i=0}^{i=14}(X-\beta^i)^2$,

$\beta=\alpha$ est la racine primitive 15$^{\text{ieme}}$ de l'unité qui est une racine primitive de $\mathbb{K}$.

1.4.3 Décomposition de X^n-1 en produit de polynômes irréductibles sur $\mathbb{F}_p$.

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

Définition 1.17.

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 noté $P_n(\mathbb{K})$ est donnée par:

$$P_n(\mathbb{K})=\{\beta\in G_n(\mathbb{K}) / \beta \text{ engendre } G_n(\mathbb{K})\}.$$

Définition 1.18.

Soit $\mathbb{K}=\mathbb{F}_{p^r}$ corps des racines nièmes de l'unité sur $\mathbb{F}_p$.

On appelle **Polynôme cyclotomique** d'indice n, le polynôme noté $\emptyset_n(X)\in\mathbb{F}_p[X]$ dont ses racines sont les racines nièmes primitives de l'unité dans K. i.e.

$$\emptyset_n(X)=\prod_{\varepsilon\in P_n(\mathbb{K})}(X-\varepsilon).$$

Définition 1.19.

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 1.11.

Pour n=6, $\varphi(6)=\text{card}\{1,5\}=2$.

Rappelons le théorème suivant concernant les générateurs d'un groupe cyclique :

Théorème 1.9.

Si G est un groupe cyclique d'ordre n engendré par g, alors :

$$(g^k \text{ engendre } G)\Leftrightarrow 1\le k\le n-1 \text{ et } k\wedge n=1.$$

L'ensemble des générateurs de G est :

$$P=\{g^k, 1\le k\le n-1 \text{ et } k\wedge n=1\} \text{ et } \text{card}(P)=\varphi(n)$$

Proposition 1.22.

Soient $n\in\mathbb{N}$ et $\mathbb{K}=\mathbb{F}_{p^r}$ corps des racines nièmes de l'unité sur $\mathbb{F}_p$.

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 :

$$P_n(\mathbb{K}) = \{\beta^j / 1 \leq j \leq n-1 \text{ et } j \wedge n = 1\} \text{ et } \text{card}(P_n(\mathbb{K})) = \varphi(n).$$

Preuve.

Il suffit d'appliquer le théorème précèdent avec $G = \mathbb{K}^*$ et $g = \beta$.

Proposition 1.23.

Soient $n \in \mathbb{N}$ et $\mathbb{K} = \mathbb{F}_{p^r}$ le corps des racines *nièmes* de l'unité sur $\mathbb{F}_p$ Si β est une racine primitive nième de l'unité alors, le polynôme cyclotomique $\emptyset_n(X)$ s'écrit :

$$\emptyset_n(X) = \prod_{\substack{1 \leq j \leq n \\ j \wedge n = 1}} (X - \beta^j) \text{ et } d^\circ(\emptyset_n(X)) = \varphi(n).$$

Preuve.

$\emptyset_n(X) = \prod_{\varepsilon \in P_n(\mathbb{K})}(X - \varepsilon)$ et ε est de la forme $\varepsilon = \beta^j$ tel que $1 \leq j \leq n-1$ et $j \wedge n = 1$.

Donc $\emptyset_n(X) = \prod_{\substack{1 \leq j \leq n \\ j \wedge n = 1}} (X - \beta^j)$ et pour le degré on a :

$$d^\circ(\emptyset(X)) = d^\circ\left(\prod_{\substack{1 \leq j \leq n \\ j \wedge n = 1}} (X - \beta^j)\right) = \sum_{\substack{1 \leq j \leq n \\ j \wedge n = 1}} d^\circ(X - \beta^j) = \sum_{\substack{1 \leq j \leq n \\ j \wedge n = 1}} 1 = card(P_n(\mathbb{K})) = \varphi(n).$$

Proposition 1.24.

Soient $n \in \mathbb{N}^*$ et p premier tel que n premier avec p et $\mathbb{K} = \mathbb{F}_{p^r}$ corps des racines nièmes de l'unité sur $\mathbb{F}_p$. Alors le polynôme X^n-1 se décompose par :

$$X^n - 1 = \prod_{d/n} \emptyset_d(X).$$

Preuve.

