

Structure de groupe et exemples fondamentaux

1. Notions de base sur les groupes

1.1 Définition et notations (Mpsi)

Définition.— On appelle groupe tout couple (G, \otimes) où G est un ensemble et \otimes une loi de composition interne sur G tels que :

(G_1) : La loi \otimes est associative.

(G_2) : Le magma (G, \otimes) admet un élément neutre.

(G_3) : Tout élément x de G est symétrisable dans (G, \otimes) .

Si de plus \otimes est commutative alors le groupe (G, \otimes) est dit commutatif ou encore abélien.

Remarques

- ✓ Un groupe est un monoïde dans lequel tout élément est inversible.
- ✓ Dans un groupe (G, \otimes) , l'objet le plus important c'est la loi de composition interne \otimes . Néanmoins, dans les questions d'ordre théorique, le groupe (G, \otimes) est souvent désigné par G , la loi \otimes étant sous entendue. Dans un groupe G il y a toujours au moins un élément à savoir l'élément neutre. Un groupe G n'est donc jamais vide.
- ✓ Par analogie avec les notations utilisées dans les ensembles de nombres pour l'addition et la multiplication, la loi d'un groupe est la plupart du temps notée multiplicativement ou additivement.

Notation multiplicative

Pour $(x, y) \in G^2$ l'élément $x \otimes y$ de G est noté $x \times y$ ou plus simplement xy .

Si le groupe G n'est pas abélien, il se peut fort bien que l'on ait $xy \neq yx$.

L'élément neutre est noté 1_G . On a donc : $\forall x \in G, x1_G = 1_G x = x$.

Le symétrique de x est noté x^{-1} et est appelé inverse de x . On a donc :

$$\forall x \in G, x x^{-1} = x^{-1} x = 1_G.$$

Notation additive

Pour $(x, y) \in G^2$ l'élément $x \otimes y$ de G est noté $x + y$.

Si G n'est pas supposé abélien, il se peut fort bien que l'on ait $x + y \neq y + x$.

L'élément neutre est noté 0_G . On a donc : $\forall x \in G, x + 0_G = 0_G + x = x$.

Le symétrique de x est noté $-x$ et est appelé opposé de x .

On a donc : $\forall x \in G, x + (-x) = (-x) + x = 0_G$.

Enfin, étant donnés deux éléments x et y de G on pose par définition $x - y = x + (-y)$.

1.2 Règles de calculs dans un groupe (Mpsi)

Soit (G, \times) un groupe noté multiplicativement. Soient x_1, x_2, x_3 des éléments de G .

Par associativité : $x_1(x_2x_3) = (x_1x_2)x_3$. On désigne les éléments $x_1(x_2x_3)$ et $(x_1x_2)x_3$ par un même symbole à savoir $x_1x_2x_3$. Cette situation se généralise par récurrence au produit de n éléments de G avec $n \geq 3$. A titre d'exemple on a : $(x_1x_2)(x_3x_4) = x_1(x_2x_3x_4) = (x_1x_2x_3)x_4$. Ces trois éléments de G , qui sont égaux, sont tous désignés par le symbole $x_1x_2x_3x_4$.

Définissons maintenant la puissance $n^{\text{ème}}$ d'un élément du groupe multiplicatif G .

Considérons $x \in G$ et $n \in \mathbb{Z}$. Par définition on pose :

$$x^n = \underbrace{x \times \cdots \times x}_{x \text{ figurant } n \text{ fois}} \text{ si } n \geq 1, \quad x^n = \overbrace{x^{-1} \times \cdots \times x^{-1}}^{x^{-1} \text{ figurant } (-n) \text{ fois}} \text{ si } n \leq -1 \text{ et } x^0 = 1_G.$$

Proposition.— Soient (G, \times) un groupe, x, y deux éléments de G et p, q deux entiers relatifs.

- 1) $(xy)^{-1} = y^{-1}x^{-1}$, $x^p y^q = x^{p+q}$ et $(x^p)^q = x^{pq}$.
- 2) Si $xy = yx$ alors $(xy)^p = x^p y^p$.

Traduction en notation additive :

Soit $(G, +)$ un groupe noté additivement. Soient $x \in G$ et $n \in \mathbb{Z}$. Par définition on pose :

$$nx = \underbrace{x + \cdots + x}_{x \text{ figurant } n \text{ fois}} \text{ si } n \geq 1, \quad nx = \overbrace{(-x) + \cdots + (-x)}^{(-x) \text{ figurant } (-n) \text{ fois}} \text{ si } n \leq -1 \text{ et } 0x = 0_G.$$

Pour p, q dans \mathbb{Z} et x, y dans G on a les règles de calcul suivantes :

$$-(x+y) = (-y) + (-x), \quad (p+q)x = px + qx \text{ et } (pq)x = p(qx).$$

Si $x+y=y+x$ alors $p(x+y)=px+py$.

1.3 Sous-groupes

Soit (G, \times) un groupe noté multiplicativement.

Définition.— Une partie H de G est un sous-groupe de (G, \times) si et seulement si :

- 1) H est non vide.
- 2) H est stable par produit ie vérifie : $\forall (x, y) \in H^2, xy \in H$.
- 3) H est stable pour l'inverse ie vérifie : $\forall x \in H^2, x^{-1} \in H$.

Théorème. Soient H une partie de G .

- 1) Si H est un sous-groupe de (G, \times) alors $1_G \in H$.
- 2) H est un sous-groupe de (G, \times) si et seulement si $H \neq \emptyset$ et $\forall (x, y) \in H^2, xy^{-1} \in H$.

Remarques

- ✓ $\{1_G\}$ et G sont des sous-groupes de (G, \times) .
- ✓ Soit H un sous-groupe de (G, \times) . Comme H est stable pour la loi \times on peut considérer l'application $x_H : H \times H \rightarrow H$ définie par : $x \times_H y = x \times y$ pour tout $(x, y) \in H^2$. L'application x_H est une loi de composition interne sur H appelée loi induite par \times sur H . On vérifie que (H, \times_H) est un groupe.
- ✓ Il est bon de savoir traduire les notions qui viennent d'être introduites en notation additive.

Proposition. Une intersection de sous-groupes de (G, \times) est un sous-groupe de (G, \times) .

Remarque : Une réunion de sous-groupes n'est pas nécessairement un sous-groupe.

1.4 Morphismes de groupes

Définition. Soient (G, \otimes) , (G', \otimes') deux groupes et $f : G \rightarrow G'$ une application.

- 1) On dit que f est un morphisme de groupes de (G, \otimes) dans (G', \otimes') si et seulement si :
 $\forall (x, y) \in G^2, f(x \otimes y) = f(x) \otimes' f(y)$.
- 2) On dit que f est un isomorphisme de groupes de (G, \otimes) sur (G', \otimes') si et seulement si f est un morphisme de groupe de (G, \otimes) dans (G', \otimes') et f est bijective.
- 3) On dit que les groupes (G, \otimes) et (G', \otimes') sont isomorphes si et seulement si il existe un isomorphisme de (G, \otimes) sur (G', \otimes') .

Remarque : dans les questions d'ordre théorique, les lois de composition internes des groupes manipulés seront désormais toutes notées à l'aide de l'unique symbole \times . Les groupes (G, \otimes) et (G', \otimes') sont donc notés (G, \times) et (G', \times) . C'est abusif mais pratique.

Proposition. Soient (G, \times) , (G', \times) des groupes.

Soit f un morphisme de groupes de (G, \times) dans (G', \times) .

- 1) $f(1_G) = 1_{G'}$ et $\forall x \in G, f(x^{-1}) = f(x)^{-1}$.
- 2) $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = f(x)^n$.
- 3) Si H est un sous-groupe de (G, \times) alors $f(H)$ est un sous-groupe de (G', \times) .

4) Si H' est un sous-groupe de (G', \times) alors $f^{-1}(H')$ est un sous-groupe de (G, \times) .

Remarque : En notation additive, 2) et 3) s'écrivent : $f(-x) = -f(x)$ et $f(nx) = nf(x)$.

