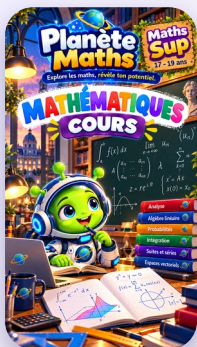


Groupes, anneaux et corps : cours de maths Maths Sup à télécharger en PDF



Le livre de cours de maths Maths Sup

Tout le programme en un seul PDF de 103 pages, à imprimer ou à garder sur ta tablette.

[Voir le livre](#)

Additionner des entiers, composer des fonctions, mélanger un jeu de cartes, calculer modulo une horloge : ces situations semblent éloignées, et pourtant elles obéissent aux mêmes règles. L'algèbre générale isole ces règles et leur donne un nom : **structure algébrique**. Ce chapitre construit le vocabulaire des lois, des groupes, des anneaux et des corps, présente le groupe des permutations, puis rassemble les outils de calcul indispensables en première année : sommes, produits et coefficients binomiaux.

1. Lois de composition interne

D Loi de composition interne

Une **loi de composition interne** (LCI) sur un ensemble E est une application $\star : E \times E \rightarrow E$, notée $(x, y) \mapsto x \star y$. Le résultat reste dans E : on dit que E est **stable** par la loi.

Une loi peut posséder des propriétés remarquables :

- **associative** : $(x \star y) \star z = x \star (y \star z)$ pour tous x, y, z ;
- **commutative** : $x \star y = y \star x$ pour tous x, y ;
- admettre un **élément neutre** e : $x \star e = e \star x = x$ pour tout x ;
- un élément x est **symétrisable** s'il existe x' tel que $x \star x' = x' \star x = e$; x' est alors un symétrique de x .

E Exemple : une loi inventée

Sur $E = \mathbb{R} \setminus \{1\}$, on pose $x \star y = x + y - xy$. Remarquons que $1 - (x \star y) = (1 - x)(1 - y)$.

Comme $1 - x$ et $1 - y$ sont non nuls, leur produit est non nul : $x \star y \neq 1$, donc E est stable. Pour l'associativité, $1 - ((x \star y) \star z) = (1 - x)(1 - y)(1 - z)$, expression symétrique en x, y, z , donc identique pour $x \star (y \star z)$. La loi est commutative, l'élément neutre est 0 , et le symétrique de x est $x' = \frac{x}{x-1}$: par exemple $2' = 2$, car $2 \star 2 = 4 - 4 = 0$.



Attention

La soustraction sur $\mathbb{Z}$ n'est pas associative : $(5 - 3) - 1 = 1$ alors que $5 - (3 - 1) = 3$. Une loi n'est pas toujours associative, ni commutative : la composition de fonctions ne l'est pas.

2. Groupes



Groupe

Un **groupe** est un couple $(G, \star)$ où $\star$ est une LCI sur G **associative**, admettant un **élément neutre** e , et pour laquelle **tout élément possède un symétrique**. Si de plus $\star$ est commutative, le groupe est dit **abélien** (ou commutatif).

Exemples de référence : $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}_+^*, \times)$, le groupe des racines n -ièmes de l'unité $(\mathbb{U}_n, \times)$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ des classes modulo n , et le groupe des bijections d'un ensemble dans lui-même, muni de la composition (non abélien dès que l'ensemble a trois éléments). En revanche $(\mathbb{N}, +)$ n'est pas un groupe (pas d'opposé) ni $(\mathbb{Z}, \times)$ (seuls 1 et -1 sont inversibles).



Règles de calcul dans un groupe

Dans un groupe $(G, \star)$: l'élément neutre est unique ; le symétrique d'un élément est unique, noté x^{-1} (ou $-x$ en notation additive) ; $(x \star y)^{-1} = y^{-1} \star x^{-1}$; tout élément est **régulier** : $x \star a = x \star b \Rightarrow a = b$.

