Chapitre 12 — "L'essentiel" sur les groupes et anneaux

Préambule. Ce chapitre a pour principal objet la définition de nouvelles structures, qui sont sous-jacentes à la plupart des ensembles dans lesquels vous êtes habitués à faire des maths (les ensembles de nombres entiers, réels ou complexes, de suites, de fonctions, de polynômes notamment).

Au-delà des définitions (qui sont comme toujours à connaître), le plus important est surtout de bien avoir en tête les nombreux exemples de groupes et d'anneaux présentés dans ce chapitre ; ce seront les acteurs principaux de l'algèbre linéaire (étudiée au second semestre, et en Spé).

Quant aux propriétés de ce cours (binôme de Newton, propriétés des éléments inversibles, propriétés des éléments nilpotents), elles seront surtout utilisées dans le cadre des matrices : dès le chapitre portant sur le calcul matriciel, et encore une fois, en algèbre linéaire.

Table des matières

1. Lois de composition interne

1.1. **Généralités.** Une loi de composition interne sur un ensemble E est un moyen d'associer à 2 éléments x et y de E un nouvel élément de E noté $x * y$. Formellement :

Définition. Soit E un ensemble. On appelle **loi de composition interne (ℓci) dans** E une application $\varphi : E \times E \longrightarrow E$.

Par la suite, on convient de noter $x * y$ l'image $\varphi(x, y)$.

Exemples.

1/ L'addition (ou la multiplication) des entiers, des rationnels, des réels, des complexes, des polynômes à coefficients réels ou complexes, des fonctions continues sur $\mathbb{R}$, ou des suites réelles est une ℓci dans $\mathbb{Z}$, dans $\mathbb{Q}$, dans $\mathbb{R}$, dans $\mathbb{C}$, dans $\mathbb{K}[X]$,[1] dans $\mathscr{C}^0(\mathbb{R}, \mathbb{R})$ ou dans $\mathbb{R}^{\mathbb{N}}$ respectivement.

2/ La soustraction est une ℓci dans $\mathbb{Z}$, mais pas dans $\mathbb{N}$.

3/ La multiplication est une ℓci dans $\mathbb{R}_+^*$; mais pas dans $\mathbb{R}_-^*$.

4/ L'union (ou l'intersection) donne lieu à une ℓci dans $\mathscr{P}(E)$.

1. La notation $\mathbb{K}[X]$ désigne l'ensemble des polynômes à coefficients dans $\mathbb{K}$, càd pour faire court l'ensemble des écritures formelles : $a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ où n désigne un entier naturel et les a_i des éléments de $\mathbb{K}$.

5/ Pour n un entier naturel, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n. L'addition donne lieu à une ℓci dans $\mathbb{K}_n[X]$ (le degré d'une somme de polynômes de $\mathbb{K}_n[X]$ étant au plus égal à n). Mais pas la multiplication : X^2 et X sont dans $\mathbb{K}_2[X]$, pas X^3 !

6/ Soit E un ensemble. La composition usuelle des applications est une ℓci sur E^E.

7/ *(S2i)* Dans $\mathbb{R}^3$, le produit vectoriel est une ℓci (le produit vectoriel de deux vecteurs étant un vecteur). Mais le produit scalaire n'en est pas une (le produit scalaire de deux vecteurs étant un nombre réel, et pas un vecteur).

8/ Une **matrice carrée de taille 2 à coefficients réels** est un tableau de réels à 2 lignes et 2 colonnes : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. L'ensemble des matrices carrées de taille 2 est noté $\mathrm{M}_2(\mathbb{R})$. Pour deux éléments

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{et} \qquad A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

on définit l'addition et la multiplication en posant :

$$A + A' = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \qquad \text{et} \qquad A \times A' = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

L'addition et la multiplication donnent encore lieu à des ℓci dans $\mathrm{M}_2(\mathbb{R})$.

