Chapitre 1 Notions d'algèbre.

On va présenter dans ce chapitre quelques notions algébriques utilisées en théorie des codes et en cryptographie tout au long des chapitres qui suivent.

1.1 Groupes.

1.1.1 Groupe, sous-groupe et groupe quotient.

Définition 1.1.1. *Soit G* un ensemble muni d'une loi interne noté multiplicativement *(.),* alors, (*G*, .) est un *groupe*, si et seulement s'il vérifie les conditions suivantes:

1. La loi (.) est *associative*: $\forall\, x, y, z \in G : (x \,.\, y).\, z = x \,.\, (y \,.\, z)$
2. La loi (.) admet un *élément neutre* noté 1_G ou 1: $\forall\, x \in G : x.1 = 1.x = x$.
3. chaque élément *x* de G admet un *symétrique* noté x^{-1}: $\forall\, x \in G, \exists\, x^{-1} \in G : x^{-1}.x = x.x^{-1} = 1$.

Remarque 1.1.1.

1. Si la loi est noté additivement (+), l'élément neutre est noté 0_G ou 0, le symétrique de *x* est noté (–*x*) dit *opposé* de *x*.
2. Le groupe *G* est dit *commutatif* ou *abélien* si la loi (.) est commutative: $\forall\, x, y \in G : x.y = y.x$

Exemple 1.1.1.

1. $(\mathbb{Z}, +)$ est un groupe additif abélien.
2. $(\mathbb{R}^n, +)$ est un groupe abélien.
3. $(\mathbb{R}[X], +)$ est un groupe abélien.
4. $(\mathbb{R}^*, *)$ est un groupe multiplicatif abélien.
5. (S_n, o) ensemble des permutations de $E=\{1,..., n\}$, munit de la loi de composition est un groupe non abélien, dit *groupe symétrique* d'indice *n*.

Définition 1.1.2.

Soit (*G*, .) un groupe et $H \subset G$. *H* est un *sous-groupe* de *G* et on écrit $H \leq G$, si et seulement si,

1. $H \neq \emptyset$ $(1 \in H)$.
2. *H est stable par la loi (.) c'est-à-dire :* $x.y \in H$, *pour tous* $x, y \in H$.
3. *H est stable par passage à l'inverse c'est-à-dire :* $x^{-1} \in H$, *pour tous* $x \in H$.

La définition ci-dessus est équivalente à :

1. $H \neq \emptyset$
2. $H \leq G$, si et seulement si, $x.y^{-1} \in H$, pour tous $x, y \in H$.

Exemple 1.1.2

1. *G* et {1} sont des sous-groupes de G dits *sous-groupes triviaux*.
2. H sous-groupe de ($\mathbb{Z}$, +), si et seulement si, $\exists\, n\in\mathbb{N}$: H=$n\mathbb{Z}$.
3. $\mathbb{R}_n[X]$ est un sous-groupe de ($\mathbb{R}[X]$, +).
4. $\mathbb{R}_+^*$ est un sous-groupe de ($\mathbb{R}^*$, .).
5. A_n ensemble des permutations paires du groupe S_n est un sous-groupe de S_n.

Définition 1.1.3. Un sous-groupe *H* de *G* est dit *sous-groupe normal* dans *G* (on le note $H \trianglelefteq G$), si et seulement si, pour tout élément *g* de *G* on a : *gH=Hg*.

Hg={*hg*/ $h\in H$} et *gH* ={*gh*/ $h\in H$} dites les *classes à droites* respectivement *classes à gauche* modulo *H*. Dans le cas d'un groupe additif on les note $H+g=\{h+g/\ h\in H\}$ et $g+H=\{g+h/\ h\in H\}$

Cette définition est équivalente à: $H \trianglelefteq G$, si est seulement si, $\forall\, g\in G, h\in H: g.x.g^{-1} \in H$.

Exemple 1.1.3.

1- *H*=$n\mathbb{Z}$ est un sous-groupe normal de $\mathbb{Z}$.
2- Tout sous-groupe d'un groupe abélien est un sous-groupe normal.
3- A_n ensembles des permutations paires est un sous-groupe normal de (S_n, o).
4- $\mathbb{R}_n[X]$ est un sous-groupe de ($\mathbb{R}[X]$, +).

