

Fiche récapitulatif "Structure algébrique"

Structure	Définition	Propriétés
Groupes usuels	• $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ sont des groupes commutatifs (abéliens). • $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$ sont des groupes commutatifs. • $(IK[X], +)$ est un groupe abélien. • $(M_n(K), +)$ est un groupe abélien. • $(GL_n(K), \times)$ est un groupe.	• $GL_n(IK)$ est un ouvert. ($GL_n(K) \neq \det^{-1}(IK^*)$). • $GL_n(\mathbb{R})$ n'est pas connexe par arcs.
Sous-groupe	Soit $(G, *)$ un groupe et $H \subset G$. • H est un sous-groupe de G si : $\begin{cases} \cdot e_G \in H \\ \cdot \forall x, y \in H \quad x * y \in H \\ \cdot \forall x \in H \quad x^{-1} \in H \end{cases}$ $\Leftrightarrow \begin{cases} \cdot e_G \in H \\ \cdot \forall x, y \in H \quad x * y^{-1} \in H \end{cases}$	• Si H est un sous-groupe de G, alors $(H, *)$ est un groupe. • Si $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, *)$, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de $(G, *)$.
Sous-groupes classiques	• $S_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}), \text{ telque } {}^t A = A\}$ est un sous-groupe de $(M_n(\mathbb{R}), +)$. • $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}), \text{ telque } {}^t A A = I_n\}$ est un sous-groupe de $GL_n(\mathbb{R})$. • $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}), \text{ telque } \det(A) = 1\}$ est un sous-groupe de $O_n(\mathbb{R})$.	• $O_n(\mathbb{R})$ est un compact (fermé et borné de $M_n(\mathbb{R})$) • $SO_n(\mathbb{R})$ est un compact (fermé inclus dans un compact).
Sous groupe engendré par une partie	Soient $(G, *)$ un groupe et A une partie quelconque de G. Le sous-groupe engendré par la partie A est le petit sous-groupe de G qui contient la partie A et c'est : $\langle A \rangle = \bigcap_{A \subset H, (H \text{ sous-groupe})} H.$ $\langle A \rangle = \{x_1 * \dots * x_n, \text{ avec } x_i \in A \text{ ou } x_i^{-1} \in A\}.$	• $y \in \langle A \rangle \iff y = x_1 * \dots * x_n$ avec $x_i \in A$ ou $x_i^{-1} \in A$. • Si le groupe est noté additivement $(G, +)$ et $a \in G$, alors $\langle a \rangle = \{ka, a \in \mathbb{Z}\}$. • Si le groupe est noté multiplicativement $(G, \times)$, et $a \in G$, alors $\langle a \rangle = \{a^k, a \in \mathbb{Z}\}$.

Groupe monogènes	On dit que $(G, *)$ est un groupe monogène si il existe un élément $a \in G$ tel que $G = \langle a \rangle$.	- Si $(G, *)$ est un groupe monogène, alors il est commutatif. - Tout groupe monogène et infini est isomorphe à $(\mathbb{Z}, +)$.
Groupe cyclique	On dit que $(G, *)$ est un groupe cyclique s'il est monogène et de cardinale fini.	$(\mathbb{Z}/n\mathbb{Z}, +) = \langle \bar{a} \rangle$ avec $a \wedge n = 1$. - Si $(G, *)$ est un groupe cyclique avec $\text{card}(G) = n$, alors $(G, *)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
Ordre d'un élément	Soient $(G, *)$ un groupe d'élément neutre e_G et $x \in G$. Pour $n \in \mathbb{N}^*$, on note $x^n = \underbrace{x * x * \dots * x}_{n \text{ fois}}$. On dit que x est d'ordre fini si il existe $p \in \mathbb{N}^*$ tel que $x^p = e_G$. Dans ce cas l'ordre de x est : $o(x) = \min\{p \in \mathbb{N}^* \text{ tel que } x^p = e_G\}.$	- Si $(G, *)$ un groupe fini avec $\text{card}(G) = m$, alors $\forall a \in G, a^m = e_G$. - Soit $k \in \mathbb{N}^*, x^k = e_G \iff o(x)$ divise k. Théorème de Lagrange Soient $(G, *)$ un groupe fini et H un sous groupe de G, alors $\text{card}(H)$ divise $\text{card}(G)$
Morphisme de Groupes	Soient $(G, *)$ et (G', T) deux groupes. $f : (G, *) \rightarrow (G', T)$ est un morphisme de groupes si $\forall (x, y) \in G^2, f(x * y) = f(x) T f(y)$	Soit $e_G, e_{G'}$ les éléments neutres respectivement des groupes G et G', alors $f(e_G) = e_{G'}$. $\forall x \in G, f(x^{-1}) = f(x)^{-1}$. - Si H est un sous groupe de G, alors $f(H)$ est un sous groupe de G'. - Si K est un sous groupe de G', alors $f^{-1}(K)$ est un sous groupe de G. $\text{Ker}(f)$ est un sous-groupe de G. $\text{Im}(f)$ est un sous-groupe de G'.
Anneaux usuels	$(\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times)$ sont des Anneaux commutatifs. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un Anneau commutatif. $(IK[X], +, \times)$ est un Anneau commutatif. $(M_n(K), +, \times)$ est un Anneau non commutatif. - Soit E un IK-e.v., alors $(\mathcal{L}(E), +, \circ)$ est un Anneau non commutatif.	