Définition. Soit E un ensemble, muni d'une ℓci notée $*$.

La ℓci $*$ est :

➤ **associative** si : $\forall\, (x,y,z) \in E^3,\ (x * y) * z = x * (y * z)$.

➤ **commutative** si : $\forall\, (x,y) \in E^2,\ x * y = y * x$

Exemples.

1/ L'addition (ou la multiplication) des entiers, des rationnels, des réels, des complexes, des polynômes à coefficients réels ou complexes, des fonctions continues sur $\mathbb{R}$, ou des suites réelles sont des ℓci associatives et commutatives.

2/ L'union (ou l'intersection) de deux parties de E est une ℓci (dans $\mathscr{P}(E)$) associative et commutative.

3/ L'addition des polynômes dans $\mathbb{K}_n[X]$ est une ℓci associative et commutative. La multiplication des polynômes dans $\mathbb{K}[X]$ est une ℓci associative et commutative.

4/ L'addition des matrices dans $\mathrm{M}_2(\mathbb{R})$ est une ℓci associative et commutative.

5/ Soit E un ensemble. La composition usuelle des applications est une ℓci associative mais NON-commutative sur E^E. Plus généralement, la composition des applications est associative, mais non commutative.

6/ La multiplication des matrices dans $\mathrm{M}_2(\mathbb{R})$ est une ℓci associative mais NON-commutative. Par exemple :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ et : } \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

1.2. Elément neutre pour une ℓci.

Définition - Propriété. Soit E un ensemble, muni d'une ℓci notée $*$.

Un élément x de E est **neutre** si : $\forall\, y \in E,\ x * y = y * x$.

Lorsque la loi $*$ est associative, l'élément neutre est unique (dès qu'il existe), et est souvent noté e.

Exemples.

1/ Dans $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ le neutre pour l'addition (*resp.* la multiplication) est 0 (*resp.* 1).

2/ Dans $\mathscr{P}(E)$, le neutre pour l'union (*resp.* l'intersection) est $\emptyset$ (*resp.*E).

3/ Dans $\mathbb{K}[X]$, le neutre pour l'addition est le polynôme nul, noté $0_{\mathbb{K}[X]}$ ou $\widetilde{0}$.

4/ Dans $\mathscr{C}^1(\mathbb{R},\mathbb{R})$, le neutre pour l'addition est la fonction identiquement nulle sur $\mathbb{R}$.

5/ Dans $\mathrm{M}_2(\mathbb{R})$, le neutre pour l'addition est la matrice nulle $0_{\mathrm{M}_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Le neutre pour la multiplication est la matrice $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

6/ Dans $\mathbb{R}^{\mathbb{N}}$, le neutre pour l'addition est la suite nulle.

7/ Dans E^E, l'élément neutre pour la composition des applications est id_E (l'identité de E).

1.3. Eléments inversibles pour une ℓci.

Définition - Propriété. Soit $(E, *)$ un ensemble muni d'une ℓci associative, pour laquelle il existe un élément neutre e.

Un élément x de E est dit **inversible** s'il existe un élément y de E tel que :

$$x * y = \mathrm{e} \qquad \underline{\underline{\mathrm{ET}}} \qquad y * x = \mathrm{e}.$$

Lorsque la loi $*$ est associative, y est unique (dès qu'il existe) : il est alors appelé **inverse** de x et est noté x^{-1}.

Exemples.

1/ Dans $\mathbb{Z}$, l'inverse de n pour l'addition est son opposé $-n$. Il en serait de même dans $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ (toujours pour la somme).

2/ Dans $\mathbb{R}$, tout réel non nul est inversible pour la multiplication. Il n'en est pas de même dans $\mathbb{Z}$: par exemple 2 n'est pas inversible pour la multiplication.

3/ Dans $\mathbb{K}[X]$, tout polynôme est inversible pour l'addition, et a pour inverse $-P$. En revanche, X n'est pas inversible pour la multiplication dans $\mathbb{K}[X]$ (de fait, seuls les polynômes constants non nuls le sont).