Proposition et définition 1.1.1. Soit (*G*, .) un groupe, *H* sous-groupe normal de *G*, la relation $\mathcal{R}$ définit par : $x, y \in G, x\,\mathcal{R}\, y \Leftrightarrow x.y^{-1}\in H$ est une relation d'équivalence compatible avec la loi (.), l'ensemble quotient $G/\mathcal{R}$ est noté *G/H* et l'opération définie dans *G/H* par : $\bar{x}\ .\ \bar{y}=\overline{x.y}$, est une loi interne dans *G/H* tel que : (*G /H*, .) est un groupe dit *groupe quotient* de *G* par *H*, d'élément neutre $1_{G/H}=H$ et pour tous $x\in H$, $(xH)^{-1} = x^{-1}H$.

Remarque 1.1.2.

1. Si *G* est abélien alors, *G/H l*'est aussi.
2. *gH=H* si et seulement si, $g\in H$.

Exemple 1.1.4. Soit *G*= ($\mathbb{Z}$, +) groupe abélien des entiers relatifs et *H*=$n\mathbb{Z}$ un sous-groupe normal de $\mathbb{Z}$, le groupe quotient $\mathbb{Z}$ /n$\mathbb{Z}$ est définie par : $\mathbb{Z}/n\mathbb{Z}= \{\bar{k}=k+n\mathbb{Z},\ k\in\mathbb{Z}\}$ et on a:

$\mathbb{Z}/n\mathbb{Z} =\{\bar{r},\ 0\leq r\leq n\text{-}1\}$.

Exemple 1.1.5. Soit *G*= ($\mathbb{R}[X]$, +) groupe abélien des polynômes à coefficients dans $\mathbb{R}$. H=$<X^2+1>$ le sous-groupe engendré par le polynôme P= X^2+1. Le groupe quotient $\mathbb{R}[X]/<X^2+1>$ est définie par : $\mathbb{R}[X]/<X^2+1>= \{\bar{P}=a\bar{X}+b,\ a, b\in\mathbb{R}\}$ et $(\mathbb{R}[X]/<X^2+1>, +) \cong (\mathbb{C}, +)$.

1.1.2 Groupe monogène et groupe cyclique.

Définition 1.1.4. Un groupe G est dit *groupe monogène* s'il admet un générateur $a \in G$,
c.à.d. $\exists\, a \in G$, pour tout $g \in G$, $\exists k \in \mathbb{Z}$ tel que $g=a^k$
On note le groupe monogène engendré par a par: $G=\langle a\rangle$ et on a: $G=\langle a\rangle=\{a^k / k\in\mathbb{Z}\}$.
Si le groupe G est additif alors, $G=\langle a\rangle=\{ka / k\in\mathbb{Z}\}$.

Exemple 1.1.6. $(\mathbb{Z}, +)$ est un groupe monogène additif engendré par : $a=1$ ou $a=-1$.
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe monogène engendré par : $a=\bar{1}$ ou $a=-\bar{1}$

Définition 1.1.5. Un groupe G est dit *groupe cyclique* s'il est monogène fini. Tout générateur a de G est appelé *élément primitif* de G. On note $G=\langle a\rangle=\{a^k / k\in\mathbb{Z}\}$ et on a si G est d'ordre n alors : $G=\{ a^k / k\in\{0,..,n-1\}\}=\{1, a, a^2,\ldots, a^{n-1}\}$. Dans le cas d'un groupe cyclique additif d'ordre n on note $G=\{ka / k\in\{0,..,n-1\}\}=\{0, a, 2a, \ldots, (n-1)a\}$

Exemple 1.1.7.

1. *Le groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique additif d'ordre n et $\mathbb{Z}/n\mathbb{Z} =\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.
2. L'ensemble $C=\{z\in\mathbb{C}: z^n=1\}$des racines nièmes de l'unité dans $\mathbb{C}$ forme un groupe multiplicatif cyclique d'ordre n.

1.1.3 Morphisme et groupes isomorphes.

Définition 1.1.6. Soit $(G, .)$, $(G', .)$ deux groupes et soit f une application de G dans G' alors,

1. f est dite *morphisme de groupes*, si et seulement si,
   pour tous $x, y\in G :\ f(x .y)= f(x). f(y)$.
2. Le *noyau* de f est l'ensemble noté *Kerf* défini par: $Kerf =\{x\in G : f(x)=1_{G'}\}$.
3. L'*image* de f est l'ensemble noté *Imf* défini par: $Imf=\{y\in G': \exists x\in G: y= f(x)\}$ ou encore $\mathrm{Im}f =\{f(x) / x\in G\}$.

