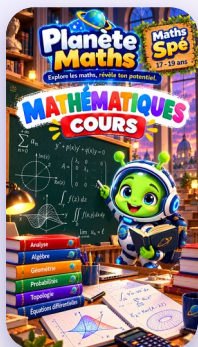


Algèbre générale et dualité : cours de maths Maths Spé à télécharger en PDF



Le livre de cours de maths Maths Spé

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

[Voir le livre](#)

Ce chapitre rassemble les structures de l'algèbre générale (groupes, anneaux, polynômes) et l'outil central de l'algèbre linéaire abstraite : la dualité. Tu y apprends à reconnaître une structure, à manipuler ses morphismes, puis à voir un espace vectoriel à travers ses formes linéaires. Tout se passe sur un corps $\mathbb{K}$ quelconque ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Z}/p\mathbb{Z}$).

1. Groupes et morphismes

D

Groupe

Un groupe est un ensemble G muni d'une loi interne $*$ associative, possédant un élément neutre e , et dans lequel chaque élément x admet un symétrique x^{-1} . Il est abélien si $x * y = y * x$ pour tous x, y .

D Morphisme de groupes

Une application $f : G \rightarrow H$ est un morphisme si $f(xy) = f(x)f(y)$ pour tous $x, y \in G$. On note $\ker f = \{x \in G \mid f(x) = e_H\}$ son noyau et $\text{Im } f$ son image.

P Propriétés

Un morphisme vérifie $f(e_G) = e_H$ et $f(x^{-1}) = f(x)^{-1}$. Son noyau est un sous-groupe de G , son image un sous-groupe de H , et f est injectif si et seulement si $\ker f = \{e_G\}$.

L'ordre d'un élément x est le plus petit entier $k \geq 1$ tel que $x^k = e$. Le **théorème de Lagrange** affirme que, dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe ; en particulier l'ordre de chaque élément divise $|G|$. Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, la classe de k est d'ordre $\frac{n}{\text{pgcd}(n, k)}$.

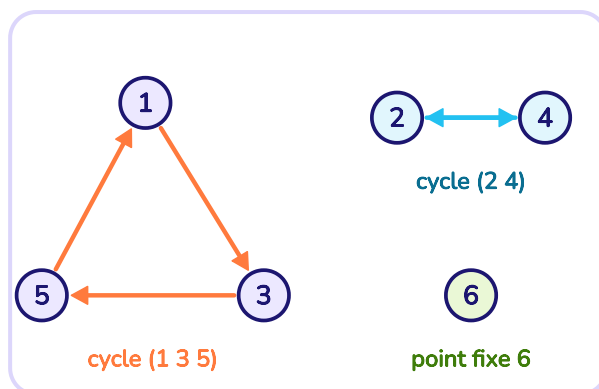
E Exemple 1 Dans $\mathbb{Z}/12\mathbb{Z}$, la classe de 9 a pour ordre $\frac{12}{\text{pgcd}(12, 9)} = \frac{12}{3} = 4$: en effet $9, 18, 27, 36 \equiv 9, 6, 3, 0$. L'application $k \mapsto k \bmod 4$ est un morphisme de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$, de noyau $\{0, 4, 8\}$.

I 2. Groupe symétrique

Le groupe symétrique $\mathfrak{S}_n$ est l'ensemble des bijections de $\{1, \dots, n\}$ dans lui-même, muni de la composition ; il a $n!$ éléments et n'est pas commutatif dès que $n \geq 3$.

P Décomposition en cycles

Toute permutation s'écrit, de façon unique à l'ordre près, comme produit de cycles à supports disjoints, et ces cycles commutent. L'ordre de la permutation est le ppcm des longueurs des cycles. Il existe un unique morphisme non trivial $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$, la **signature** : une transposition vaut -1 et un cycle de longueur ℓ vaut $(-1)^{\ell-1}$.



Le noyau de ε est le groupe alterné $\mathfrak{A}_n$, d'ordre $\frac{n!}{2}$.