La preuve de la règle sur $(x \star y)^{-1}$ tient en une ligne :

$(x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = x \star x^{-1} = e$. Attention à l'ordre des facteurs, il s'inverse.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

chaque ligne et chaque colonne contient 0, 1, 2, 3 une

La table ci-dessus est celle de $(\mathbb{Z}/4\mathbb{Z}, +)$. Dans un groupe fini, chaque ligne et chaque colonne contient tous les éléments exactement une fois : c'est la régularité en action. L'élément neutre **0** apparaît une fois par ligne, et deux éléments symétriques l'un de l'autre sont placés de façon symétrique autour de la diagonale (ici $1 + 3 = 0$ et $2 + 2 = 0$).

3. Sous-groupes

P

Caractérisation des sous-groupes

Une partie H d'un groupe $(G, \star)$ est un **sous-groupe** si et seulement si : H contient e ; pour tous $x, y \in H$, $x \star y^{-1} \in H$. Un sous-groupe est alors lui-même un groupe pour la loi induite.

E**Exemple : intersection et somme dans $\mathbb{Z}$**

Pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$: $0 \in n\mathbb{Z}$ et la différence de deux multiples de n est un multiple de n . Pour $4\mathbb{Z}$ et $6\mathbb{Z}$, l'intersection est $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$ (multiples communs : $\text{ppcm} = 12$), et la somme $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$ ($\text{pgcd} = 2$). En revanche la **réunion** $4\mathbb{Z} \cup 6\mathbb{Z}$ n'est pas un sous-groupe : $4 + 6 = 10$ n'appartient à aucun des deux.

P**Sous-groupes de $\mathbb{Z}$**

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Preuve : si $H \neq \{0\}$, il contient un entier strictement positif ; soit n le plus petit. Pour $h \in H$, la division euclidienne $h = nq + r$ avec $0 \leq r < n$ donne $r = h - nq \in H$, donc $r = 0$ par minimalité de n , et $H = n\mathbb{Z}$.

Un élément x d'un groupe est d'**ordre fini** s'il existe $m \geq 1$ avec $x^m = e$; le plus petit tel m est l'**ordre** de x . Dans $\mathbb{Z}/n\mathbb{Z}$, la classe de k est d'ordre $\frac{n}{\text{pgcd}(n, k)}$. Dans un groupe fini, l'ordre d'un sous-groupe divise celui du groupe (théorème de Lagrange, admis ici), et l'ordre de chaque élément divise l'ordre du groupe.

4. Morphismes de groupes

D Morphisme

Une application $f : (G, \star) \rightarrow (G', \cdot)$ est un **morphisme de groupes** si $f(x \star y) = f(x) \cdot f(y)$ pour tous $x, y \in G$. Le **noyau** est $\text{Ker } f = \{x \in G \mid f(x) = e'\}$, l'**image** est $\text{Im } f = f(G)$. Un morphisme bijectif est un **isomorphisme**.

P Propriétés

Un morphisme vérifie $f(e) = e'$ et $f(x^{-1}) = f(x)^{-1}$. Son noyau est un sous-groupe de G , son image un sous-groupe de G' , et f est **injectif si et seulement si** $\text{Ker } f = \{e\}$.

Pour l'injectivité : si $f(x) = f(y)$, alors $f(x \star y^{-1}) = e'$, donc $x \star y^{-1} \in \text{Ker } f = \{e\}$ et $x = y$.
Exemples classiques : l'exponentielle $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ est un isomorphisme (de réciproque $\ln$) ; la réduction modulo n , $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, est un morphisme surjectif de noyau $n\mathbb{Z}$; le déterminant $\det : (\text{GL}_n(\mathbb{R}), \times) \rightarrow (\mathbb{R}^*, \times)$ en est un autre.

E Exemple : un morphisme calculé

L'application $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, $n \mapsto 7n$, est un morphisme car $7(a + b) = 7a + 7b$. Son noyau est $\{0\}$, donc f est injectif ; son image est $7\mathbb{Z}$, donc f n'est pas surjectif. En revanche $g(n) = n + 1$ n'est pas un morphisme car $g(0) = 1 \neq 0$.