Proposition 1.1.2.

1. *Kerf* est un sous-groupe normal de G.
2. *Imf* est un sous-groupe de G'.

Remarque 1.1.3.
Si f est bijectif, il est dit *isomorphisme* et G et G' sont dits *isomorphes* et on écrit $G \cong G'$.
Si $G=G'$, f est dit *endomorphisme* et si de plus il est bijectif alors f est dit *automorphisme*.

Proposition 1.1.3. Tout groupe monogène infini (respectivement cyclique d'ordre n) est isomorphe au groupe $\mathbb{Z}$ (respectivement $\mathbb{Z}/n\mathbb{Z}$).

Théorème 1.1.1.

Si $f:(G,.)\to(G',.)$ un morphisme de groupes alors : $G/Kerf \cong Imf$.

Pour tout x de G on peut identifier la classe de x ($xKerf$) par son image $f(x)$.

1.2 Anneaux.

1.2.1 Anneau, idéal, anneau principal.

Définition 1.2.1. Soit A un ensemble et (+) ,(.) Deux lois dans A. $(A, +, .)$ est un *anneau*, si et seulement s'il vérifie les conditions suivantes:

1. $(A, +)$ groupe abélien (d'élément neutre 0_A ou 0 dit *élément nul*).
2. (.) associative et distributive sur (+).
3. (.) admet un élément neutre noté 1_A ou 1.
4. Si la loi (.) est commutative alors A est dit *anneau commutatif*.

Définition 1.2.2. Soit A un anneau, un élément x de $A-\{0\}$ est dit *diviseur de zéro* s'il existe un élément y de $A-\{0\}$ tel que $x.y = 0$ ou $y.x = 0$.

Définition 1.2.3. Un anneau A est dit *anneau intègre* s'il n'admet pas de diviseurs de zéro.

Exemple 1.2.1.

1. Les anneaux $(\mathbb{Z}, +, .)$, $(\mathbb{R}, +, .)$ et $(\mathbb{R}[X], +, .)$ sont des anneaux commutatifs intègres.
2. $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, .)$ est un anneau non intègre.

Définition 1.2.4.

1. Un élément $a\in A-\{0_A\}$ est dit *inversible* (ou *unité*) dans A s'il existe un élément b de $A-\{0_A\}$ tel que $a.b = b.a = 1_A$.

   L'ensemble des unités de A est noté $\mathcal{U}(A)$ ou A^*. i.e. $\mathcal{U}(A)= \{a\in A, \text{ a inversible}\}$.
2. Si tout élément non nul de A est inversible alors l'anneau $U(A)= A-\{0\}$ est dit *corps*.

Proposition 1.2.1. $(\mathcal{U}(A), .)$ est un groupe multiplicatif dit *groupe des unités* de A.

Définition 1.2.5. Soit $(A, +, .)$ un anneau, $I\subset A$ est dit *idéal* de A si et seulement si,

1. $I \leq (A, +)$.
2. Pour tous $x\in I, a\in A : xa\in I$ et $ax\in I$.

Exemple 1.2.2. Si A est un anneau commutatif et $a \in A$

1. *{0} et A* sont des ideaux de A dit 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 *et* ax est dit *multiple* de a et I est donc l'ensemble des multiples de a dans A .
3. $I=n\mathbb{Z} = <n>$ ensemble des multiples de n dans $\mathbb{Z}$ est un idéal principal de $\mathbb{Z}$.

Remarque 1.2.1.

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

Exemple 1.2.3.

1. L'anneau $\mathbb{Z}$ est principal.
2. L'anneau $\mathbb{R}[X]$, est un anneau principal.

1.2.2 Morphisme d'anneaux, anneau quotient et anneau Euclidien.

Définition 1.2.7. $(A, +, .)$, $(A', +, .)$ deux Anneaux, une application f de A dans A' est dite *morphisme d'anneaux*, si et seulement si, pour tous $x, y \in A$ on a :

1. $f(x+y)= f(x)+ f(y)$.
2. $f(x.y)= f(x). f(y)$.
3. $f(1_A)=1_{A'}$.