4/ Dans $\mathbb{R}^{\mathbb{N}}$, l'inverse d'une suite u pour l'addition est son opposée $-u$ (et son inverse pour la multiplication existe SSI tous ses termes sont non nuls).

5/ Dans E^E, une application f est inversible pour la composition SSI elle est bijective.

6/ Dans $\mathrm{M}_2(\mathbb{R})$, l'inverse d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pour l'addition est son opposée : $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. En outre, nous verrons dans le prochain chapitre que A est inversible pour la multiplication SSI son déterminant est non nul ($ad - bc \neq 0$). Dans ce cas, son inverse est :

$$A^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

(Propriétés de l'inverse). Soit E un ensemble muni d'une ℓci associative $*$, qui admet un élément neutre e.

1/ Si x et y sont deux éléments inversibles de E, alors $x * y$ est inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$

2/ Si x est un élément inversible de E, alors x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.

Remarque. On utilisera essentiellement cette propriété :

- dans le cadre des matrices, pour affirmer que le produit de deux matrices inversibles A et B dans $\mathrm{M}_n(\mathbb{K})$ est inversible, et que :

$$(A \times B)^{-1} = B^{-1} \times A^{-1}$$

- dans le cadre des applications, pour affirmer que la composée de deux bijections (de E dans E) f et g est bijective, et que :

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

2. Groupes et sous-groupes

2.1. Groupes : définitions et exemples.

Définition. $(G,*)$ est un **groupe** si :

(G1) $*$ est une ℓci sur G ;

(G2) la ℓci $*$ est associative ;

(G3) la ℓci $*$ admet un élément neutre (noté e_G ou e) ;

(G4) tout élément g de G est inversible (pour $*$).

Si de plus la ℓci $*$ est commutative, on dit que $(G,*)$ est un **groupe abélien**.

Exemples.

1/ $(\mathbb{Z},+)$, $(\mathbb{D},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes abéliens.

2/ $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $\left(\mathbb{R}_+^*,\times\right)$, $(\mathbb{C}^*,\times)$ sont des groupes abéliens.

3/ $(\mathbb{N},+)$ n'est pas un groupe. Dans $\mathbb{N}$, l'addition est une ℓci, associative, commutative, avec un élément neutre (0) ; mais un entier naturel n'est pas inversible (sauf s'il est nul) dans $\mathbb{N}$.

4/ $(\mathbb{Z},\times)$ n'est pas un groupe (3 n'est pas inversible dans $\mathbb{Z}$ pour la loi $\times$).

5/ $(\mathbb{K}[X],+)$, $(\mathbb{K}_n[X],+)$, $\left(\mathbb{K}^{\mathbb{N}},+\right)$, $\left(\mathrm{M}_2(\mathbb{R}),+\right)$, $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+\right)$ sont des groupes abéliens.

6/ $(\mathbb{U},\times)$ est un groupe abélien. Et pour tout entier naturel $n \geqslant 2$, $(\mathbb{U}_n,\times)$ est un groupe abélien.

7/ $\left(E^E,\circ\right)$ n'est pas un groupe (toute application de E dans E n'est pas bijective). En revanche, l'ensemble des bijections de E dans E (également appelées **permutations de** E), noté σ_E, est un groupe (non abélien) pour la composition.

8/ $\left(\mathrm{Sim}^+(\mathbb{C}),\circ\right)$ est un groupe ($\mathrm{Sim}^+(\mathbb{C})$ désignant l'ensemble des similitudes directes du plan complexe) non abélien.

9/ $(\mathbb{K}[X],\times)$, $(\mathbb{K}_n[X],\times)$, $\left(\mathbb{K}^{\mathbb{N}},\times\right)$ ne sont pas des groupes.