5. Anneaux et corps

D Anneau

Un **anneau** est un triplet $(A, +, \times)$ tel que $(A, +)$ est un groupe abélien, $\times$ est associative, possède un neutre 1_A , et est **distributive** sur $+$: $a(b + c) = ab + ac$ et $(a + b)c = ac + bc$. L'anneau est **commutatif** si $\times$ l'est.

Dans un anneau, $0 \cdot x = 0$ et $(-1) \cdot x = -x$. Mais le produit de deux éléments non nuls peut être nul : on parle alors de **diviseurs de zéro**. Un anneau commutatif sans diviseur de zéro (et $1 \neq 0$) est dit **intègre**. L'ensemble $A^\times$ des éléments inversibles pour $\times$ est un groupe.

D Corps

Un **corps** est un anneau commutatif dans lequel $1 \neq 0$ et où **tout élément non nul est inversible**.

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps ; $\mathbb{Z}$ est un anneau intègre qui n'est pas un corps. Tout corps est intègre. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ montrent la richesse du sujet.

P Inversibles de $\mathbb{Z}/n\mathbb{Z}$

La classe de k est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(k, n) = 1$. En particulier $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

E**Exemple : $\mathbb{Z}/10\mathbb{Z}$ n'est pas un corps**

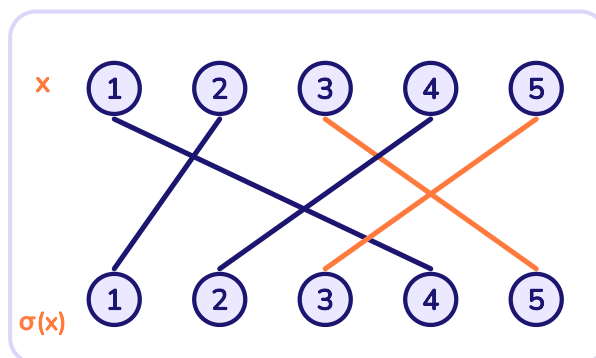
Dans $\mathbb{Z}/10\mathbb{Z}$, $2 \times 5 = 10 = 0$: **2** et **5** sont des diviseurs de zéro, donc l'anneau n'est pas intègre. Les inversibles sont les classes premières avec **10** : **1, 3, 7, 9**, avec $3 \times 7 = 21 = 1$ et $9 \times 9 = 81 = 1$.

!**Astuce de Zyro**

Dans un corps, on peut simplifier par tout élément non nul. Dans un anneau qui a des diviseurs de zéro, $ab = ac$ n'entraîne pas $b = c$: méfie-toi des simplifications automatiques !

6. Le groupe symétrique

Une **permutation** de $\{1, \dots, n\}$ est une bijection de cet ensemble dans lui-même. L'ensemble S_n des permutations, muni de la composition $(\sigma\tau)(x) = \sigma(\tau(x))$, est un groupe de cardinal $n!$, non abélien dès que $n \geq 3$. On écrit σ en ligne par la liste $(\sigma(1), \dots, \sigma(n))$.



Sur la figure, la flèche part du haut (x) vers le bas ($\sigma(x)$). On suit $1 \rightarrow 4 \rightarrow 2 \rightarrow 1$ puis $3 \rightarrow 5 \rightarrow 3$: ce sont les deux **cycles** de la permutation. On la note $\sigma = (1\ 4\ 2)(3\ 5)$.

P**Décomposition en cycles**

Toute permutation se décompose de façon unique, à l'ordre près, en produit de cycles à supports disjoints, qui commutent entre eux. Un cycle de longueur k est d'ordre k , et l'ordre d'une permutation est le **ppcm** des longueurs de ses cycles. Un cycle de longueur k s'écrit comme produit de $k - 1$ transpositions.