Définition. Soit $f : G \rightarrow G'$ un morphisme de groupes de (G, \times) dans (G', \times) .

L'ensemble $\text{Ker } f = \{x \in G, f(x) = 1_{G'}\}$ est appelé noyau du morphisme f .

L'ensemble $\text{Im } f = \{y \in G', \exists x \in G \mid y = f(x)\}$ est appelé image du morphisme f .

Proposition. Soit $f : G \rightarrow G'$ un morphisme de groupes de (G, \times) dans (G', \times) .

- 1) $\text{Ker } f$ est un sous-groupe de (G, \times) et $\text{Im } f$ est un sous-groupe de (G', \times) .
- 2) f est injective $\Leftrightarrow \text{Ker } f = \{1_G\}$ et f surjective $\Leftrightarrow \text{Im } f = G'$.
- 3) Si f est un isomorphisme de groupe alors f^{-1} est un isomorphisme de groupe.

1.5 Notion de groupe produit

Soient (G_1, \times) et (G_2, \times) deux groupes notés multiplicativement.

On définit sur le produit cartésien $G_1 \times G_2$ une loi de composition interne en posant par définition : $(x_1, x_2) \times (y_1, y_2) = (x_1 y_1, x_2 y_2)$ pour tout $(x_1, x_2), (y_1, y_2)$ dans $G_1 \times G_2$.

Proposition. $(G_1 \times G_2, \times)$ est un groupe d'élément neutre $(1_{G_1}, 1_{G_2})$.

Il est appelé groupe produit de (G_1, \times) et (G_2, \times) . L'inverse de $(x_1, x_2) \in G_1 \times G_2$ est (x_1^{-1}, x_2^{-1}) .

Si les groupes (G_1, \times) et (G_2, \times) sont commutatifs alors $(G_1 \times G_2, \times)$ l'est aussi.

Remarque : Si $(G_1, +)$ et $(G_2, +)$ sont deux groupes notés additivement alors la loi produit est aussi notée additivement ce qui s'écrit $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ pour $(x_1, x_2), (y_1, y_2)$ dans $G_1 \times G_2$.

Proposition. Soient (G_1, \times) et (G_2, \times) deux groupes notés multiplicativement.

On munit $G_1 \times G_2$ de sa structure de groupe produit.

- 1) Les applications $\pi_1 : G_1 \times G_2 \rightarrow G_1$ et $\pi_2 : G_1 \times G_2 \rightarrow G_2$ définies par $\pi_1(x_1, x_2) = x_1$ et $\pi_2(x_1, x_2) = x_2$ sont des morphismes surjectifs de groupes.
- 2) Les applications $\theta_1 : G_1 \rightarrow G_1 \times G_2$ et $\theta_2 : G_2 \rightarrow G_1 \times G_2$ définies par $\theta_1(x_1) = (x_1, 1_{G_2})$ et $\theta_2(x_2) = (1_{G_1}, x_2)$ sont des morphismes injectifs de groupes.
- 3) $\pi_1 \circ \theta_1 = \text{Id}_{G_1}$, $\pi_2 \circ \theta_2 = \text{Id}_{G_2}$ et $\forall x \in G_1 \times G_2, x = (\pi_1(x), \pi_2(x))$.

2. Groupes de nombres

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes mais pas $(\mathbb{N}, +)$.

$(\{-1, 1\}, \times)$, (\mathbb{Q}^*, \times) , $(\mathbb{Q}^{*+}, \times)$, (\mathbb{R}^*, \times) , $(\mathbb{R}^{*+}, \times)$, (\mathbb{C}^*, \times) sont des groupes mais pas (\mathbb{Z}^*, \times) .

Théorème.— (Sous-groupes de $(\mathbb{Z}, +)$)

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, n décrivant \mathbb{Z} . Plus précisément :

1) Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

2) Si H est un sous-groupe de $(\mathbb{Z}, +)$ alors : $\exists! n \in \mathbb{N}$, $H = n\mathbb{Z}$. Plus précisément :

Si $H = \{0\}$ alors $H = 0\mathbb{Z}$ et si $H \neq \{0\}$ alors $H = n\mathbb{Z}$ avec $n = \min(H \cap \mathbb{R}^{*+})$.

Théorème.— (Sous-groupes des complexes de module 1 et des racines $n^{\text{ièmes}}$ de l'unité)

On note U l'ensemble des nombres complexes de module 1 et pour $n \geq 1$ on désigne par U_n

l'ensemble des racines $n^{\text{ième}}$ de l'unité. $U = \{z \in \mathbb{C}, |z| = 1\}$ et $U_n = \{z \in \mathbb{C}, z^n = 1\}$.

1) U est un sous-groupe de (\mathbb{C}^*, \times) .

2) U_n est un sous-groupe fini de cardinal n de (\mathbb{C}^*, \times) . Plus précisément : si $\omega_n = e^{i\frac{2\pi}{n}}$ alors $1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ sont deux à deux distincts, $\omega_n^n = 1$ et on a $U_n = \{1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}\}$.

Proposition.— On considère $n \in \mathbb{N}^*$ et on pose $\omega_n = e^{i\frac{2\pi}{n}}$.

1) Si ξ est complexe de module 1 alors $|\xi| = 1$ puis $\bar{\xi} = \frac{1}{\xi}$. Pour tout $k \in \mathbb{Z}$ on a : $\overline{\omega_n^k} = \omega_n^{n-k}$.

2) Pour $n \geq 2$ la somme des racines $n^{\text{ièmes}}$ de l'unité vaut 0.

3) Si $n = 2p$ alors les racines $n^{\text{ièmes}}$ de l'unité sont : $1, \omega_n, \omega_n^2, \dots, \omega_n^{p-1}, -1, \overline{\omega_n^{p-1}}, \dots, \overline{\omega_n^2}, \overline{\omega_n}$.

Si $n = 2p + 1$ alors les racines $n^{\text{ièmes}}$ de l'unité sont : $1, \omega_n, \omega_n^2, \dots, \omega_n^p, \overline{\omega_n^p}, \dots, \overline{\omega_n^2}, \overline{\omega_n}$.

Proposition.— $U_2 = \{-1, 1\}$, $U_3 = \{1, j, j^2\}$ avec $j = e^{i\frac{2\pi}{3}}$ et $U_4 = \{1, -1, i, -i\}$.

D'autre part : $j^3 = 1$, $1 + j + j^2 = 0$ et $\bar{j} = j^2$.

Remarque : On dit qu'un complexe z est une racine de l'unité si et seulement si il existe $n \in \mathbb{N}^*$ tel que z soit une racine $n^{\text{ième}}$ de l'unité. L'ensemble des racines de l'unité est donc égal à $\bigcup_{n \in \mathbb{N}^*} U_n$.

Il est à noter que $\bigcup_{n \in \mathbb{N}^*} U_n$ est un sous-groupe de (U, \times) .

Exemples importants de morphismes de groupes

- ✓ L'exponentielle complexe est un morphisme de groupes de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \times) .
- ✓ L'exponentielle réelle est un isomorphisme de groupes de $(\mathbb{R}, +)$ dans $(]0, +\infty[, \times)$.
- ✓ Le logarithme népérien est un isomorphisme de groupes de $(]0, +\infty[, \times)$ dans $(\mathbb{R}, +)$.

3. Le groupe $(\mathbb{Z} / n\mathbb{Z}, +)$

Dans tout le paragraphe n désigne un entier naturel non nul.

Etant donnés deux entiers relatifs a et b on dit que a est congru à b modulo n si et seulement si $a - b \in n\mathbb{Z}$. Pour exprimer cela on note $a \equiv b \pmod{n}$.

La relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} qui est compatible avec l'addition et la multiplication. La classe de $a \in \mathbb{Z}$ pour la relation de congruence modulo n est égal à $a + n\mathbb{Z}$. Elle est noté \bar{a} . Il s'agit d'une partie de \mathbb{Z} .

Proposition.— Pour $(a, b) \in \mathbb{Z}^2$ on a : $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z}$.

Définition.— L'ensemble des parties de \mathbb{Z} de la forme \bar{a} , a décrivant \mathbb{Z} est noté $\mathbb{Z} / n\mathbb{Z}$.