Comme $n \wedge p = 1$(donc $n = N$), alors si β est une racine primitive nième de l'unité, le groupe $G_n(\mathbb{K}) = \{1, \beta, \ldots, \beta^{n-1}\}$ est de cardinal n. Si d divise n, on note $P_d(\mathbb{K})$: 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 donc :

$X^n - 1 = \prod_{j \in [0, n-1]} (X - \beta^j) = \prod_{\varepsilon \in} G_n(\mathbb{K}) (X - \varepsilon) = \prod_{d/n} \prod_{\varepsilon \in P_d(\mathbb{K})} (X - \varepsilon)$,

or $\prod_{\varepsilon \in P_d(\mathbb{K})} (X - \varepsilon)$ n'est que le polynôme cyclotomique $\emptyset_d(X)$ d'où $X^n - 1 = \prod_{d/n} \emptyset_d(X)$.

Conséquence 1.3.

Si n n'est pas premier avec p, alors $n = N.p^m$ avec $N \wedge p = 1$ et on a :

$$X^n - 1 = \prod_{d/n} (\emptyset_d(X))^{p^m}.$$

Preuve.

Il suffit 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 1.25.

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 $\mathbb{F}_p$.

Preuve.

On démontre par récurrence sur n. Si n=1, $\emptyset_1(X)$=X-1 donc unitaire et $\emptyset_1(x) \in \mathbb{F}_p[X]$. On suppose que pour tout m < n : $\emptyset_m(X)$ unitaire et $\emptyset_m(X) \in \mathbb{F}_p[X]$. On a :

$$X^n - 1 = \prod_{d/n} \emptyset_d(X) . = \prod_{\substack{d/n \\ d \neq n}} \emptyset_d(X) . \emptyset_n(X),$$

donc

$$X^n - 1 = P(x).\emptyset_n(X) \text{ avec } P(x) = \prod_{d/n, d \neq n} \emptyset_d(X).$$

On a : pour tout d/n : d < n, d'après le processus de récurrence , $\emptyset_d(X)$ est unitaire et $\emptyset_d(X) \in \mathbb{F}_p[X]$, donc $P(X)$ est unitaire et $P(X) \in \mathbb{F}_p[X]$ et comme X^n-1$\in \mathbb{F}_p[X]$ est unitaire alors de l'égalité $X^n - 1 = P(X).\emptyset_n(X)$, on déduit que $\emptyset_n(X) \in \mathbb{F}_p[X]$ et $\emptyset_n(X)$ unitaire.

1.4.4 Calcul direct des polynômes cyclotomiques.

Proposition 1.26.

Si p est un entier premier alors :

$$\emptyset_p(X) = X^{p-1} + \ldots + X + 1.$$

Preuve. Comme p premier, les diviseurs de p sont 1 et p, donc on a

$X^p - 1 = \emptyset_1(X)\emptyset_p(X) = (X - 1)\, \emptyset_p(X)$ donc $\emptyset_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$.

Exemple 1.12.

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

Conséquence 1.4.

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.

$X^{p^k} - 1 = \prod_{d/p^k} \emptyset_d(X) = \emptyset_{p^k}(X) \prod_{d/p^{k-1}} \emptyset_d(X) \Rightarrow X^{p^k} - 1 = \emptyset_{p^k}(X)\, (X^{p^{k-1}} - 1)$

Ce qui donne : $\emptyset_{p^k}(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1}$.

Remarque 1.8.

$$\emptyset_{p^k}(X) = \frac{X^{p^k}-1}{X^{p^{k-1}}-1} = \frac{(X^{p^{k-1}})^{\mathrm{p}}-1}{X^{p^{k-1}}-1} = \emptyset_p\left(X^{p^{k-1}}\right).$$

Exemples 1.13.

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

Théorème 1.10.

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

1. Si *p* divise *n* alors : $\emptyset_{np}(X)= \emptyset_n(X^{\mathrm{p}})$.
2. Si *p* ne divise pas *n* alors : $\emptyset_{np^k}(X)= \frac{\emptyset_n\left(X^{p^k}\right)}{\emptyset_n\left(X^{p^{k-1}}\right)}$ et en particulier $\emptyset_{np}(X)=\frac{\emptyset_n(X^{\mathrm{p}})}{\emptyset_n(X)}$.

Théorème 1.11.

Soient *p* premier, $n\in\mathbb{N}^*$ et $\mathbb{K}=\mathbb{F}_{p^r}$, le corps des racines *nièmes* de l'unité sur $\mathbb{F}_p$. Alors $\emptyset_n(X)$ se décompose en produit de $\varphi(n)/r$ polynômes irréductibles de degré r et à coefficients dans $\mathbb{F}_p$.

Preuve.