10/ $(\mathscr{P}(E),\cap)$ n'est pas un groupe, sauf si $E=\emptyset$ (auquel cas on a un groupe à un élément). Idem pour $(\mathscr{P}(E),\cup)$.

11/ Un groupe $(G,*)$ est un **groupe fini** lorsque G a un nombre fini d'éléments.

Le groupe à un élément $(\{\mathrm{e}\},*)$ est appelé **groupe trivial**.

On montre que tout groupe fini de cardinal $\leqslant 4$ est abélien (en écrivant les différentes tables de multiplication de ces groupes).

Il est encore vrai que tout groupe de cardinal 5 est abélien (en utilisant un théorème de Lagrange sur les groupes au programme de MP).

En revanche, il existe au moins un groupe de cardinal 6 non-abélien : voir l'exemple présenté dans le paragraphe suivant.

2.2. Un exemple-clef : le groupe des bijections de $[\![\,1,3\,]\!]$ dans $[\![\,1,3\,]\!]$.

Notons S_3 l'ensemble des bijections de $E=\{1,2,3\}$ dans lui-même [2].

➤ Loi de composition interne : c'est ici la composition usuelle des applications. En effet, si f et g sont deux bijections de E dans E, alors $g\circ f$ est encore une bijection de E dans E, puisque la composée de deux bijections est encore une bijection (voir chapitre "Applications").

En outre, cette loi est associative, puisque la composition usuelle des applications l'est : $\forall\,(f,g,h)\in S_3^3,\ f\circ(g\circ h)=(f\circ g)\circ h$.

2. Une bijection de E dans E est appelée une **permutation** de E.

➤ Elément neutre : l'identité de E (notée id_E) est l'élément neutre pour la composition puisque pour toute $f \in S_3$ on a : $f \circ \mathrm{id}_E = \mathrm{id}_E \circ f = f$.

➤ Tout élément de S_3 est inversible : car si f est une bijection de E dans E, alors f admet une bijection réciproque f^{-1} qui est encore une bijection de E dans E.

L'ensemble S_3 est muni d'une loi de composition interne associative (la composition usuelle des applications), pour laquelle il existe un élément neutre (id_E), et où tout élément est inversible. Ainsi, $(S_3, \circ)$ est un groupe, appelé groupe des **permutations** d'un ensemble à 3 éléments.

De plus, il existe exactement six bijections de E dans E : en effet, pour définir une bijection de E dans E, on peut commencer par choisir l'image de 1 (trois choix possibles), puis celle de 2 (plus que deux choix) et enfin celle de 3 qui ne peut être que le dernier élément de E restant. Explicitement, ces six bijections sont :

$$\mathrm{id}_E : \begin{array}{ccc} 1 & \longmapsto & 1 \\ 2 & \longmapsto & 2 \\ 3 & \longmapsto & 3 \end{array} \qquad (123) : \begin{array}{ccc} 1 & \longmapsto & 2 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 1 \end{array} \qquad (132) : \begin{array}{ccc} 1 & \longmapsto & 3 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 2 \end{array} \qquad (12) : \begin{array}{ccc} 1 & \longmapsto & 2 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 3 \end{array} \qquad (13) : \begin{array}{ccc} 1 & \longmapsto & 3 \\ 2 & \longmapsto & 2 \\ 3 & \longmapsto & 1 \end{array} \qquad (23) : \begin{array}{ccc} 1 & \longmapsto & 1 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 2 \end{array}$$

Le groupe $(S_3, \circ)$ est un groupe à 6 éléments.

Pour finir, avec les notations précédemment introduites :

$$(12) \circ (13) : \begin{array}{ccc} 1 & \longmapsto & 3 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 2 \end{array} \quad \text{tandis que} \quad (13) \circ (12) : \begin{array}{ccc} 1 & \longmapsto & 2 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 1 \end{array} \quad \text{d'où } (12) \circ (13) \neq (13) \circ (12).$$

Conclusion. Le groupe $(S_3, \circ)$ est un groupe à 6 éléments, et n'est pas abélien.