On définit le *noyau* et l'*image* du morphisme d'anneaux f qu'on note *Kerf* et *Imf* respectivement, comme suit : $Kerf = \{x \in A, f(x)=0_A\} \subset A$, $Imf = \{ f(x), x \in A\} \subset A'$.

Remarque 1.2.2. Soit f un morphisme d'Anneau de A dans A', on a alors :

1. f injective, si et seulement si, $Kerf = \{0_A\}$.
2. f surjective, si et seulement si, $Imf = A'$.

Théorème 1.2.1. Soit A, A' deux anneaux, f un morphisme d'anneaux de A dans A', on a alors :
Kerf est un idéal de A et $A/Kerf \cong Imf$.

Définition 1.2.8. 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 de groupe additif et donc *Kerf* est un idéal de ($\mathbb{Z}$, +) donc,

$\exists\, n \in \mathbb{N}$ tel que $Kerf = n\mathbb{Z}$. L'entier *n* est appelé la *caractéristique* de *A*, noté car(*A*)

Propriétés 1.2.1.

1. Si *f* est injectif (n=0), *A* est dit de caractéristique nulle.
2. Si f n'est pas injectif ($n \neq 0$), on dit que *A* est de caractéristique *n* et on écrit car(*A*)=*n*.

Remarque 1.2.2. Soit *A* un anneau de caractéristique *n* alors :

n est le plus petit entier positive non-nul s'il existe vérifiant : $n.1_A=0$, si non $n=0$.

Proposition et Définition 1.2.2. Soit (*A*, +, .) un anneau, *I* idéal de *A*, comme *I* est normal dans (*A*, +) alors (*A/I*, +) tel que la loi (+) est définie par : $\bar{x}+\bar{y}=\overline{x+y}$ est un groupe abélien.
La loi (.) dans *A* est compatible avec la relation d'équivalence définie par :
$x\ R\ y$, si et seulement si, $x - y \in I$, on définit donc dans *A/I* la loi (.) par : $\bar{x}\ .\ \bar{y}=\overline{x.y}$.
(*A/I*, +, .) est un anneau, dit *anneau quotient* de *A* par *I*.

Exemple 1.2.4. 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 : $\forall\, x, y \in \mathbb{Z} : \bar{x}+\bar{y} = \overline{x+y} \Leftrightarrow (x+ n\mathbb{Z}) + (y+ n\mathbb{Z})=(x+y) + n\mathbb{Z}$.

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

Proposition 1.2.3. Soit *A* un anneau et *I* idéal de *A* on a alors :

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

Proposition et Définition 1.2.4.

1. Un élément *a* de *A* est *premier* si est seulement si <*a*> est un idéal premier.
2. Un élément *a* de *A* est *irréductible* si et seulement si <*a*> est un idéal maximal.

On a les équivalences suivantes :

1. *a* premier, si et seulement si, *A*/<*a*> anneau intègre.
2. *a* irréductible, si et seulement si *A*/<*a*> corps.

Définition 1.2.4. 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 :
$\forall\, x, y \in A$ tel que $y \neq 0_A$, $\exists!\, q, r \in A \quad x = yq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(y)$. 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.

Exemple 1.2.5.

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

1.3 Corps et corps fini

1.3.1 Construction d'un corps fini.

Définition 1.3.1. Un *corps* $(K, +, .)$ est un anneau unitaire dans lequel tout élément non nul admet un inverse.

1. Un corps K est *corps commutatif* si la loi (.) est commutative
2. Un corps K est dit *corps fini* si son cardinal est fini.

Proposition 1.3.1.

1. Si K un corps alors la caractéristique de K est nulle ou un entier premier.
2. Si K corps fini, alors car(K) est p premier et K admet un sous corps isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
   Dans ce cas on peut considérer que $\mathbb{F}_p$ est un sous-corps de K dit *sous-corps premier* de K.

Proposition et définition 1.3. 2. Si K est un corps commutatif fini alors $(K^*, .)$ est un groupe cyclique et tout générateur α de K^* est dit racine primitive de K, le polynôme minimal associé à cette racine est appelé polynôme primitif de K qu'on note M_α.