La **signature** $\varepsilon : S_n \rightarrow \{-1, 1\}$ est l'unique morphisme de groupes qui vaut -1 sur chaque transposition. Un cycle de longueur k a pour signature $(-1)^{k-1}$. Le noyau de ε , formé des permutations paires, est le **groupe alterné** A_n , de cardinal $\frac{n!}{2}$ pour $n \geq 2$.

E**Exemple : étude d'une permutation de S_5**

Pour $\sigma = (1\ 4\ 2)(3\ 5)$, l'ordre est **ppcm**(3, 2) = 6 et la signature vaut $(+1)(-1) = -1$: σ est impaire. Calculons $\sigma^2 : 1 \mapsto \sigma(4) = 2, 2 \mapsto \sigma(1) = 4, 4 \mapsto \sigma(2) = 1$, et $3 \mapsto \sigma(5) = 3, 5 \mapsto 5$. Ainsi $\sigma^2 = (1\ 2\ 4)$, un 3-cycle, de signature $+1$, ce qui confirme $\varepsilon(\sigma^2) = \varepsilon(\sigma)^2 = 1$.

M**Méthode : étudier une permutation**

1. Suivre l'image de **1**, puis de son image, jusqu'à revenir à **1** : premier cycle.
2. Recommencer avec le plus petit élément non encore rencontré.
3. Lire l'ordre (ppcm des longueurs) et la signature (produit des $(-1)^{k-1}$).

7. Sommes et produits

La notation $\sum_{k=m}^n a_k = a_m + a_{m+1} + \dots + a_n$ comporte $n - m + 1$ termes ; l'indice k est muet.

De même $\prod_{k=m}^n a_k$ désigne le produit des mêmes termes, et $n! = \prod_{k=1}^n k$. La somme est **linéaire** :

$\sum (\lambda a_k + b_k) = \lambda \sum a_k + \sum b_k$. Un **changement d'indice** $j = k + 1$ décale les bornes sans changer la valeur.

P

Sommes usuelles

$$\sum_{k=1}^n k = \frac{n(n+1)}{2} ; \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6} ; \sum_{k=0}^n q^k = \frac{1-q^{n+1}}{1-q} \text{ pour } q \neq 1.$$

Et la **somme télescopique** : $\sum_{k=m}^n (u_{k+1} - u_k) = u_{n+1} - u_m$.

E

Exemple : télescopage d'un produit

Pour $n \geq 2$,

$$\prod_{k=2}^n \left(1 - \frac{1}{k^2}\right) = \prod_{k=2}^n \frac{(k-1)(k+1)}{k \cdot k} = \frac{1 \cdot 2 \cdots (n-1)}{2 \cdot 3 \cdots n} \times \frac{3 \cdot 4 \cdots (n+1)}{2 \cdot 3 \cdots n} = \frac{1}{n} \times$$

. Pour $n = 4$: $\frac{3}{4} \times \frac{8}{9} \times \frac{15}{16} = \frac{5}{8}$.

Pour une **somme double** sur un rectangle, on peut intervertir : $\sum_{i=1}^p \sum_{j=1}^q a_{ij} = \sum_{j=1}^q \sum_{i=1}^p a_{ij}$.

Sur un domaine triangulaire, on écrit $\sum_{1 \leq i \leq j \leq n} a_{ij} = \sum_{j=1}^n \sum_{i=1}^j a_{ij} = \sum_{i=1}^n \sum_{j=i}^n a_{ij}$, en

faisant attention aux nouvelles bornes. Enfin, $\left(\sum_i a_i\right)\left(\sum_j b_j\right) = \sum_{i,j} a_i b_j$.

