Motivations

Le programme de mathématiques du second semestre du DEUG mathématiques–informatique comporte des notions assez abstraites, dont la pertinence et l'utilité ne sautent pas toujours aux yeux. Je réunis ici quelques applications des thèmes abordés, essentiellement en informatique, pour montrer que ces considérations ne sont pas coupées du monde réel, loin s'en faut.

Arithmétique

Les calculs modulaires sont omniprésents en informatique : par exemple, dans l'indexation des tables de hachage ou dans les générateurs de nombres pseudo-aléatoires les plus simples.

Les codes correcteurs permettent permettent de vérifier qu'une information a bien été transmise : ainsi, les numéros de carte bleue sont des multiples de 17 ; grace au critère de divisibilité correspondant on peut donc s'appercevoir tout de suite qu'une erreur de frappe a été commise.

Mais la principale application de l'arithmétique reste la cryptographie : les théorèmes de Fermat et d'Euler permettent de définir des systèmes cryptographiques à clef secrète et publique (RSA). La conception de générateurs de nombres pseudo-aléatoires (meilleurs que ceux mentionnés plus haut) et de certains algorithmes de compression compte parmi les applications de la cryptographie. Le lecteur intéressé peut consulter K.H. Rosen, *Elementary number theory*, Addison-Wesley, 1984.

Groupes

Trier une liste revient à trouver une permutation de ses éléments pour les remettre dans l'ordre, *i.e.*, à trouver un élément du groupe de permutations correspondant. Très souvent, cet élément va être décrit comme la composition de permutations plus simples, comme par exemple des transpositions. Pour savoir que l'algorithme a une chance de marcher, il faut savoir que l'on peut exprimer la permutation que l'on cherche à l'aide des transpositions, en d'autres termes, il faut savoir que le groupe symétrique est engendré par ces permutations. Ainsi, dans le tri à bulles, on n'utilise que les transpositions de la forme $(i\ i+1)$; on sait qu'elles engendrent le groupe symétrique.

Les groupes que l'on rencontre peuvent décrire les symétries de certains objets mathématiques (c'est grace à la théorie des groupes que l'on construit les pavages du plan) ou physiques (par exemple, en cristallographie : deux cristaux de forme différentes, tels un cubes et un octaèdre, peuvent avoir le même groupe de symétrie et correspondent à un cristal de même nature).

La théorie des jeux révèle d'autre applications des groupes : on peut ainsi comprendre comment résoudre le problème du Rubik's Cube®.

La notion d'action d'un groupe intervient dans de très nombreux problèmes combinatoires.

Tout ce que vous avez pu voir en géométrie dans votre cursus peut se ramener à l'étude de l'action d'un groupe dans le plan (ou l'espace). Avec d'autres groupes, on se retrouve avec les « géométries non euclidiennes ». La théorie des groupes permet ainsi d'unifier la géométrie.

Quand vous demandez à votre éditeur de texte de chercher une chaîne de caractères, vous pouvez en fait lui demander des choses plus compliquées, comme par exemple quels sont les mots du texte qui ne contiennent pas la lettre « e », ou s'il y a des mots qui apparaissent deux fois : les expressions régulières permettent d'exprimer toutes ces requêtes. L'ensemble des textes qui contiennent le motif demandé forme un monoïde (c'est comme un groupe, mais on ne demande pas que tout élément possède un symétrique). Une expression régulière est donc un moyen de décrire une structure algébrique proche de celle de groupe. Pour rechercher le motif, l'ordinateur va transformer l'expression régulière en un automate fini. Pour une description théorique, voir P Wolper, *Introduction à la calculabilité*, InterEditions, 1991 ; pour l'utilisation pratique, voir la documentation d'un éditeur de texte comme Emacs ou d'un langage de programmation comme Perl.

Anneaux

Les anneaux $\mathbb{Z}/n\mathbb{Z}$ interviennent en arithmétique et nous avons déjà vu certaines de leurs applications plus haut.

Les anneaux tels que $\mathbb{Z}[i\sqrt{5}]$ interviennent en théorie algébrique des nombres et donc en cryptographie, mais leur compréhension requiert des notions qui ne sont pas du tout au programme de DEUG.

La position du bras d'un robot peut être décrite par des équations polynômiales (qui disent simplement que le coude est sur un cercle de centre l'épaule et que la main est sur un cercle de centre le coude), *i.e.*, par des éléments d'un anneau de polynômes. Des calculs dans cet anneau (plus exactement, des calculs sur les idéaux de cet anneau) permettent de savoir quelles sont les positions que la main du robot peut atteindre, comment les atteindre, et parmi ces position, lesquelles sont « instables » et donc à éviter. L'étudiant intéressé peut consulter le livre de D. Cox, J. Little et D. O'Shea, *Ideals, varieties and algorithms*, Springer Verlag, 1992.

Corps

Un signal numérique est une suite de zéros et de uns, *i.e.*, une suite d'éléments du corps à 2 éléments $\mathbb{Z}/2\mathbb{Z}$. L'informatique utilise parfois aussi des corps dont le nombre d'éléments est une puissance de deux.