On a donc : $\mathbb{Z} / n\mathbb{Z} = \{\bar{a}, a \in \mathbb{Z}\} = \{x \in \mathcal{P}(\mathbb{Z}), \exists a \in \mathbb{Z} \mid x = \bar{a}\}$.

Remarque : Soit x un élément de $\mathbb{Z} / n\mathbb{Z}$. Par définition, x est une partie de \mathbb{Z} et il existe au moins un entier relatif a tel que $x = \bar{a}$. Un tel entier relatif a est appelé représentant de x et il est bon de noter qu'il n'est pas unique. Les représentants de x sont en fait ses éléments. Il y en a donc une infinité et si a est l'un d'entre eux alors les autres sont les $a + nk$, k décrivant \mathbb{Z} .

Théorème.

- 1) Pour tout $a \in \mathbb{Z}$ on a $\bar{a} = \bar{r}$ où r est le reste de la division euclidienne de a par n .
- 2) $\mathbb{Z} / n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ et les éléments $\bar{0}, \bar{1}, \dots, \bar{n-1}$ sont deux à deux distincts.
- 3) $\mathbb{Z} / n\mathbb{Z}$ est un ensemble fini de cardinal n .

Soient x et y dans $\mathbb{Z} / n\mathbb{Z}$. Par définition il existe $(a, b) \in \mathbb{Z}^2$ tel que $x = \bar{a}$ et $y = \bar{b}$.

On pose : $x \oplus y = \bar{a} + \bar{b}$. Une telle définition semble dépendre du choix que l'on peut faire des représentants a et b de x et de y . En fait il n'en est rien et \oplus ainsi définie est une loi de composition interne sur $\mathbb{Z} / n\mathbb{Z}$. Pour des raisons de simplicité d'écriture la loi \oplus est notée $+$.

On retiendra que par définition même : $\forall (a, b) \in \mathbb{Z}^2, \bar{a} + \bar{b} = \bar{a+b}$.

Théorème.-

- 1) $(\mathbb{Z} / n\mathbb{Z}, +)$ est un groupe abélien fini de cardinal n et d'élément neutre $\bar{0}$.
- 2) Pour tout $a \in \mathbb{Z}$, l'inverse de \bar{a} dans $(\mathbb{Z} / n\mathbb{Z}, +)$ est égal à $\bar{-a}$ et on a donc $\bar{-a} = \overline{(-a)}$.
- 3) L'application $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z} / n\mathbb{Z}$ définie par $\pi_n(a) = \bar{a}$ est un morphisme surjectif de groupes de $(\mathbb{Z}, +)$ sur $(\mathbb{Z} / n\mathbb{Z}, +)$.

Proposition.- Le groupe $(\mathbb{Z} / n\mathbb{Z}, +)$ et le groupe (U_n, \times) sont isomorphes.

L'application $(\bar{k} \mapsto \omega_n^k)$ est un isomorphisme de groupes de $(\mathbb{Z} / n\mathbb{Z}, +)$ sur (U_n, \times) .

4. Groupe symétrique (Mpsi)

Etant donné un ensemble E , l'ensemble des bijections de E sur E est noté S_E .

Théorème.- (S_E, \circ) est un groupe. Il est appelé groupe symétrique de E .

Définition.- Un élément σ de S_E est appelée une permutation de E .

Si $\sigma \in S_E$ alors l'ensemble $\text{Supp } \sigma = \{x \in E \mid \sigma(x) \neq x\}$ est appelé support de σ .

Dans toute la suite on considère $n \in \mathbb{N}^*$ et on note S_n le groupe symétrique de $[1, n]$.

Théorème.- (S_n, \circ) est un groupe fini de cardinal $n!$.

Remarques

✓ Une permutation σ de S_n est notée $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

La permutation $\text{Id}_{[1,n]}$ est notée e . La composée $\sigma_1 \circ \sigma_2$ de permutations de S_n est notée $\sigma_1 \sigma_2$ et est appelée produit de σ_1 par σ_2 .

✓ (S_1, \circ) et (S_2, \circ) sont des groupes abéliens. Pour $n \geq 3$, (S_n, \circ) n'est pas commutatif.

Définition.- Soit $p \in [2, n]$.

On dit qu'une permutation γ de l'ensemble $[1, n]$ est un p-cycle si et seulement si il existe p entiers deux à deux distincts j_1, \dots, j_p de $[1, n]$ tels que : $\gamma(j_1) = j_2, \gamma(j_2) = j_3, \dots, \gamma(j_{p-1}) = j_p, \gamma(j_p) = j_1$ et $\forall k \in [1, n] \setminus \{j_1, \dots, j_p\}, \gamma(k) = k$. Pour un tel p-cycle γ on adopte la notation : $\gamma = (j_1, \dots, j_p)$. Un 2-cycle est appelé une transposition.

Proposition.- Soit $\gamma = (j_1, \dots, j_p)$ un p-cycle.

- 1) Le support de γ est égal à $\{j_1, \dots, j_p\}$ et on a : $\gamma = (j_1, j_2)(j_2, j_3) \cdots (j_{p-1}, j_p)$.
- 2) Les permutations $e, \gamma, \gamma^2, \dots, \gamma^{p-1}$ sont deux à deux distinctes et $\gamma^p = e$.
- 3) $\gamma^{-1} = (j_p, j_{p-1} \cdots, j_2, j_1)$ est un p-cycle.

Proposition.-

- 1) Deux p-cycles dont les supports sont disjoints commutent.
- 2) Si τ est une transposition alors $\tau^2 = e$ et $\tau^{-1} = \tau$.
- 3) Dans S_n il y a $\binom{n}{2}$ transpositions.

Remarque : Un produit de p-cycles n'est pas nécessairement un p-cycle.

Théorème.-

- 1) Si $n \geq 2$ alors toute permutation de $[1, n]$ distincte de l'identité peut s'écrire comme un produit de cycles à supports disjoints. Une telle écriture est unique à l'ordre près des facteurs.
- 2) Si $n \geq 2$ alors toute permutation de $[1, n]$ peut s'écrire comme un produit de transpositions.

Théorème-définition.- Il existe une unique application $\epsilon : S_n \rightarrow \{-1, 1\}$ vérifiant :

$\epsilon(\tau) = -1$ pour toute transposition τ de S_n et $\epsilon(\sigma_1 \circ \sigma_2) = \epsilon(\sigma_1)\epsilon(\sigma_2)$ pour tout $(\sigma_1, \sigma_2) \in S_n^2$.

Cette unique application ϵ est appelée signature.

C'est morphisme de groupe de (S_n, \circ) dans $(\{-1, 1\}, \times)$.

Définition.- Une permutation paire est une permutation de signature égale à 1.

Une permutation impaire est une permutation de signature égale à -1.

Proposition.- Un p-cycle de S_n est de signature $(-1)^{p-1}$. Une transposition de S_n est impaire.

5. Groupes de matrices

5.1 Groupe linéaire et spécial linéaire d'ordre n

$(M_n(\mathbb{K}), \times)$ est un monoïde d'élément neutre I_n où $I_n = \text{Diag}(1, \dots, 1)$.

On notera que $(M_n(\mathbb{K}), \times)$ n'est pas un groupe.

Définition.- Soit $A \in M_n(\mathbb{K})$.

- 1) La matrice A est dite inversible si et seulement si elle est inversible dans le magma $(M_n(\mathbb{K}), \times)$ c'est-à-dire si il existe $B \in M_n(\mathbb{K})$ telle que $AB = BA = I_n$. En cas d'existence l'inverse de A dans $(M_n(\mathbb{K}), \times)$ est noté A^{-1} .
L'ensemble des matrices inversibles de $M_n(\mathbb{K})$ est noté $GL_n(\mathbb{K})$.
- 2) La matrice A est dite inversible à droitessi il existe $B \in M_n(\mathbb{K})$ telle que $AB = I_n$. La matrice A est dite inversible à gauchessi il existe $B \in M_n(\mathbb{K})$ telle que $BA = I_n$.