2.3. **Sous-groupes.**

Soit $(G, *)$ un groupe. Un **sous-groupe** de G est un groupe $(H, *)$, où H est une partie de G. Cette définition formelle est assez peu utile en pratique, et on utilise plutôt la propriété ci-dessous pour caractériser les sous-groupes.

Caractérisation des sous-groupes. Soit $(G, *)$ un groupe. $(H, *)$ est un sous-groupe de G si :

- **(SG1)** $H \subset G$
- **(SG2)** $\mathrm{e} \in H$
- **(SG3)** $\forall\, (h, h') \in H^2,\ h * h' \in H$ (H est stable pour $*$)
- **(SG4)** $\forall h \in H,\ h^{-1} \in H$ (H est stable par passage à l'inverse).

Exemples :

1/ $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{D}, +)$ qui est un sous-groupe de $(\mathbb{Q}, +)$ qui est un sous-groupe de $(\mathbb{R}, +)$ qui est un sous-groupe de $(\mathbb{C}, +)$.

2/ Pour $n \in \mathbb{N}$, $(\mathbb{K}_n[X], +)$ est un sous-groupe de $(\mathbb{K}[X], +)$.

3/ Pour tout entier naturel $n \geqslant 2$, $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ qui est un sous-groupe de $(\mathbb{C}^*, \times)$.

4/ Lorsque $(G, *)$ est un groupe, $(\{\mathrm{e}_G\}, *)$ est un sous-groupe (sous-groupe trivial).

5/ Dans $(S_3, \circ)$ (défini plus haut), il existe trois sous-groupes à deux éléments : $(\{\mathrm{id}, (12)\}, \circ)$, $(\{\mathrm{id}, (13)\}, \circ)$ et $(\{\mathrm{id}, (23)\}, \circ)$. Il existe également un sous-groupe à 3 éléments $(\{\mathrm{id}, (123), (132)\}, \circ)$; ce dernier est appelé sous-groupe des permutations paires de S_3, et il est noté A_3.

Remarque. Tout sous-groupe d'un groupe abélien est lui-même abélien. On ne peut rien dire en général d'un sous-groupe non-abélien.

2.4. Morphismes de groupes.

Définition. Un morphisme de groupes de $(G, *)$ dans $(H, \sharp)$ est une application $f : G \longrightarrow H$ telle que :

$$\forall\, (g, g') \in G^2, \quad f\,(g * g') = f(g) \sharp f(g')$$

Exemples.

1/ L'application $x \in \mathbb{R} \longmapsto \mathrm{e}^x \in \mathbb{R}_+^*$ est un morphisme de groupes.

2/ L'application $z \in \mathbb{U}_5 \longmapsto z^3 \in \mathbb{U}_5$ est un morphisme de groupes.

Propriétés. Soit f un morphisme de groupes de $(G, *)$ dans $(H, \sharp)$. On a :

$$1/ \quad f\,(\mathrm{e}_G) = \mathrm{e}_H \qquad \text{et} \qquad 2/ \quad \forall\, g \in G,\ f\left(g^{-1}\right) = [f(g)]^{-1}$$

Définitions. Soit f un morphisme de groupes de $(G, *)$ dans $(H, \sharp)$.

1/ Le **noyau de** f est la partie de G notée $\ker f$ définie par :

$$\ker f = \{g \in G,\ f(g) = \mathrm{e}_H\}$$

2/ L'**image de** f est la partie de H notée $\mathrm{im} f$ définie par :

$$\mathrm{im} f = f(G) \qquad \text{càd} \qquad \mathrm{im} f = \{f(g),\ g \in G\}$$

Propriétés. Soit f un morphisme de groupes de $(G, *)$ dans $(H, \sharp)$. Alors :

1/ $\ker f$ est un sous-groupe de G.