Sous-Anneau	Soit $(A, +, \times)$ un anneau d'élément neutre 1_A pour la loi $\times$ et $B \subset A$. B est un sous-anneau de l'anneau $(A, +, \times)$ si : $\begin{cases} 1_A \in B \\ \forall (x, y) \in B^2, x - y \in B \text{ et } x \times y \in B \end{cases}$	Si B est un sous-anneau de l'anneau $(A, +, \times)$, alors $(B, +, \times)$ est un anneau.
	Soit $(A, +, \times)$ un anneau. On pose $Inv(A)$ l'ensemble des éléments de A inversibles pour la loi $\times$, alors $(Inv(A), \times)$ est un groupe	L'ensemble des éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est : $Inv(\mathbb{Z}/n\mathbb{Z}) = \{k \in \mathbb{Z}, tq k \wedge n = 1\}$
	• Soient a et $b \in A$ tel que $ab = ba$ (a et b commutent), alors $(ab)^n = a^n b^n$ • Formule de binôme : $(a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$	• Soient a et $b \in A$ tel que $ab = ba$ $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} = (a - b) \cdot$ • $1 - b^n = (1 - b) \sum_{k=0}^{n-1} b^k = (1 - b) \cdot$
Anneau intègre	Soit $(A, +, \times)$ un anneau. On dit que A est un anneau intègre si $\forall x$ et y dans A, si $xy = 0$, alors $x = 0$ ou $y = 0$.	L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est intègre si et seulement si n est un nombre premier.
Idéal	Soient $(A, +, \times)$ un anneau commutatif et $I \subset A$. I est un idéal de l'anneau $(A, +, \times)$ si $\begin{cases} 0_A \in I \\ \forall (x, y) \in I^2, x - y \in I \\ \forall x \in I, \forall a \in A, ax \in I \end{cases}$	• Pour tout $x \in A$, l'ensemble $xA = \{ax, a \in A\}$ est un idéal de A.

Morphisme d'anneaux	Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux . • Un morphisme de l'anneaux $(A, +, \times)$ vers l'anneau $(B, +_B, \times_B)$. est une application $f : A \rightarrow B$ vérifiant : $\begin{cases} f(1_A) = 1_B \\ f(x +_A y) = f(x) +_B f(y) \\ f(x \times_A y) = f(x) \times_B f(y) \end{cases}$	• $\ker(f)$ est un idéal de $(A, +, \times)$. • f est injectif si et seulement si $\ker(f) = \{0_A\}$. • f est surjectif si et seulement si $\text{Im}(f) = B$.
Corps	$(IK, +, \times)$ un corps si $\begin{cases} IK \neq \{0\} \\ (IK, +, \times) \\ \forall x \in IK \setminus \{0\}, x \text{ est inversible} \end{cases}$	$(\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathbb{Q}, +, \times)$ sont des corps
Sous-corps	Soit $(K, +, \times)$ un corps d'élément neutre 1 pour la loi $\times$ et $L \subset K$. L est un sous-corps du corps $(K, +, \times)$ si : $\begin{cases} 1 \in L \\ \forall (x, y) \in L^2, x - y \in L \text{ et } x \times y \in L \\ \forall x \in L \setminus \{0\}, x^{-1} \in L \end{cases}$	• Si L est un sous-corps d'un corps $(K, +, \times)$, alors $(L, +, \times)$ est un Corps. • L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est un nombre premier.
Sous-algèbre	Soit $(A, +, \cdot, \times)$ une IK-algèbre et $B \subset A$. B est une sous-algèbre de l'algèbre $(A, +, \cdot, \times)$ si $\begin{cases} B \neq \emptyset \\ \forall (x, y) \in B^2, \forall \lambda \in IK, \lambda \cdot x + y \in B \\ \forall (x, y) \in B^2, x \times y \in B \end{cases}$	
Morphisme d'algèbres	Soient $(A, +, \cdot, \times)$, $(B, +, \cdot, \times)$ deux IK-algèbres $f : A \rightarrow B$. On dit que f est un morphisme d'algèbres si $\begin{cases} \forall (x, y) \in A^2, f(x + y) = f(x) + f(y) \\ \forall (x, y) \in A^2, f(x \times y) = f(x) \times f(y) \\ \forall x \in A \text{ et } \lambda \in IK, f(\lambda x) = \lambda f(x) \end{cases}$	