E Exemple 2 Dans $\mathfrak{S}_6$, la permutation $\sigma = (1\ 3\ 5)(2\ 4)$ a pour ordre $\text{ppcm}(3, 2) = 6$ et pour signature $(-1)^2 \times (-1)^1 = -1$. Sa puissance $\sigma^3 = (2\ 4)$ est une transposition, car $(1\ 3\ 5)^3 = \text{id}$.

3. Anneaux et idéaux

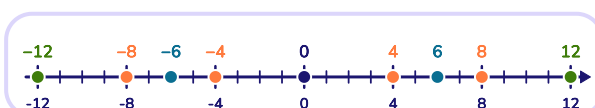
D Anneau, idéal

Un anneau $(A, +, \times)$ est un groupe abélien pour $+$, muni d'une multiplication associative, distributive sur $+$, avec un élément neutre 1 . Un **idéal** I est un sous-groupe additif tel que $ax \in I$ pour tout $a \in A$ et tout $x \in I$.

Le noyau d'un morphisme d'anneaux est un idéal. Dans $\mathbb{Z}$, les idéaux sont exactement les $n\mathbb{Z}$: on dit que $\mathbb{Z}$ est principal. La classe de k est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(k, n) = 1$; l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

P Somme et intersection

$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ où $d = \text{pgcd}(a, b)$, et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ où $m = \text{ppcm}(a, b)$. La première égalité est l'identité de Bézout : il existe u, v entiers tels que $au + bv = d$.



E

Exemple 3 $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$ car $2 = 2 \times 4 - 1 \times 6$, et $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$ (points verts de la figure). Dans $\mathbb{Z}/15\mathbb{Z}$, la classe de **4** est inversible d'inverse **4** car **16** $\equiv$ **1**, alors que **3** $\times$ **5** $\equiv$ **0** : **3** et **5** sont des diviseurs de zéro.

4. Polynômes et arithmétique

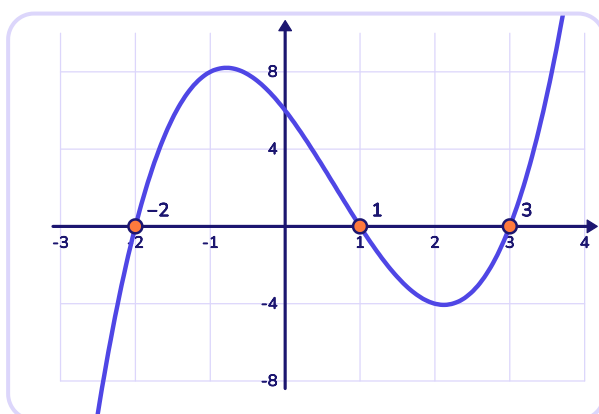
L'anneau $\mathbb{K}[X]$ se comporte comme $\mathbb{Z}$: il possède une **division euclidienne** (pour $B \neq 0$, il existe un unique couple (Q, R) avec $A = BQ + R$ et $\deg R < \deg B$), tous ses idéaux sont principaux, et deux polynômes ont un pgcd unitaire unique, obtenu par l'algorithme d'Euclide.

M

Méthode : pgcd de deux polynômes

1. Divise A par B pour obtenir le reste R_1 .
2. Divise B par R_1 , puis R_1 par R_2 , et ainsi de suite.
3. Le dernier reste non nul, rendu unitaire, est le pgcd ; en remontant on obtient une relation de Bézout $AU + BV = \text{pgcd}$.

Un scalaire a est racine de P si et seulement si $(X - a) \mid P$; le reste de la division de P par $X - a$ vaut $P(a)$. Un polynôme non nul de degré n a au plus n racines dans $\mathbb{K}$.



E Exemple 4 Le polynôme $P = (X + 2)(X - 1)(X - 3) = X^3 - 2X^2 - 5X + 6$ a trois racines simples (figure). Le reste de sa division par $X - 4$ est $P(4) = 6 \times 3 \times 1 = 18$, et $\text{pgcd}(P, X^2 - 1) = X - 1$, car -1 n'est pas racine de P .