Théorème (Mpsi).- Soit $A \in M_n(\mathbb{K})$.

- 1) A est inversible $\Leftrightarrow A$ est inversible à droite $\Leftrightarrow A$ est inversible à gauche.
- 2) A est inversible $\Leftrightarrow \det A \neq 0 \Leftrightarrow \text{rg } A = n \Leftrightarrow \text{Ker } A = \{0_{M_{n,n}(\mathbb{K})}\}$.

En particulier on a : $GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid \det A \neq 0\}$.

Définition.- On pose : $SL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid \det A = 1\}$.

Proposition.- (Groupe linéaire et spécial linéaire d'ordre n)

- 1) $(GL_n(\mathbb{K}), \times)$ est un groupe. Il est appelé groupe linéaire d'ordre n .
- 2) $(SL_n(\mathbb{K}), \times)$ est un groupe et est appelé groupe spécial linéaire d'ordre n .

5.2 Groupe orthogonal et spécial orthogonal d'ordre n

Définition.- $A \in M_n(\mathbb{R})$ est une matrice orthogonale si et seulement si ${}^tAA = I_n$.

L'ensemble des matrices orthogonales de $M_n(\mathbb{R})$ est noté $O_n(\mathbb{R})$.

On a donc : $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid {}^tAA = I_n\}$.

Proposition.-

- 1) Le déterminant d'une matrice orthogonale vaut 1 ou -1.
- 2) Toute matrice orthogonale est inversible et a pour inverse sa transposée.

Définition.- Une matrice orthogonale de déterminant égal à 1 (resp -1) est dite positive (resp négative). L'ensemble des matrices orthogonales positives est noté $SO_n(\mathbb{R})$.

Par définition même on a donc : $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det A = 1\}$.

Proposition.- (Groupe orthogonal et spécial orthogonal d'ordre n)

- 1) $(O_n(\mathbb{R}), \times)$ est un groupe. Il est appelé groupe orthogonal d'ordre n .
- 2) $(SO_n(\mathbb{R}), \times)$ est un groupe. Il est appelé groupe spécial orthogonal d'ordre n .

Proposition (Mpsi).- Soit $A \in M_n(\mathbb{R})$.

On munit \mathbb{R}^n de son produit scalaire usuel, celui qui rend la base canonique orthonormale.

On note (C_1, \dots, C_n) la famille des vecteurs colonnes de A et (L_1, \dots, L_n) celle des vecteurs lignes de A . Les assertions suivantes sont équivalentes :

- 1) $A \in O_n(\mathbb{R})$.
- 2) (C_1, \dots, C_n) est une famille orthonormale de \mathbb{R}^n .
- 3) (L_1, \dots, L_n) est une famille orthonormale de \mathbb{R}^n .

6. Groupes d'endomorphismes

Soit E un \mathbb{K} -espace vectoriel de dimension finie $n \geq 1$.

On note $L(E)$ l'ensemble des endomorphismes de E .

$(L(E), \circ)$ est un monoïde d'élément neutre Id_E mais ce n'est pas un groupe.

Si $u \in L(E)$ et si B est une base de E alors la matrice de u dans la base B est notée $M_B(u)$.

6.1 Groupe linéaire et spécial linéaire

Définition.- Un automorphisme de E est endomorphisme bijectif de E .

On note $GL(E)$ l'ensemble des automorphismes de E .

On pose : $SL(E) = \{u \in L(E) \mid \det u = 1\}$.

Proposition (Mpsi).- Soit E un \mathbb{K} -espace vectoriel de dimension finie $n \geq 1$.

On considère un endomorphisme u de E et une base B de E .

$u \in GL(E) \Leftrightarrow M_B(u) \in GL_n(\mathbb{K})$ et $u \in SL(E) \Leftrightarrow M_B(u) \in SL_n(\mathbb{K})$.

Proposition.- Soit E un \mathbb{K} -espace vectoriel de dimension finie $n \geq 1$.

- 1) $(GL(E), \circ)$ est un groupe, est appelé groupe linéaire de E et est isomorphe à $(GL_n(\mathbb{K}), \times)$.
- 2) $(SL(E), \circ)$ est un groupe, est appelé groupe spécial linéaire de E et est isomorphe à $(SL_n(\mathbb{K}), \times)$.

6.2 Groupe orthogonal et spécial orthogonal

Soit $(E, (\cdot | \cdot))$ un espace euclidien de dimension $n \geq 1$.

La norme associée au produit scalaire $(\cdot | \cdot)$ est notée $\| \cdot \|$.

On rappelle que pour tout $x \in E$ on a : $\|x\| = \sqrt{(x | x)}$.

Définition.— Soit $f : E \rightarrow E$ une application.

On dit que f conserve le produit scalaire si et seulement si : $\forall (x,y) \in E^2, (f(x)|f(y)) = (x|y)$.

On dit que f conserve la norme si et seulement si : $\forall x \in E, \|f(x)\| = \|x\|$.

Définition.— Une isométrie vectorielle de E est un endomorphisme de E qui conserve la norme.

Un automorphisme orthogonal de E est un automorphisme de E qui conserve le produit scalaire.

Une rotation est un automorphisme orthogonal de déterminant égal à 1.

On note $O(E)$ l'ensemble des automorphismes orthogonaux

On note $SO(E)$ l'ensemble des rotations de E .

Par définition même on a donc : $SO(E) = \{u \in O(E) \mid \det u = 1\}$.

Théorème.— Soit $u : E \rightarrow E$ une application (On notera que u n'est pas supposée linéaire).

Les assertions suivantes sont équivalentes :

- 1) L'application u est une isométrie vectorielle.
- 2) L'application u est un automorphisme orthogonal.
- 3) L'application u conserve le produit scalaire.
- 4) u est linéaire et l'image par u d'une base orthonormale de E est une base orthonormale de E .

Proposition (Mpsi).— Soit $(E, (\cdot|\cdot))$ un espace euclidien de dimension $n \geq 1$.

On considère un endomorphisme u de E et une base orthonormale B de E .

- 1) $u \in O(E) \Leftrightarrow M_B(u) \in O_n(\mathbb{R})$.
- 2) $u \in SO(E) \Leftrightarrow M_B(u) \in SO_n(\mathbb{R})$.
- 3) Si u est un automorphisme orthogonal alors le déterminant de u vaut 1 ou -1.

Proposition.— Soit $(E, (\cdot|\cdot))$ un espace euclidien de dimension $n \geq 1$.

- 1) $(O(E), \circ)$ est un groupe, est appelé groupe orthogonal de E et est isomorphe à $(O_n(\mathbb{R}), \times)$.
- 2) $(SO(E), \circ)$ est un groupe, est appelé groupe spécial orthogonal de E et est isomorphe à $(SO_n(\mathbb{R}), \times)$.

Proposition (Mpsi).— Soit $(E, (\cdot|\cdot))$ un espace euclidien de dimension 2.

Pour tout réel $\theta \in \mathbb{R}$ on pose $R(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$.

$$1) \forall (\theta, \theta') \in \mathbb{R}^2, R(\theta + \theta') = R(\theta) + R(\theta').$$

$$2) \forall \theta \in \mathbb{R}, R(\theta) \in SO_2(\mathbb{R}) \text{ et } R(\theta)^{-1} = R(-\theta).$$

$$3) SO_2(\mathbb{R}) = \{R(\theta), \theta \in \mathbb{R}\}.$$

4) L'application R est un morphisme de groupe surjectif de $(\mathbb{R}, +)$ sur $(SO_2(\mathbb{R}), \times)$.

7. Pour aller plus loin (HP)

7.1 Sous-groupes, morphismes de groupes

Proposition — Soient H et K deux sous-groupes de (G, \times) .

$H \cup K$ est un sous-groupe de (G, \times) si et seulement si $H \subset K$ ou $K \subset H$.