Soit $\mathbb{K}=\mathbb{F}_{p^r}$, le corps des racines *nièmes* de l'unité sur $\mathbb{F}_p$. Soit β une racine *n*ieme 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 pour tout $i\in \mathrm{I}_n$: $p^r i = i$ dans $\mathbb{Z}/n\mathbb{Z}$ et comme *i* est premier avec *n* alors, les ensembles $J_i =\{ i, pi, \dots , p^{r-1} i\}$ où $i\wedge n=1$ dits **classes cyclotomiques**, sont de cardinal *r* et forment une partition à I_n c.à.d $I_n = \bigcup_{t=1}^{t=k} J_t$.

$\emptyset_n(X) = \prod_{\varepsilon\in P_n(\mathbb{K})}(X-\varepsilon) = \prod_{\substack{1\le j\le n\\ j\wedge \mathrm{n}=1}}\left(X-\beta^j\right) = \prod_{\mathrm{j}\in I_n}\left(X-\beta^j\right) = \prod_{\mathrm{j}\in \bigcup_{t=1}^{t=k} J_t}\left(X-\beta^j\right)$

avec card(J_t) = *r* alors: $\emptyset_n(X) = \prod_{\mathrm{j}\in J_1}\left(X-\beta^j\right)\prod_{\mathrm{j}\in J_2}\left(X-\beta^j\right)\dots\prod_{\mathrm{j}\in J_k}\left(X-\beta^j\right)$.

Si j_i est le représentant de la classe J_i , alors pour tout $i\in[1,k]$:

$\prod_{\mathrm{j}\in J_i}\left(X-\beta^j\right) = \prod_{0\le l\le r-1}\left(X-\beta^{j_i p^l}\right)$.

Lemme 1.1.

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 $\beta, \beta^p, \dots, \beta^{p^{r-1}}$ (dits **conjugués** de β) sont distincts.
2. M_β s'écrit : $M_\beta=\prod_{0\le l\le r-1}\left(X-\beta^{p^l}\right)$ et pour tout $l\in[1,r\text{-}1]$: $M_\beta = M_{\beta^{p^l}}$. D'après le lemme ci-dessus : $\emptyset_n(X)= M_{\beta^{j_1}}M_{\beta^{j_2}}\dots M_{\beta^{j_k}}$, qui est le produit de $k= \varphi(n)/r$ polynômes irréductibles, car on a: $\mathrm{d}^\circ(\emptyset_n(X)) = k\mathrm{d}^\circ(M_{\beta^{j_1}}) \Rightarrow \varphi(n)= k.r \Rightarrow k= \varphi(n)/r$.

Exemple 1.14.

Soit n=15 et p=2, le corps des racines 15-èmes de l'unité est $\mathbb{K}=\mathbb{F}_{p^r}$ 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 $\varphi(15)/r = 8/4 = 2$ polynômes irréductibles de degré r=4 c.à.d. $\emptyset_{15}(X) = (X^4 + aX^3 + bX^2 + cX + 1)(X^4 + a'X^3 + b'X^2 + c'X + 1)$. D'autre part $\emptyset_{15}(X) = \emptyset_{3.5}(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1$. Après développement et identification, on trouve : $a = b = b' = c' = 0$ et $c = a' = 1$ et donc $\emptyset_{15}(X) = (X^4 + X + 1)(X^4 + X^3 + 1)$.

Conséquence 1.5.

Soient p premier, $n \in \mathbb{N}^*$ tel que $n \wedge p = 1$ et soit $\mathbb{K}=\mathbb{F}_{p^r}$ le corps des racines nièmes de l'unité. 7

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 1.15.

Soient p=3 et n=5. Le corps de décomposition de X^5 -1 sur $\mathbb{F}_3$ est $\mathbb{K}=\mathbb{F}_{3^r}$ où r est le plus petit entier non nul tel que n=5 divise 3^r -1, on trouve que r=4, et on a $\varphi(5) = 4 = r$, donc $\emptyset_5(X) = X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{F}_3$.

Exemple 1.16.

La décomposition de X^9 -1 sur $\mathbb{F}_2$, 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^{iemes} de l'unité est $\mathbb{K}=\mathbb{F}_{2^6}$ et $\varphi(9)=6=r$, donc $\emptyset_9(X)$ est irréductible.

Le théorème ci-dessous nous permet de Décomposer le polynôme $X^n - 1$ en produit de polynômes irréductibles sur $\mathbb{F}_p$.

Théorème 1.12.

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 $\mathbb{F}_p$.

Preuve.

Il suffit d'appliquer la proposition 1.25 et sa Conséquence 1.3 et le Théorème 1.11 et sa Conséquence 1.5.

Remarque 1.9.

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

Exemple 1.17.