8. Coefficients binomiaux

D Coefficient binomial

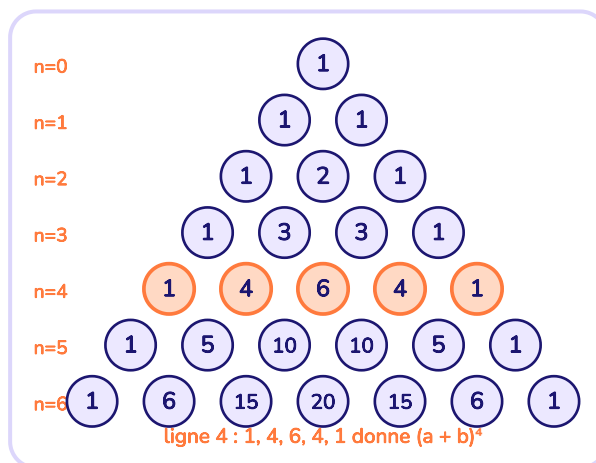
Pour $0 \leq k \leq n$, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. C'est le nombre de parties à k éléments d'un ensemble à n éléments.

P Propriétés

Symétrie : $\binom{n}{k} = \binom{n}{n-k}$. Relation de Pascal : $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

Formule du **binôme de Newton** : si a et b **commutent** dans un anneau,

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$



La relation de Pascal se lit sur le triangle : chaque nombre est la somme des deux voisins situés au-dessus de lui. La ligne n donne les coefficients de $(a + b)^n$. La condition de commutation est essentielle : pour deux matrices qui ne commutent pas, $(A + B)^2 \neq A^2 + 2AB + B^2$ en général.

E**Exemple : développer avec le binôme**

$$(2x + 3)^4 = \binom{4}{0}(2x)^4 + \binom{4}{1}(2x)^3 \cdot 3 + \binom{4}{2}(2x)^2 \cdot 9 + \binom{4}{3}(2x) \cdot 27 + \binom{4}{4} \cdot 81$$

En choisissant $a = b = 1$ on trouve $\sum_{k=0}^n \binom{n}{k} = 2^n$; avec $a = 1, b = -1$,

$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ pour $n \geq 1$. L'identité $k \binom{n}{k} = n \binom{n-1}{k-1}$ permet des simplifications utiles.

À retenir

- Un **groupe** : LCI associative, neutre, tout élément symétrisable ; $(x \star y)^{-1} = y^{-1} \star x^{-1}$.
- H est un **sous-groupe** de G si $e \in H$ et $x \star y^{-1} \in H$ pour tous $x, y \in H$; ceux de $\mathbb{Z}$ sont les $n\mathbb{Z}$.
- Un **morphisme** envoie neutre sur neutre ; f est injectif si et seulement si $\text{Ker } f = \{e\}$.
- Un **anneau** : $(A, +)$ groupe abélien, $\times$ associative, distributive ; un **corps** : tout non nul est inversible ; $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
- S_n est de cardinal $n!$; on décompose en **cycles disjoints**, l'ordre est le ppcm des longueurs, la signature d'un k -cycle vaut $(-1)^{k-1}$.
- Le **binôme** $(a + b)^n = \sum \binom{n}{k} a^k b^{n-k}$ exige que a et b commutent ; $\sum_k \binom{n}{k} = 2^n$.

Le livre de cours de maths Maths Sup

Tout le programme en un seul PDF de 103 pages, à imprimer ou à garder sur ta tablette.

[Voir le livre](#)

Zyro te conseille la suite

Exercices de maths

Groupes, anneaux et corps : exercices de maths Maths Sup

Contrôles de maths

Groupes, anneaux et corps : contrôle de maths Maths Sup

QCM de maths

Groupes, anneaux et corps : QCM de maths Maths Sup

Exercices de maths

Espaces vectoriels et applications linéaires : exercices de maths Maths Sup

 Exercices de maths

Matrices et déterminants : exercices de maths Maths Sup

 Contrôles de maths

Espaces vectoriels et applications linéaires : contrôle de maths Maths Sup

Zyro vous emmène sur nos sites partenaires

Embarquez pour d'autres planètes du savoir et leurs applis.

Décollage