5. Déterminants

Pour $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$, on pose $\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n a_{\sigma(i), i}$. On retrouve ainsi le rôle de la signature.

P Propriétés

Le déterminant est linéaire par rapport à chaque colonne et change de signe quand on échange deux colonnes. De plus $\det(AB) = \det A \det B$, $\det(\lambda A) = \lambda^n \det A$, $\det({}^t A) = \det A$, et A est inversible si et seulement si $\det A \neq 0$. Ajouter à une colonne un multiple d'une autre ne change pas le déterminant.

E Exemple 5 Le déterminant de Vandermonde $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = (b - a)(c - a)(c - b)$.
Pour $(a, b, c) = (1, 2, 4)$, on obtient $1 \times 3 \times 2 = 6$.

6. Formes linéaires et hyperplans

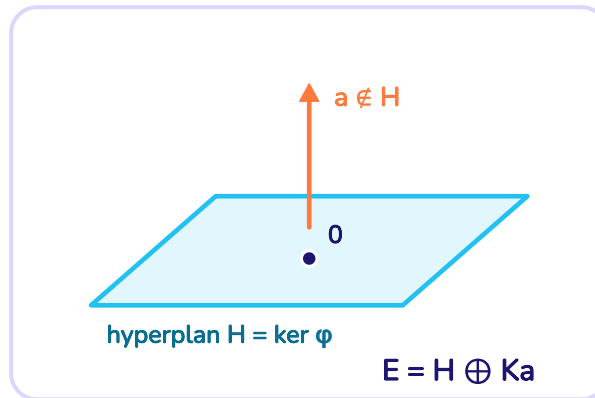
D Dualité

Le dual de E est $E^* = \mathcal{L}(E, \mathbb{K})$: ses éléments sont les **formes linéaires** sur E . Un **hyperplan** de E est le noyau d'une forme linéaire non nulle.

P

Hyperplans

Si $\dim E = n$, un hyperplan est de dimension $n - 1$. Si $H = \ker \varphi$ et $a \notin H$, alors $E = H \oplus \mathbb{K}a$. Deux formes non nulles ont le même noyau si et seulement si elles sont proportionnelles.



E

Exemple 6 La forme $\varphi(x, y, z) = 3x - y + 2z$ sur $\mathbb{R}^3$ a pour noyau un plan, de base $(1, 3, 0)$ et $(0, 2, 1)$: on vérifie $3 - 3 = 0$ et $-2 + 2 = 0$. La forme $6x - 2y + 4z$ a le même noyau, c'est 2φ .

7. Base duale

P

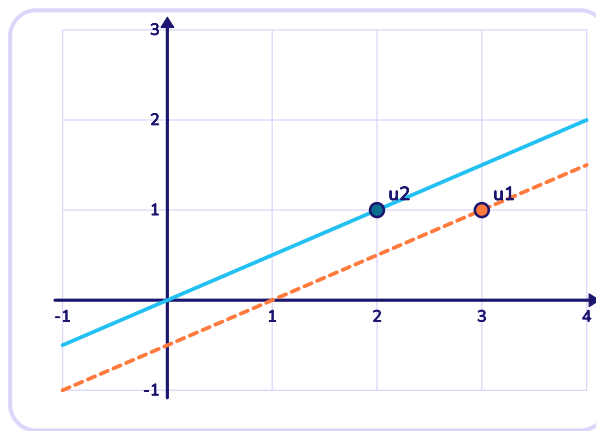
Base duale

Si $(e_1, \dots, e_n)$ est une base de E , les formes coordonnées e_i^* , définies par $e_i^*(e_j) = \delta_{ij}$, forment une base de E^* . Ainsi $\dim E^* = \dim E$ et, pour tout $x \in E$ et toute $\varphi \in E^*$, $x = \sum_i e_i^*(x) e_i$ et $\varphi = \sum_i \varphi(e_i) e_i^*$.