2/ $\mathrm{im} f$ est un sous-groupe de H.

3/ f est injective SSI $\ker f = \{\mathrm{e}_G\}$

4/ f est surjective SSI $\mathrm{im} f = H$

3. Anneaux

3.1. Anneaux : définitions et exemples.

Définition. Un **anneau** $(A,+,\times)$ est un ensemble A muni de deux ℓci associatives telles que :

1/ $(A,+)$ est un groupe abélien (de neutre 0_A) ;

2/ $\exists 1_A \in A,\ \forall a \in A,\ 1_A \times a = a \times 1_A = a$ (1_A neutre pour la multiplication) ;

3/ $\forall a \in A,\ 0_A \times a = a \times 0_A = a$ (0_A élément **absorbant**) ;

4/ $\forall (a,b,c) \in A^3,\ a \times (b+c) = a \times b + a \times c$ (distributivité de $\times$ par rapport à $+$).

De plus, l'anneau $(A,+,\times)$ est dit **commutatif** si la loi $\times$ est commutative.

Exemples :

1/ $(\mathbb{Z},+,\times)$, $(\mathbb{D},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.

2/ $\left(\mathscr{C}^1(\mathbb{R},\mathbb{R}),+,\times\right)$ est un anneau commutatif : l'anneau des fonctions de classe $\mathscr{C}^1$ sur $\mathbb{R}$ et à valeurs réelles.

3/ $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ est un anneau commutatif : l'anneau des suites réelles.

4/ $(\mathbb{K}[X],+,\times)$ est un anneau commutatif : l'anneau des polynômes à coefficients dans $\mathbb{K}$.

5/ $(\mathrm{M}_2(\mathbb{R}),+,\times)$ est un anneau NON commutatif : celui des matrices carrées de taille 2 à coefficients réels.

3.2. Quelques propriétés des anneaux.

Remarque. En général, dans un anneau (non commutatif), les identités remarquables "de votre enfance" ne sont plus valables. Par exemple, pour tout couple (a,b) d'éléments de A, on a :

$$(a+b)^2 = a^2 + a \times b + b \times a + b^2$$

Mais attention ! Il se peut très bien que :

$$a^2 + a \times b + b \times a + b^2 \neq a^2 + 2a \times b + b^2$$

Néanmoins, sous réserve que l'on choisisse des éléments de l'anneau qui commutent (càd des éléments a et b tels que $ab = ba$), on aura toujours le droit d'utiliser les indetités remarquables bien connues, comme le justifie la propriété ci-dessous.

Formule du binôme de Newton dans un anneau. Soient a et b deux éléments de A, **tels que** $a \times b = b \times a$ (on dit que a et b **commutent**). On a :

$$\forall n \in \mathbb{N},\ (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} b^k \times a^{n-k}$$

Remarque. La nouvelle application de cette formule sera le calcul de A^N pour une matrice carrée $A \in \mathrm{M}_n(\mathbb{K})$.

Propriétés. Soient a et b deux éléments de A, **tels que** $a \times b = b \times a$. On a :

1/ $\forall n \in \mathbb{N}^*,\ a^n - b^n = (a-b) \times \sum_{k=0}^{n-1} a^k \times b^{n-1-k} = (a-b) \times \sum_{k=0}^{n-1} b^k \times a^{n-1-k}$

2/ $\forall n \in \mathbb{N}^*,\ 1_A - a^n = (1_A - a) \times \sum_{k=0}^{n-1} a^k$ càd : $1_A - a^n = (1_A - a)\left(1_A + a + a^2 + \cdots + a^{n-1}\right)$

Remarque. La seconde proriété, qui est un corollaire immédiat de la première, est celle dont on se sert pratiquement pour :

- ➤ Justifier que les racines du polynôme $1+X+\cdots+X^n$ sont exactement les éléments de $\mathbb{U}_{n+1}\setminus\{1\}$;
- ➤ Calculer l'inverse d'une matrice A, dans des cas particuliers.