Théorème — (Sous groupes de $(\mathbb{R}, +)$)

Si H est un sous-groupe de $(\mathbb{R}, +)$ alors ou bien H est dense dans \mathbb{R} ou bien il existe un unique $a \in \mathbb{R}^+$ tel que $H = a\mathbb{Z}$. Plus précisément : si H est un sous-groupe de $(\mathbb{R}, +)$ non réduit au singleton $\{0\}$ et si $\alpha = \inf(H \cap \mathbb{R}^{*+})$ alors H est dense dans \mathbb{R} si $\alpha = 0$ et $H = \alpha\mathbb{Z}$ si $\alpha > 0$.

Proposition — Soit $f : G \rightarrow G'$ un morphisme de groupes de (G, \times) dans (G', \times) .

Si l'ensemble G est fini alors $\text{Ker } f$ et $\text{Im } f$ sont finis et on a : $|G| = |\text{Ker } f| \times |\text{Im } f|$.

7.2 Groupe symétrique

Soit $n \in \mathbb{N}^*$. (S_n, \circ) est un groupe fini de cardinal $n!$.

La signature ε est un morphisme de groupe de (S_n, \circ) dans $(\{-1, 1\}, \times)$.

On note A_n l'ensemble des permutations paires.

Par définition même on a donc : $A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$.

Théorème — Pour $n \geq 2$, (A_n, \circ) est un groupe de cardinal $\frac{n!}{2}$.

Il est appelé groupe alterné de $[1, n]$.

Théorème — Soit $n \in \mathbb{N}$.

1) Si j_1, \dots, j_p sont des entiers deux à deux distincts de $[1, n]$ et si $\sigma \in S_n$ alors on a la formule :

$$\sigma(j_1, \dots, j_p)\sigma^{-1} = (\sigma(j_1), \dots, \sigma(j_p)).$$

2) Si i, j sont des entiers distincts de $[1, n]$ alors on a $(i, j) = (1, i)(1, j)(1, i)$.

3) On pose : $T_n = \{(1, i), 2 \leq i \leq n\}$. Si $n \geq 2$ alors toute permutation de S_n peut s'écrire comme un produit d'éléments de T_n .

Théorème.- (Générateurs du groupe spécial linéaire)

Toute matrice A de $SL_n(\mathbb{K})$ peut s'écrire comme un produit de matrices élémentaires de transvection.

En particulier : $SL_n(\mathbb{K}) = \langle T \rangle$ où T est l'ensemble constitué des matrices élémentaires de transvection.

Niels Abel (1802-1829)

Né à Finnoy, une île norvégienne, c'est à l'âge de treize ans qu'Abel se découvre une passion pour les mathématiques. Son professeur de mathématiques, Holmboe, reconnaît son talent au point qu'il inscrit comme appréciation sur le bulletin d'Abel : "A l'excellence de son intelligence s'unit une passion et un intérêt insatiable pour la mathématique, si bien qu'à n'en pas douter, s'il lui est donné de vivre, il deviendra probablement un très grand mathématicien". Pour la petite histoire le principal de l'établissement avait demandé à Holmboe de modifier ses derniers mots qui à l'origine étaient : "le plus grand mathématicien du monde" Grâce à des fonds récoltés par Holmboe, Abel poursuit ses études à l'université d'Oslo. Il obtient une bourse et l'utilise pour voyager en France, en Italie et en Allemagne où il rencontre quelques grands mathématiciens de l'époque. Abel publie ses premières recherches et se fait ainsi connaître du monde scientifique. Il demande alors sans succès un poste d'enseignant et, sans argent, déjà affaibli par la tuberculose, il rentre en Norvège où il meurt à l'âge de vingt-sept ans. Deux jours plus tard arrive sa nomination à l'université de Berlin... Abel est l'un des initiateurs de la théorie des fonctions elliptiques et a fondé la théorie des intégrales abéliennes. On lui doit aussi de nombreux théorèmes d'analyse ainsi que la découverte d'équations algébriques résolubles par radicaux.

Joseph-Louis Lagrange (1736-1813)

Giuseppe Lodovico Lagrangia est né le 25 janvier 1736 à Turin, alors capitale du royaume de Sardaigne. Il est pourtant considéré comme un mathématicien français et non italien, ceci de sa propre volonté (la branche paternelle de sa famille étant française). Lagrange étudia brillamment à l'université de sa ville natale; son intérêt pour les mathématiques ne se manifeste que vers 17 ans, à la lecture d'un mémoire de Halley sur l'utilisation de l'algèbre en optique. Il se plonge alors aussitôt, seul et sans aide, dans l'étude des mathématiques. Très rapidement, il obtient des résultats probants. A la fin de l'année 1755, Lagrange devient professeur à l'école d'artillerie de Turin., ville où il fonde en 1757 une académie des sciences. Son talent est très vite reconnu, et il écrit durant ses premières années de brillants mémoires où il applique les méthodes du calcul des variations à la mécanique. En 1764 notamment, Lagrange gagne le Grand Prix de l'Académie des Sciences de Paris. Il le regagnera 1772, 1774 et 1780. En 1766, grâce à l'appui de D'Alembert, Lagrange succède à Euler au poste prestigieux de directeur des mathématiques à l'Académie des Sciences de Berlin. Il passera 20 ans là-bas. Il publie avec une régularité impressionnante des mémoires qui touchent tous les domaines des mathématiques et de la mécanique : astronomie, probabilités, théorie des équations algébriques Les dernières années à Berlin sont consacrées à l'étude du monumental Traité de Mécanique Analytique, où il reprend, complète et unifie les connaissances accumulées depuis Newton. Ce livre, qui devient pour tous ses contemporains une référence, se veut notamment une apologie de l'utilisation des équations différentielles en mécanique.

En 1787, Lagrange part pour la France où il devient membre de l'Académie des Sciences de Paris. Il est un des rares à traverser la Révolution sans être inquiété: il est même Président de la Commission des poids et des mesures, et est à ce titre un des pères du système métrique et de l'adoption de la division décimale des mesures.

Lagrange participe encore à la création de l'Ecole Polytechnique dont il est le premier professeur d'analyse. Il décède le 10 avril 1813, après avoir reçu de Napoléon Ier tous les honneurs de la nation française.

Structure d'anneau et de corps

1. Notions de base sur les anneaux (Mpsi)

1.1 Définition et notations

Définition.— On appelle anneau tout triplet $(A, +, \times)$ où A est un ensemble, $+$ et \times des lois de composition internes tels que :

(A_1) $(A, +)$ est un groupe abélien.

(A_2) (A, \times) est un monoïde.

(A_3) \times est distributive par rapport à $+$.

Si de plus \times est commutative on dit que l'anneau $(A, +, \times)$ est commutatif.

Notations adoptées dans un anneau

Soit $(A, +, \times)$ un anneau.

L'élément neutre du groupe $(A, +)$ est noté 0_A . Par suite : $\forall a \in A, a + 0_A = a$.

L'élément neutre du monoïde (A, \times) est noté 1_A . Par suite : $\forall a \in A, a \times 1_A = a$.

$(A, +)$ étant un groupe tout élément a de A est symétrisable dans $(A, +)$. Le symétrique de a dans

$(A, +)$ est noté $-a$ et est appelé opposé de a dans A . On a donc : $\forall a \in A, a + (-a) = 0_A$.

Par contre un élément de A n'est pas nécessairement symétrisable dans (A, \times) .

C'est d'ailleurs la seule chose qui empêche (A, \times) d'être un groupe.

Définition.— On dit que $a \in A$ est inversible dans l'anneau $(A, +, \times)$ si et seulement si il est symétrisable dans le monoïde (A, \times) c'est-à-dire si et seulement si il existe $b \in A$ tel que $ab = ba = 1_A$. Dans ces conditions le symétrique de a dans (A, \times) est noté a^{-1} et est appelé inverse de a dans l'anneau $(A, +, \times)$.

On note A^\times l'ensemble des éléments inversibles de l'anneau $(A, +, \times)$.

Par définition même on a donc : $A^\times = \{a \in A, \exists b \in A \mid ab = ba = 1_A\}$.

Théorème.— Soit $(A, +, \times)$ un anneau.

(A^\times, \times) est un groupe et est appelé groupe des éléments inversibles de l'anneau $(A, +, \times)$.