Espaces vectoriels

En première approximation, les problèmes physiques que l'on rencontre sont linéaires (en termes calculatoires, si on ne retient que les premiers termes d'un développement limité, on obtient des équations linéaires) et leurs solutions forment des espaces vectoriels. Par exemple, les solutions d'une équation différentielle linéaire forment un espace vectoriel : une combinaison linéaire de solutions en est encore une.

Un code correcteur est une façon de coder une information de manière légèrement redondante afin de pouvoir repérer et éventuellement corriger des erreurs de transmission : c'est grace à cela que l'on entend pas les rayures sur un CD. Beaucoup de codes correcteurs reposent sur de l'algèbre linéaire (sur un corps fini k dont le nombre d'éléments est une puissance de deux) : le message initial correspond à des points sur un sous-espace vectoriel et le message reçu, s'il y a des erreurs, sera en dehors de ce sous-espace ; il suffit alors de prendre le point « le plus proche » dans le sous-espace vectoriel. Ici aussi, les groupes interviennent : le groupe linéaire $\mathrm{GL}_n(k)$ et le groupe des automorphismes du corps.

Les espaces vectoriels que l'on rencontre le plus souvent sont des espaces de fonctions. Par exemple, un signal sonore peut être vu comme une fonction. L'égaliseur de votre chaîne hifi va découper ce signal en une somme de sinusoïdes, en d'autres termes, il va exprimer la fonction dans une base de sinusoïdes. Dans une telle base, on peut renforcer els aigus ou les graves, modifier le son selon sa hauteur, choses que l'on ne pouvait pas faire auparavant. Les coordonnées dans cette base constituent la transformée de Fourrier de la fonction : votre livre d'algorithmique favori vous explique comment cet algorithme est implémenté. La plupart des opérations sur un signal, comme le filtrage, *i.e.*, l'élimination du bruit, sont linéaires et s'implémentent à l'aide de matrices.

Après le son, l'image : on peut voir une image comme une fonction qui à un pixel associe sa couleur, *i.e.*, un triplet d'entiers (rouge, vert, bleu). Les fonctions qui à chaque pixel associent un triplet de nombres réels forment un espace vectoriel. Certains algorithmes de compression d'image consistent à trouver une base de cet espace vectoriel, à exprimer l'image dans cette base et à oublier les coordonnées les moins grandes (il y a donc une légère perte de qualité). On peut choisir une base constituée de fonctions sinusoïdales (JPEG) ou de choses plus compliquées (des ondelettes, MPEG3).

Applications linéaires

Les utilisations des applications linéaires sont déjà présentes dans les paragraphes précédents : les opérations de compression, de cryptage, la transformée de Fourrier sont des applications linéaires. D'autres seront détaillées dans les paragraphes suivants, car les matrices sont un moyen calculatoire de manipuler des aplications linéaires.

Résoudre une équation différentielle linéaire (ou une EDP linéaire) revient à trouver le noyau d'une application linéaire.

Matrices

Au commencement de l'ère informatique, les ordinateurs étaient utilisés par les entreprises pour résoudre des problèmes d'optimisation linéaire. Cela consiste à jongler avec les différents fournisseurs et clients, avec la nature et le volume des stocks : la situation se modélise par des inéquations linéaires (les dépenses sont inférieurs à la somme dont on dispose, le volume du stock est inférieur à celui des entrepots, etc.) et on cherche à maximiser une quantité linéaire, le profit. Résoudre ce genre de problème se ramène à des manipulations sur des matrice. En d'autres termes, même si vous décidez d'abandonner mathématiques et informatique pour devenir grossiste en fruits et légumes, l'algèbre linéaire va vous servir.

Les matrices, en tant que « tableaux de nombres », servent à étudier des objets très divers : ainsi, à un graphe, on peut associer sa matrice d'incidence. Des notions telles que l'inversibilité ou le noyau s'interprètent au niveau du graphe, en termes de connexité ou de cycles. D'autres objets mathématiques, tels les nœuds, peuvent s'étudier au travers d'une matrice.

Quand vous concevez des images de synthèse, vous commencez par décrire les objets de votre scène, puis vous les placez au bon endroit, avec la bonne orientation : il s'agit d'une transformation *affine*. On peut représenter ces applications affines comme des applications linéaires dans un espace de dimension supérieure et donc par des matrices ; la multiplication de ces matrices correspond à la composition des applications linéaires ou affines correspondantes.

Arithmétique

À savoir

- Définition du pgcd et du ppcm ;
- Théorème de Gauss ;
- Théorème de Bezout ;
- Décomposition d'un entier en produit de facteurs premiers ;
- Algorithme d'Euclide : calcul du pgcd ;
- Algorithme d'Euclide : résolution de $au + bv = d$;
- Calculs modulo n ;
- Résolution d'équations dans $\mathbb{Z}/n\mathbb{Z}$.