3.3. Vilains petits canards : diviseurs de zéro et éléments nilpotents.

Les notions présentées ici seront presque exclusivement utilisées dans l'anneau des matrices carrées (chapitre suivant et futurs chapitres d'algèbre linéaire).

Définition. Soit $(A,+,\times)$ un anneau. On appelle **diviseur de zéro** un élément a de A tel que :

$$1)\ a\neq 0_A \qquad 2)\ \exists\, b\in A,\ b\neq 0_A,\ a\times b=0_A$$

Exemples :

1/ Dans $(\mathbb{Z},+,\times)$, $(\mathbb{D},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{K}[X],+,\times)$ il n'existe pas de diviseur de zéro (c'est pourquoi vous avez pu appliquer jusqu'ici la règle : "un produit de facteurs est nul SSI l'un au moins de ses facteurs est nul").

2/ Dans $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$, la suite de terme général $1+(-1)^n$ est un diviseur de zéro.

3/ Dans $\left(\mathrm{M}_2(\mathbb{R}),+,\times\right)$, la matrice $A=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ est un diviseur de zéro.

4/ Dans $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+,\times\right)$, la fonction f nulle sur $\mathbb{R}_-$ et égale à l'identité sur $\mathbb{R}_+$ est un diviseur de zéro.

Définition. Un anneau $(A,+,\times)$ est **intègre** s'il ne contient aucun diviseur de zéro.

Exemples :

1/ $(\mathbb{Z},+,\times)$, $(\mathbb{D},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{K}[X],+,\times)$ sont des anneaux intègres.

2/ Les anneaux $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$, $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$, $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+,\times\right)$, $\left(\mathrm{M}_2(\mathbb{R}),+,\times\right)$ ne sont pas intègres.

Définition. Soit $(A,+,\times)$ un anneau. On appelle **élément nilpotent** un élément a de A tel que :

$$\exists\, n\in\mathbb{N}^*,\ a^n=0_A$$

Exemples :

1/ Dans $(\mathbb{Z},+,\times)$, $(\mathbb{D},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{K}[X],+,\times)$, 0 est l'unique diviseur de 0.

2/ Dans $\mathrm{M}_2(\mathbb{R})$, la matrice $A=\begin{pmatrix}0&2\\0&0\end{pmatrix}$ est nilpotente (un calcul rapide permet de se convaincre que $A^2=0_{\mathrm{M}_2(\mathbb{R})}$).

3/ Dans $\mathrm{M}_3(\mathbb{R})$, la matrice $A=\begin{pmatrix}0&2&1\\0&0&4\\0&0&0\end{pmatrix}$ est nilpotente (un calcul un peu moins rapide permet de se convaincre que $A^3=0_{\mathrm{M}_3(\mathbb{R})}$).

Remarques. Les éléments nilpotents possèdent les propriétés suivantes, dont les démos sont des petits exercices d'application de la définition.

1/ Dans un anneau intègre, 0 est l'unique élément nilpotent.

2/ Si a et b sont nilpotents, et commutent (càd sont tels que $ab = ba$), alors $(a+b)$ et $(a \times b)$ sont nilpotents.

Propriété. Si a est nilpotent, alors $(1-a)$ est inversible.

Exemple d'application. La matrice $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$ est nilpotente (car $A^3 = 0_{\mathrm{M}_3(\mathbb{R})}$).

On déduit alors de la propriété ci-dessus que la matrice : $\mathrm{I}_3 - A = \begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{pmatrix}$ est inversible, et que $(\mathrm{I}_3 - A)^{-1} = \mathrm{I}_3 + A + A^2$.

3.4. Courte présentation des corps.

Propriété. Soit $(A, +, \times)$ un anneau *(non nul)*. On note A^* l'ensemble des éléments inversibles de A.
Alors : $(A^*, \times)$ est un groupe. En outre, c'est un groupe abélien dès que A est commutatif.