Exemples fondamentaux

- $(\mathbb{Z}, +, \times)$ est un anneau commutatif et $\mathbb{Z}^\times = \{-1, 1\}$.
- Si D est un ensemble alors $(\mathbb{K}^D, +, \times)$ est un anneau commutatif et $(\mathbb{K}^D)^\times$ est égal à l'ensemble des applications de D dans \mathbb{K} qui ne s'annulent pas sur D .
- $(\mathbb{K}[X], +, \times)$ est un anneau commutatif et $\mathbb{K}[X]^\times$ est égal à l'ensemble des polynômes constants et non nuls. $\mathbb{K}[X]^\times$ est donc égal à l'ensemble des polynômes de degré zéro.
- $(M_n(\mathbb{K}), +, \times)$ est un anneau non commutatif et $M_n(\mathbb{K})^\times = GL_n(\mathbb{K})$.
- Si E est un \mathbb{K} -espace vectoriel alors $(L(E), +, \circ)$ est un anneau non commutatif et $L(E)^\times = GL(E)$.
- $(2\mathbb{Z}, +, \times)$ n'est pas un anneau.

1.2 Règles de calcul dans un anneau

Dans tout ce paragraphe, $(A, +, \times)$ est un anneau.

1) $(A, +)$ étant un groupe on peut définir le symbole nx pour $n \in \mathbb{Z}$ et $x \in A$.

$$nx = \underbrace{x + \cdots + x}_{x \text{ figurant } n \text{ fois}} \text{ si } n \geq 1, \quad nx = \underbrace{(-x) + \cdots + (-x)}_{x \text{ figurant } (-n) \text{ fois}} \text{ si } n \leq -1 \text{ et } 0x = 0_A. \text{ Dans ces conditions :}$$

$$px + qx = (p + q)x, \quad p(qx) = (pq)x, \quad px + py = p(x + y) \text{ pour } (x, y) \in A^2 \text{ et } (p, q) \in \mathbb{Z}^2.$$

2) La loi de composition \times étant associative on peut définir la puissance $n^{\text{ième}}$ de $x \in A$ pour $n \in \mathbb{N}$. $x^n = \underbrace{x \times \cdots \times x}_{x \text{ figurant } n \text{ fois}}$ si $n \geq 1$ et $x^0 = 1_A$. Dans ces conditions :

$$x^p x^q = x^{p+q} \text{ et } (x^p)^q = x^{pq} \text{ pour } x \in A \text{ et } (p, q) \in \mathbb{N}^2. \text{ Il est à noter que si l'anneau } (A, +, \times) \text{ n'est pas commutatif alors il se peut très bien que } (xy)^p \neq x^p y^p.$$

3) On suppose ici que $x \in A^\times$ c'est-à-dire que x est inversible dans A . On peut alors définir la puissance $n^{\text{ième}}$ de l'élément x pour n strictement négatif en posant : $x^n = (x^{-1})^{-n}$ si $n \leq -1$. Pour $x \in A^\times$ et pour $(p, q) \in \mathbb{Z}^2$ les règles $x^p x^q = x^{p+q}$ et $(x^p)^q = x^{pq}$ sont encore valables.

Proposition.— Soit $(A, +, \times)$ un anneau.

- 1) $\forall x \in A, 0_A x = x 0_A = 0_A$.
- 2) $\forall (x, y) \in A^2, x(-y) = (-x)y = -(xy)$.
- 3) $\forall (x, y) \in A^2, \forall n \in \mathbb{Z}, x(ny) = (nx)y = n(xy)$.
- 4) $\forall (x, y) \in A^2, (-x)(-y) = xy$.

Remarques

- ✓ Les règles 2 et 4 constituent ce que l'on appelle la règle des signes.
- ✓ Un anneau A est dit nul lorsque $0_A = 1_A$. Dans un tel anneau A il n'y a qu'un seul élément à savoir l'élément 0_A . Ce cas de figure est donc assez peu intéressant...
- ✓ $\forall x \in A, x(-1_A) = (-1_A)x = -x$ et $\forall x \in A, \forall n \in \mathbb{Z}, nx = (n1_A)x$.

1.3 Symbole somme dans un anneau

Pour $n \geq 1$ et $(a_1, \dots, a_n) \in A^n$ on pose par définition : $\sum_{k=1}^n a_k = a_1 + \dots + a_n$.

Propriétés

- 1) $\sum_{k=1}^n a_k + \sum_{k=1}^m b_k = \sum_{k=1}^n (a_k + b_k)$, $\sum_{k=1}^n aa_k = a \left(\sum_{k=1}^n a_k \right)$ et $\sum_{k=1}^n a_k a = \left(\sum_{k=1}^n a_k \right) a$.
- 2) $\sum_{k=1}^m \left(\sum_{l=1}^n a_{k,l} \right) = \sum_{l=1}^n \left(\sum_{k=1}^m a_{k,l} \right)$ Cette valeur commune est notée $\sum_{(k,l) \in [1,m] \times [1,n]} a_{k,l}$.
- 3) $\sum_{(k,l) \in [1,m] \times [1,n]} a_k b_l = \sum_{k=1}^m a_k \left(\sum_{l=1}^n b_l \right) = \sum_{l=1}^n \left(\sum_{k=1}^m a_k \right) b_l = \left(\sum_{k=1}^m a_k \right) \left(\sum_{l=1}^n b_l \right)$.

Théorème. Soient a, b des éléments de A et $n \in \mathbb{N}^*$.

- 1) Si $ab = ba$ alors $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$.
- 2) En particulier : $a^n - 1_A = (a - 1_A)(a^{n-1} + a^{n-2} + \dots + a + 1_A)$.

Théorème. (Binôme de Newton)

Soit $(a, b) \in A^2$. Si $ab = ba$ alors on a : $\forall n \in \mathbb{N}, (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$.

2. Sous-anneaux – morphismes d'anneaux

Définition. Soit $(A, +, \times)$ un anneau.

Une partie B de A est un sous-anneau de $(A, +, \times)$ si et seulement :

- 1) $\forall (x, y) \in B^2, x - y \in B$ (B est stable par différence).
- 2) $\forall (x, y) \in B^2, xy \in B$ (B est stable par produit).
- 3) $1_A \in B$.

Remarques

- ✓ Si B est un sous-anneau de $(A, +, \times)$ alors B est un sous-groupe de $(A, +)$.
- ✓ Si B est un sous-anneau de $(A, +, \times)$ alors d'après 1) et 2) $+$ et \times peuvent être considérées comme des lois de composition internes sur B et B muni de ces lois induites devient un anneau.

Exemple : Soit A un anneau non nul (on a donc $0_A \neq 1_A$). Le singleton $\{0_A\}$ n'est pas un sous-anneau de $(A, +, \times)$. Par contre A est toujours un sous-anneau de $(A, +, \times)$.

Définition. Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. Un morphisme d'anneaux de $(A, +, \times)$ dans $(B, +, \times)$ est une application $f : A \rightarrow B$ vérifiant les propriétés suivantes :

- 1) $\forall (x, y) \in A^2, f(x + y) = f(x) + f(y)$.
- 2) $\forall (x, y) \in A^2, f(xy) = f(x)f(y)$.
- 3) $f(1_A) = 1_B$.

Terminologie

- ✓ On dit que $f : A \rightarrow B$ est un isomorphisme d'anneaux de A sur B si et seulement si f est un morphisme d'anneaux de A dans B et si f est une bijection de A sur B .
- ✓ Deux anneaux $(A, +, \times)$ et $(B, +, \times)$ sont dits isomorphes si et seulement si il existe un isomorphisme d'anneaux de $(A, +, \times)$ sur $(B, +, \times)$.

Proposition. Si les anneaux $(A, +, \times)$ et $(B, +, \times)$ sont isomorphes alors les groupes (A^\times, \times) et (B^\times, \times) sont isomorphes.

Définition. Soit $f : A \rightarrow B$ un morphisme d'anneaux de $(A, +, \times)$ dans $(B, +, \times)$.

Par définition on pose : $\text{Ker } f = \{a \in A \mid f(a) = 0_B\}$ et $\text{Im } f = \{b \in B, \exists a \in A \mid b = f(a)\}$.