Rappelons que le polynôme minimale d'un élément β d'un corps fini K de caractéristique un entier premier p est le polynôme générateur de l'idéal (principal) I_β définie par: $I_\beta = \{P \in \mathrm{F}_p[X]: P(\beta) = 0\}$
Remarque 1.3.1. M_α est un polynôme unitaire de degré minimal dans I_β, irréductible sur $\mathbb{F}_p$ et vérifiant $M_\alpha(\alpha) = 0$.

Théorème 1.3.1. (Waderburn) Tout corps fini K est commutatif.

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

Théorème 1.3. 2. Tout corps fini 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.

1.3.2 Existence des corps finis.

Définition 1.3.2. Une extension L d'un corps commutatif K est dite corps de rupture (respectivement corps de décomposition) d'un polynôme P sur K, ($P \in K[X]$), si et seulement si, $\exists \alpha \in K$, $a \in L$, (respectivement $a_1, a_2, \ldots, a_n \in L$ tel que $P=\alpha(X-a)Q$
(Respectivement $P=\alpha \prod_{i=1}^{i=n}(X-a_i)$) avec $Q \in K[X]$.

Proposition 1.3.3. Soit K un corps commutatif et $P \in K[X]$ avec $d^\circ(P) \geq 1$ alors P admet un corps de rupture et un corps de décomposition sur K.

Théorème 1.3.2. Si $n \in \mathbb{N}^*$ et p entier premier alors il existe un corps fini K de cardinal p^n et un polynôme irréductible P sur $\mathbb{F}_p$ de degré n.

1.3.3 Corps de Galois.

Proposition et définition 1.3.4. 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 1.3.2. Pour décrire le corps de Galois K de caractéristique p sur le corps r, 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 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 1.3.1. Construction d'un corps de Galois $K= \mathbb{F}_9$, $q= 9 =3^2$ donc $p=\text{car}(K)=3$, $r=d^\circ(M_\alpha)=2$, $\mathbb{F}_9= \{0\} \cup \mathbb{F}_9^* = \{0, \alpha^i, 0 \leq i \leq 7\} = \{0, 1, \alpha, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$. 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 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 $\mathbb{F}_9=\{a\overline{X}+b/\ a, b\in \mathbb{F}_3\}$. Posons $\overline{X}=\beta$, alors $\mathbb{F}_9=\{0, 1, 2, \beta, 2\beta, \beta+1, \beta+2, 2\beta+1, 2\beta+2\}$.

Exemple 1.3.2. Construction d'un corps de Galois de cardinal $q=8=2^3$ donc $p=\text{car}(K)=2$,
$\mathbb{F}_8=\{0\}\cup\mathbb{F}_8^*=\{0, \alpha^i, 0\leq i\leq 6\}=\{0, 1, \alpha, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. 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 $\mathbb{F}_8=\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1\ \alpha^2+\alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$.

1.4 Matrice de permutation.

1.4.1 Definitions

Défnition 1.4.1 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
Si $P=(p_{ij})_{1\leq i, j\leq n}$; $\exists\ \sigma\in S_n$ (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*.

1.4.2 Propriétés

Proposition 1.4.1 Si P_σ la matrice de permutation associée à la permutation σ:

1. L'ensemble des matrices de permutation d'ordre n noté P_n forme un sous-groupe isomorphe au groupe symétrique S_n.
2. P_σ est une matrice inversible. Si σ est paire $\det(P_\sigma)=1$, si non $\det(P_\sigma)=-1$.
3. L'inverse de P_σ est P_σ^{-1} qui égale à ${}^tP_\sigma$ (la matrice transposée de P_σ)
4. Multiplier une matrice *M* à droite par P_σ revient à permuter les colonnes de la matrice A suivant la permutation σ.
5. Multiplier une matrice *M* à gauche par P_σ revient à permuter les lignes de la matrice A suivant la **permutation inverse** P_σ^{-1}de P_σ.
6. On a $P_\sigma^{-1}=P_\sigma^t$ et si P_σ est une matrice symétrique alors $P_\sigma^{-1}=P_\sigma$.

Exemple 1.3.3.

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_σ on permute la première et la troisième colonne de A et pour S.A on permute la première ligne avec la quatrième et la troisième ligne avec la deuxième ligne.

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 $S.A=\begin{pmatrix} 1&1&1&1&1&1&1&1\\ 1&1&0&1&0&0&1&0\\ 0&1&1&1&0&1&0&0\\ 1&0&1&1&1&0&0&0 \end{pmatrix}$.