Exemples :

1/ $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$; $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$; $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$.

2/ $\mathbb{Z}^* = \{1, -1\}$; ainsi $\mathbb{Z}^* \subsetneq \mathbb{Z}\setminus\{0\}$

3/ $\mathbb{K}[X]^* = \mathbb{K}^*$; ainsi $\mathbb{K}[X]^* \subsetneq \mathbb{K}[X]\setminus\{0\}$

4/ $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R})\right)^*$ est l'ensemble des fonctions continues sur $\mathbb{R}$ qui ne s'annulent pas. Ainsi : $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R})\right)^* \subsetneq \left(\mathscr{C}^0(\mathbb{R},\mathbb{R})\right)\setminus\{0\}$

5/ $\mathrm{M}_2(\mathbb{R})^* = \mathrm{GL}_2(\mathbb{R})$; ainsi $\mathrm{M}_2(\mathbb{R})^* \subsetneq \mathrm{M}_2(\mathbb{R})\setminus\{0\}$

6/ $\mathbb{Q}[\mathrm{i}]^* = \mathbb{Q}[\mathrm{i}]\setminus\{0\}$; $\mathbb{Q}\left[\sqrt{2}\right]^* = \mathbb{Q}[\sqrt{2}]\setminus\{0\}$.

7/ $\mathbb{Z}[\mathrm{i}]^* = \{\pm 1; \pm \mathrm{i}\}$; ainsi $\mathbb{Z}[\mathrm{i}]^* \subsetneq \mathbb{Z}[\mathrm{i}]\setminus\{0\}$

Définition. Un anneau commutatif $(A, +, \times)$ est un **corps** si $A^* = A\setminus\{0_A\}$.
Il revient au même dire qu'un corps est un anneau commutatif *(non nul)* où tout élément non nul est inversible.

Exemples. Grâce aux exemples précédents, on peut affirmer que :

1/ $\mathbb{R}$ est un corps (le corps des réels) ; $\mathbb{C}$ est un corps (le corps des complexes) ; $\mathbb{Q}$ est un corps (le corps des rationnels).

2/ L'anneau des entiers $\mathbb{Z}$ n'est pas un corps.

3/ L'anneau des entiers de Gauss $\mathbb{Z}[\mathrm{i}]$ n'est pas un corps.

4/ L'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ n'est pas un corps.

5/ L'anneau $\mathscr{C}^0(\mathbb{R},\mathbb{R})$ des fonctions continues sur $\mathbb{R}$ et à valeurs réelles n'est pas un corps.

6/ L'anneau $\mathbb{C}^{\mathbb{N}}$ des suites complexes n'est pas un corps.

7/ L'anneau $\mathrm{M}_2(\mathbb{R})$ n'est pas un corps.

4. Synthèse - A savoir, à savoir faire

En résumé, voici la liste des connaissances et des savoir-faire à acquérir dans la première partie ce chapitre :

- Connaître TOUS les énoncés du chapitre présentés dans ce résumé.
- Bien avoir compris les exemples de groupes et d'anneaux présentés, et être capable d'en citer une majorité.
- Savoir montrer que "quelquechose" est un groupe, en prouvant que c'est un sous-groupe d'un groupe usuel.
- Connaître les propriétés spécifiques à l'anneau des matrices carrées $\mathrm{M}_2(\mathbb{R})$: l'anneau $\mathrm{M}_2(\mathbb{R})$ n'est ni commutatif, ni intègre, il possède des éléments nilpotents, on peut y utiliser la formule du binôme de Newton (avec l'hypothèse de commutativité).
- Bien avoir compris l'exemple-clef du groupe S_3 (qui sera au cœur du chapitre consacré aux ensembles finis, et qui permettra en fin d'année de définir la notion de déterminant).