Les ensembles $\text{Ker } f$ et $\text{Im } f$ sont respectivement appelés noyau et image de f .

3. Intégrité, notion d'anneau produit

3.1 Anneau intègre

Définition. Un anneau $(A, +, \times)$ est dit sans diviseurs de zéro si et seulement si il vérifie la propriété : $\forall (a, b) \in A^2, ab = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.

Un anneau intègre est un anneau commutatif non nul et sans diviseurs de zéro.

Remarque : Dire que l'anneau $(A, +, \times)$ admet des diviseurs de zéro signifie qu'il existe au moins un couple $(a, b) \in A^2$ vérifiant : $ab = 0_A$ et $a \neq 0_A$ et $b \neq 0_A$.

Exemples

- ✓ $(\mathbb{Z}, +, \times)$ et $(\mathbb{K}[X], +, \times)$ sont des anneaux intègres.
- ✓ $(\mathbb{K}^D, +, \times)$ est un anneau commutatif non nul non intègre.
- ✓ $(M_n(\mathbb{K}), +, \times)$ pour $n \geq 2$ et $(L(E), +, \circ)$ lorsque $\dim E \geq 2$, sont des anneaux non nuls, non commutatifs et admettant des diviseurs de zéro donc non intègres.

3.2 Anneau produit

Soient $(A_1, +, \times)$ et $(A_2, +, \times)$ deux anneaux.

On définit sur le produit cartésien $A_1 \times A_2$ deux lois de composition internes $+$ et \times en posant :

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \text{ et } (a_1, a_2) \times (b_1, b_2) = (a_1 \times b_1, a_2 \times b_2). \quad (*)$$

Proposition.— $(A_1 \times A_2, +, \times)$ est un anneau.

- 1) $0_{A_1 \times A_2} = (0_{A_1}, 0_{A_2})$ et $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$.
- 2) L'opposé de $(a_1, a_2) \in A_1 \times A_2$ alias $-(a_1, a_2)$ est égal à $(-a_1, -a_2)$.
- 3) $(a_1, a_2) \in A_1 \times A_2$ est inversible dans $A_1 \times A_2$ si et seulement si a_1 est inversible dans A_1 et a_2 est inversible dans A_2 et dans ces conditions : $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. On a :
$$(A_1 \times A_2)^\times = A_1^\times \times A_2^\times.$$
- 4) Si les anneaux $(A_1, +, \times)$ et $(A_2, +, \times)$ sont commutatifs alors $(A_1 \times A_2, +, \times)$ l'est aussi.
- 5) Si les anneaux $(A_1, +, \times)$ et $(A_2, +, \times)$ sont tous deux non nuls alors l'anneau $(A_1 \times A_2, +, \times)$ possède des diviseurs de zéro et est donc non intègre.

Remarque : Lorsque l'on munit l'ensemble $A_1 \times A_2$ des lois $+$ et \times définies par les formules $(*)$ on dit que l'on munit $A_1 \times A_2$ de sa structure d'anneau produit. Le fait que les anneaux $(A_1, +, \times)$ et $(A_2, +, \times)$ soient intègres n'entraîne absolument pas que l'anneau $(A_1 \times A_2, +, \times)$ le soit à son tour.

4. Structure de corps

4.1 Corps, sous corps, morphisme de corps

Définition.— Un corps est un anneau commutatif non nul dans lequel tout élément non nul est inversible.

Proposition.— Si $(K, +, \times)$ est un corps alors $(K, +)$ est un groupe abélien, $(K \setminus \{0_K\}, \times)$ est un groupe, $(K, +, \times)$ est un anneau intègre, $K^\times = K \setminus \{0_K\}$ et $1_K \neq 0_K$.

Exemples

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.
- $(\mathbb{Z}, +, \times)$ n'est pas un corps.

Définition.— Soit $(K, +, \times)$ un corps. Une partie L de K est un sous corps de $(K, +, \times)$ si et seulement si

- 1) $\forall (x, y) \in L^2$, $x - y \in L$ (L est stable par différence).
- 2) $\forall (x, y) \in L^2$, $xy \in L$ (L est stable par produit).
- 3) $\forall x \in L \setminus \{0_K\}$, $x^{-1} \in L$ (L est stable pour l'inverse).
- 4) $1_K \in L$.

Définition.— Soient $(K, +, \times)$ et $(K', +, \times)$ deux corps. Un morphisme de corps de $(K, +, \times)$ dans $(K', +, \times)$ est un morphisme d'anneaux de $(K, +, \times)$ dans $(K', +, \times)$.

Remarques

- ✓ Si L est un sous corps de $(K, +, \times)$ alors L muni des lois induites est un corps.
- ✓ L'avantage d'un morphisme de corps sur un morphisme d'anneaux, c'est que les ensembles de départ et d'arrivée ont plus de propriétés (ce sont des corps et pas seulement des anneaux).

4.2 Notation fractionnaire dans un corps

Soit $(K, +, \times)$ un corps. On considère $a \in K$ et $b \in K \setminus \{0_K\}$. b est non nul donc inversible et on peut parler de b^{-1} . La loi \times étant commutative on a : $ab^{-1} = b^{-1}a$. L'élément ab^{-1} est noté $\frac{a}{b}$.

Dès lors :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

$$\frac{1}{a} = a^{-1}.$$

Cela pour tout $(a, c) \in K^2$ et $(b, d) \in (K \setminus \{0_K\})^2$.

Théorème (HP).- (Corps des fractions d'un anneau intègre)

Etant donné un anneau intègre $(A, +, \times)$, il existe un unique corps $(K, +, \times)$ contenant A qui vérifie :

$$\forall x \in K, \exists a \in A, \exists b \in A \setminus \{0_A\} \mid x = \frac{a}{b}.$$

Le corps $(K, +, \times)$ est appelé corps des fractions de l'anneau intègre $(A, +, \times)$.

Exemples : $(\mathbb{Q}, +, \times)$ est le corps des fractions de $(\mathbb{Z}, +, \times)$.

$(K(X), +, \times)$ est le corps des fractions de $(K[X], +, \times)$.

4.3 Exemples d'espaces vectoriels obtenus à partir de corps commutatifs

Première situation

Soit $(K, +, \times)$ un corps. La loi \times est une loi de composition interne sur K c'est-à-dire une application de $K \times K \rightarrow K$. Elle peut donc être « vue » comme une loi de composition externe sur K à domaine d'opérateurs dans K. On vérifie alors que $(K, +, \times)$ est un K-espace vectoriel. Ce K-espace vectoriel est de dimension un ce qui s'écrit $\dim_K K = 1$.

Tout corps $(K, +, \times)$ peut être « vu » comme un K-espace vectoriel et que $\dim_K K = 1$.

Exemple : \mathbb{Q} est un \mathbb{Q} -espace vectoriel de dimension 1.

Seconde situation

Soit L un sous corps du corps $(K, +, \times)$. Pour $x \in K$ et $\lambda \in L$ on pose : $\lambda \cdot x = \lambda \times x$. L'application $\cdot : L \times K \rightarrow K$ ainsi définie est une loi de composition externe sur K à domaine d'opérateurs dans L. On vérifie que $(K, +, \cdot)$ est un L-espace vectoriel.

Si L est un sous corps du corps $(K, +, \times)$ alors K peut être « vu » comme un L-espace vectoriel.

Exemple : C est un C-espace vectoriel de dimension 1 et un \mathbb{R} -espace vectoriel de dimension 2.

5. Notion d'idéal dans un anneau commutatif

Soit $(A, +, \times)$ un anneau commutatif.

5.1 Définition et premières propriétés

Définition.- Une partie I de A est un idéal de l'anneau $(A, +, \times)$ si et seulement si :

- 1) I est un sous-groupe de $(A, +)$
- 2) $\forall a \in A, \forall i \in I, ai \in I$.