Décomposer le polynôme $X^5 - 1$ en polynômes irréductibles sur $\mathbb{F}_2$.

Soit $\mathbb{K}=\mathbb{F}_{2^r}$, le corps des racines *nièmes* de l'unité sur $\mathbb{F}_2$. 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 $\mathbb{K}=\mathbb{F}_{16}$.

$X^5 - 1 = \prod_{d/5} \emptyset_d(X) = \emptyset_1(X).\ \emptyset_5(X) = (X\text{-}1)\ \emptyset_5(X)$. Décomposons $\emptyset_5(X)$ en produit de polynômes irréductibles sur $\mathbb{F}_2$. On a $\varphi(5)=4=r$ et donc $\emptyset_5(X) = X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$. Donc $X^5 - 1 = (X\text{-}1)(X^4 + X^3 + X^2 + X + 1)$.

Exercice 1.3.

Décomposer les polynômes X^{15} -1 , X^9 -1, X^{18} -1 sur $\mathbb{F}_2$ et $\mathbb{F}_3$ et $\mathbb{F}_5$.

1.5 Matrice de permutation et ses propriétés.

1.5.1 Matrice de permutation

Définition 1.20.

Une **matrice de permutation** d'ordre n est une matrice carré P d'ordre n dont les colonnes (ou les lignes) sont une permutation des colonnes (ou des lignes) de la matrice identité

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Si $P = (p_{ij})_{1\le i,\, j\le n}$; $\exists\ \sigma \in S_n$ (S_n le groupe symétrique d'indice n) tel que :

$$p_{ij} = \delta_{i,\sigma(j)} = \begin{cases} 1, & si\ \ i = \sigma(j). \\ 0, & si\ non. \end{cases}$$

$\delta_{i,j}$ représente le **symbole de Kronecker**.

Si σ est la permutation associée à la matrice de permutation P, on note P_σ au lieu de P.

1.5.2 Propriétés de la matrice de permutation

Proposition 1.27.

Si P_σ la matrice de permutation associée à la permutation σ:

1. $\sigma, \tau \in S_n$: $P_\sigma\, P_\tau = P_{\sigma o \tau}$, où (o) représente la loi de composition des applications.
2. L'ensemble des matrices de permutation d'ordre n noté P_n forme un sous-groupe du groupe multiplicatif des matrices carrés d'ordre n isomorphe au groupe symétrique S_n. Cet isomorphisme est l'application f : $(S_n, o) \to (P_n, .)$, $\sigma \to f(\sigma) = P_\sigma$.
3. P_σ est une matrice inversible. Si σ est paire $\det(P_\sigma)=1$, si non $\det(P_\sigma)= -1$, et l'inverse de P_σ est P_σ^{-1} qui égale à ${}^tP_\sigma$ (la matrice transposée de P_σ) et si P_σ est une matrice symétrique alors $P_\sigma^{-1} = P_\sigma$.
4. Multiplier une matrice M à droite par P_σ revient à permuter les colonnes de la

matrice M suivant la permutation σ.

5. Multiplier une matrice M à gauche par P_σ revient à permuter les lignes de la matrice M suivant la permutation inverse $P_\sigma^{-1} = {}^tP_\sigma$.
6. Les colonnes de la matrice P_σ sont les vecteurs de la base canonique de $\mathbb{R}^n$, dont on a modifié l'ordre. Si on note $e_1, e_2, \ldots, e_n$ ces vecteurs, alors $P_\sigma(e_i) = e_{\sigma(i)}$. Ainsi P_σ envoie une base orthonormale sur une base orthonormale, donc P_σ est une **matrice orthogonale**.

Exemple 1.18.

Soit la matrice $A = \begin{pmatrix} 1&0&1&1&1&0&0&0 \\ 0&1&1&1&0&1&0&0 \\ 1&1&0&1&0&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{pmatrix}$ et la matrice de permutation P_σ tel que $\sigma = \tau_{13}$ et soit la matrice $S = \begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \end{pmatrix}$ avec $S^{-1} = S$ alors :

Pour le produit $A.P_\sigma$ on permute la première et la troisième colonne de A et pour le produit $S.A$ on permute la première ligne avec la quatrième et la troisième ligne avec la deuxième ligne.

On trouve $A.P_\sigma = \begin{pmatrix} 1&0&1&1&1&0&0&0 \\ 1&1&0&1&0&1&0&0 \\ 0&1&1&1&0&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{pmatrix}$ et $S.A = \begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&0&1&0&0&1&0 \\ 0&1&1&1&0&1&0&0 \\ 1&0&1&1&1&0&0&0 \end{pmatrix}$.