M

Méthode : calculer une base duale

1. Écris la matrice P dont les colonnes sont les coordonnées des e_j dans la base canonique.
2. Calcule P^{-1} : ses lignes sont les formes e_i^* exprimées dans la base duale de la base canonique.
3. Vérifie $e_i^*(e_j) = \delta_{ij}$.



E

Exemple 7 Dans $\mathbb{R}^2$, prenons $u_1 = (3, 1)$ et $u_2 = (2, 1)$, soit $P = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$, de déterminant 1, et $P^{-1} = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$, donc $u_1^*(x, y) = x - 2y$ et $u_2^*(x, y) = -x + 3y$. Contrôle : $u_1^*(3, 1) = 1$, $u_1^*(2, 1) = 0$, $u_2^*(3, 1) = 0$, $u_2^*(2, 1) = 1$.

!

Zyro Pour te souvenir de la base duale, pense à une règle de coordonnées : chaque forme e_i^* ne regarde que la i -ème composante du vecteur et ignore tout le reste.

8. Algèbre linéaire sur un corps

Tout ce qui précède (bases, dimension, théorème du rang, pivot de Gauss, déterminant) reste vrai sur n'importe quel corps $\mathbb{K}$. Il faut seulement se souvenir que, sur $\mathbb{Z}/2\mathbb{Z}$, on a $1 + 1 = 0$. Le

théorème du rang s'écrit $\dim E = \dim \ker u + \operatorname{rg} u$, et le rang d'une matrice est égal à celui de sa transposée.

P Interpolation de Lagrange

Si $a_0, \dots, a_n$ sont des scalaires distincts, les formes d'évaluation $\operatorname{ev}_{a_i} : P \mapsto P(a_i)$ forment une base du dual de $\mathbb{K}_n[X]$. Leur base antéduale est formée des polynômes $L_i = \prod_{j \neq i} \frac{X - a_j}{a_i - a_j}$, et tout $P \in \mathbb{K}_n[X]$ vérifie $P = \sum_i P(a_i) L_i$.

E **Exemple 8** Sur le corps $\mathbb{Z}/2\mathbb{Z}$, l'espace $E = (\mathbb{Z}/2\mathbb{Z})^2$ a 4 éléments. Une base est un couple de vecteurs non nuls distincts : $3 \times 2 = 6$ bases possibles, autant que de matrices inversibles 2×2 , c'est-à-dire que d'éléments de $\mathfrak{S}_3$.

⚠ **Erreur classique** Dans un groupe non commutatif, $(xy)^{-1} = y^{-1}x^{-1}$ et non $x^{-1}y^{-1}$; de même $\det(A + B) \neq \det A + \det B$ en général.

À retenir

- Un morphisme de groupes est injectif si et seulement si son noyau est trivial ; l'ordre d'un élément divise l'ordre du groupe fini.
- Toute permutation est produit de cycles disjoints : son ordre est le ppcm des longueurs, sa signature est multiplicative.
- Les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$ sont principaux : somme = pgcd, intersection = ppcm, Bézout.
- a est racine de P si et seulement si $(X - a) \mid P$; le reste modulo $X - a$ est $P(a)$.
- $\det(AB) = \det A \det B$ et $\det A \neq 0$ si et seulement si A est inversible.
- Un hyperplan est le noyau d'une forme non nulle ; deux équations d'un même hyperplan sont proportionnelles.
- La base duale est donnée par les lignes de P^{-1} ; elle donne les coordonnées dans la base et conduit à Lagrange.

Le livre de cours de maths Maths Spé

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

Algèbre générale et dualité : exercices de maths Maths Spé

 Contrôles de maths

Algèbre générale et dualité : contrôle de maths Maths Spé

 QCM de maths

Algèbre générale et dualité : QCM de maths Maths Spé

 Exercices de maths

Courbes, surfaces et géométrie euclidienne : exercices de maths Maths Spé

 Exercices de maths

Réduction des endomorphismes : exercices de maths Maths Spé

 Contrôles de maths

Courbes, surfaces et géométrie euclidienne : contrôle de maths Maths Spé

Zyro vous emmène sur nos sites partenaires

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

Décollage