Proposition.-

1) Une partie I de A est un idéal de l'anneau $(A, +, \times)$ si et seulement si :

$$I \neq \emptyset \text{ et } \forall (a, b) \in A^2, \forall (i, j) \in I^2, ai + bj \in I.$$

2) Une intersection d'idéaux de $(A, +, \times)$ est un idéal de $(A, +, \times)$.

3) Si $a \in A$ alors $aA = \{ax \mid x \in A\}$ est le plus petit idéal de $(A, +, \times)$ qui contient a.

4) Si un idéal I de $(A, +, \times)$ contient 1_A alors $I = A$.

5) Si un idéal I de $(A, +, \times)$ contient un élément de A^\times alors $I = A$.

Proposition.- Soient $(A, +, \times)$ un anneau commutatif et $(B, +, \times)$ un anneau.

Si $\varphi : A \rightarrow B$ est un morphisme d'anneaux alors $\text{Ker } \varphi$ est un idéal de l'anneau $(A, +, \times)$.

Exemples

➤ $\{0_A\}$ et A sont des idéaux de l'anneau commutatif $(A, +, \times)$.

➤ Les seuls idéaux d'un corps $(K, +, \times)$ sont $\{0_K\}$ et K.

➤ Pour tout $a \in \mathbb{R}$, $I_a = \{f \in \mathbb{R}^\mathbb{R} \mid f(a) = 0\}$ est un idéal de l'anneau commutatif $(\mathbb{R}^\mathbb{R}, +, \times)$.

5.2 Idéaux de l'anneau des entiers relatifs

Théorème.- (Division euclidienne dans \mathbb{Z})

Si $(a, b) \in \mathbb{Z}^2$ et si $b \neq 0$ alors : $\exists! (q, r) \in \mathbb{Z}^2 \mid a = bq + r$ et $0 \leq r < |b|$.

Théorème.- (Idéaux de $(\mathbb{Z}, +, \times)$)

Les idéaux de l'anneau $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$, n décrivant \mathbb{Z} . Plus précisément :

- 1) Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.
- 2) Si I est un idéal de $(\mathbb{Z}, +, \times)$ alors : $\exists! n \in \mathbb{N} \mid I = n\mathbb{Z}$.

5.3 Idéaux de l'anneau des polynômes à une indéterminée

Soit $(K, +, \times)$ un corps.

Théorème.- (Division euclidienne dans $K[X]$)

Soient A, B des polynômes de $K[X]$ tels que $B \neq 0$.

$\exists! (Q, R) \in K[X]^2 \mid A = BQ + R$ et $\deg R < \deg B$.

Définition (HP).— On dit qu'un polynôme $P \in K[X]$ est normalisé si et seulement si ou bien P est nul ou bien P est unitaire.

Théorème.— (Idéaux de $(K[X], +, \times)$)

Les idéaux de l'anneau $(K[X], +, \times)$ sont les $PK[X]$, $P \in K[X]$. Plus précisément :

- 1) Pour tout $P \in K[X]$, $PK[X]$ est un idéal de $(K[X], +, \times)$.
- 2) Si I est un idéal de l'anneau $(K[X], +, \times)$ alors il existe un unique polynôme normalisé P de $K[X]$ tel que : $I = PK[X]$.

6. Pour aller plus loin (HP)

6.1 Notion d'élément nilpotent dans un anneau

Définition.— Soient $(A, +, \times)$ un anneau et $a \in A$.

On dit que a est nilpotent si et seulement si il existe $m \in \mathbb{N}^*$ tel que $a^m = 0_A$.

Proposition.— Soient $(A, +, \times)$ un anneau et $a \in A$.

- 1) 0_A est nilpotent. Si A est intègre alors 0_A est le seul élément nilpotent de A .
- 2) Si A est non nul alors les éléments inversibles de A ne sont pas nilpotents.
- 3) Si a est un élément nilpotent de A alors $p = \min\{k \in \mathbb{N}^* \mid a^k = 0_A\}$ existe et est appelé indice de nilpotence de a . Si $a = 0_A$ alors $p = 1$ et si $a \neq 0_A$ alors $p \geq 2$.
- 4) Si a est un élément nilpotent et non nul de A alors son indice de nilpotence p est supérieur ou égal à deux, $a^p = 0_A$ et $a^{p-1} \neq 0_A$.

Proposition.— Soient $(A, +, \times)$ un anneau et $(a, b) \in A^2$.

Si a et b sont nilpotents et si $ab = ba$ alors $a + b$ et ab sont nilpotents.

Proposition.— Soient $(A, +, \times)$ un anneau et a un élément nilpotent de A . Il existe donc $p \in \mathbb{N}^*$ tel que $a^p = 0_A$. L'élément $1_A - a$ est inversible et on a : $(1_A - a)^{-1} = 1_A + a + a^2 + \dots + a^{p-1}$.

6.2 Morphisme d'anneaux

Proposition.— Tout morphisme de corps est injectif.

Proposition.— Un anneau intègre fini est un corps.

6.3 Idéaux

Proposition.— Soient I et J des idéaux de l'anneau commutatif $(A, +, \times)$.

Les ensembles $I + J$, IJ et \sqrt{I} définis par

$$\begin{cases} I + J = \{x \in A, \exists i \in I, \exists j \in J, x = i + j\} \\ IJ = \left\{ x \in A, \exists n \in \mathbb{N}^*, \exists (i_1, \dots, i_n) \in I^n, \exists (j_1, \dots, j_n) \in J^n \mid x = \sum_{k=1}^n i_k j_k \right\} \\ \sqrt{I} = \{x \in A, \exists n \in \mathbb{N} \mid x^n \in I\} \end{cases}$$

sont des idéaux de l'anneau $(A, +, \times)$.

Définition.— Un anneau $(A, +, \times)$ est dit principal si et seulement si $(A, +, \times)$ est un anneau intègre dans lequel tout idéal est de la forme aA avec $a \in A$.

Proposition.— Soit $(A, +, \times)$ un anneau commutatif.

- 1) Si $(I_n)_{n \in \mathbb{N}}$ est une suite croissante d'idéaux de $(A, +, \times)$ alors $\bigcup_{n \in \mathbb{N}} I_n$ est un idéal de $(A, +, \times)$.
- 2) Si $(A, +, \times)$ est principal alors toute suite croissante d'idéaux de $(A, +, \times)$ est stationnaire.

Isaac Newton (1642-1727)

Né en Angleterre à Woolsthorpe Newton devient titulaire de la chaire de mathématiques de Cambridge en 1669. Son œuvre en physique est fondamentale. L'optique mais surtout la théorie de la gravitation vont faire sa réputation. C'est en 1687 que Newton publie un ouvrage, "Philosophiae naturalis principia mathematica" qui va définitivement marquer l'histoire de la science! Dans les "Principia" Il expose ses lois de la gravitation universelle qui deviennent la clé de voûte de la physique moderne au moins jusqu'en 1905 date à laquelle Einstein publie sa théorie de la relativité restreinte. En mathématique Newton est considéré avec Leibniz comme le fondateur du calcul différentiel et intégral. Il est notamment l'un des premiers à inventer une notation et des algorithmes généraux pour le calcul infinitésimal. Il est aussi le premier à avoir introduit le concept d'équation différentielle.

Gauss (1777-1855)

Carl Friedrich Gauss, né le 30 avril 1777 à Brunswick, est considéré par ses pairs comme le prince des mathématiciens. Il est à la fois le dernier des classiques, et le premier des modernes, c'est-à-dire qu'il a résolu les problèmes les plus classiques avec les méthodes les plus modernes. Gauss était un génie particulièrement précoce : à 5 ans, le maître demandait de calculer $1+2+\dots+100$, et Gauss inscrivit immédiatement le résultat sur son ardoise : ce n'est pas qu'il fut un génial calculateur, mais il avait trouvé une formule générale pour calculer de telles sommes. A l'université, à 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique, ce que ni Euler, ni Legendre n'avaient réussi à établir. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse de doctorat en 1799 ainsi que l'invention de la théorie des congruences. Le génie de Gauss se manifesta dans d'autres domaines : on lui doit d'importants travaux en électricité, en optique, en théorie du potentiel. Le "gauss" est ainsi devenu l'unité d'induction magnétique.