Ppcm et pgcd

1. Si les entiers a et b sont premiers entre eux et si $a \mid c$ et $b \mid c$, alors $ab \mid c$.

2. Soient a, b et c des entiers non nuls. Quelle relation y a-t-il entre $\text{pgcd}(a, b)$ et $\text{pgcd}(ac, bc)$?

3. Montrer que pour tous les entiers m et n,
a. $12 \mid n^4 + 4n^3 + 5n^2 - 2n$
b. $30 \mid mn(m^4 - n^4)$
c. $3804 \mid (n^3 - n)(5^{8n+4} + 3^{4n+2})$

4. Montrer que pour tout entier n,

$$\text{ppcm}(1, 2, \ldots, 2n) = \text{ppcm}(n, n+1, \ldots, n).$$

Théorème de Gauss

5. Montrer que si les entiers a et b sont premiers entre eux, alors les restes de la division euclidienne de a, $2a$,... $(b-1)a$ par b sont non nuls et distincts.

Théorème de Bezout

6. Montrer que tout entier peut s'écrire sous la forme $6a + 10b + 15c$.

7. Si a et b sont premiers entre eux, ainsi que a et c, alors a et bc sont premiers entre eux.

8. Si a et b sont premiers entre eux, alors il en va de même pour a^n et b^m, où $m, n \geqslant 1$ sont des entiers.

Décomposition d'un entier en produit de facteurs premiers

9. Montrer que si $a^2 \mid b^2$, alors $a \mid b$.

10. Si a, b et c sont des entiers, montrer
a. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
b. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
c. $(ab \wedge ac \wedge bc)(a \vee b \vee c) = |abc|$.
d. $(ab \wedge ac \wedge bc)(a \vee b \vee c) = |abc|$.

Algorithme d'Euclide

11. Calculer le pgcd et le ppcm de 639 576 et 80 652.

12. Calculer le pgcd de 58 212, 24 948, 21 954 et 13 608.

13. Calculer $\text{pgcd}(154, 700)$. Déterminer *un* couple d'entiers (a, b) tel que $154a + 700b = d$. En déduire *tous* les couples vérifiant cette équation.

14. Résoudre les équations suivantes dans $\mathbb{Z}^2$.

$$14x - 35y = 10 \qquad 14x - 35y = 28$$
$$5x + 13y = 4 \qquad 75x + 14y = 2$$

15. Soit n un entier. Calculer le pgcd et $21n + 4$ et $14n + 3$ puis celui de $n^3 + 2n$ et $n^4 + 3n^2 + 1$. Quel est le pgcd de $n^3 + 2n^2 + n - 1$ et $n - 1$?

16. On dit qu'un élément a de $\mathbb{Z}/n\mathbb{Z}$ est *inversible* s'il existe un élément b de $\mathbb{Z}/n\mathbb{Z}$ tel que $ab = \dot{1}$. Montrer que les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\dot{k}$, où k est premier à n. Comment peut-on calculer un tel inverse ?

Calculs

17. Montrer que

$$3 \mid 16^{10} - 2^{21} \times 11^9 \qquad 4 \mid 141^7 - 7^4$$
$$3 \mid 13^{22} - 2^{13} \times 5^{19} \qquad 13 \mid 2^{70} + 3^{70}.$$

Quel est le reste de la division de 1998^{1998} par 5 ? Par 7 ? Quel est le reste de la division de $19^{52} \times 23^{41}$ par 7 ? Quel est le reste de la division de $1^n + 2^n + 3^n + 4^n$ par 4 ?

18. Trouver un entier x tel que $x \equiv 2\ (7)$, $x \equiv 1\ (8)$ et $x \equiv 3\ (9)$. On peut aussi résoudre cet exercice à l'aide du théorème de Bezout et de l'algorithme d'Euclide.

19. Montrer que pour tout entier n,

$$\begin{aligned} 6 &\mid 5n^3 + n, \\ 7 &\mid 3^{2n+1} + 2^{n+2}, \\ 7 &\mid 4^{2^n} + 2^{2^n} + 1, \\ 169 &\mid 3^{3n+3} - 26n - 27, \\ n^2 &\mid (n+1)^n - 1, \\ 12 &\mid n^4 - 4n^3 + 5n^2 - 2n. \end{aligned}$$

Donner une condition sur n pour que

$$512 \mid n^{12} - n^8 - n^4 + 1.$$

20. Montrer que $\sum_{k=0}^{4}(n+k)^2$ n'est un carré pour aucune valeur de n (on pourra regarder modulo 25).
En raisonnant modulo 8, montrer que l'équation $x^n + y^n = z^n$ n'a pas de solution avec n pair et x et y impairs.

21. Montrer que si c et n sont premiers entre eux et $ca \equiv cb\ (n)$ alors $a \equiv b\ (n)$.

22. Montrer que le cube d'un entier relatif peut s'écrire sous la forme $7k$, $7k+1$ ou $7k-1$, où k est un entier.

23. Rappeler et démontrer les critères de divisibilité par 3 et 9. Quel est le reste de la division de 123456789101112131415 par 7 ?

24. Trouver tous les entiers n tels que $2^n + 3^n$ soit un multiple de 7.

Équations modulaires

25. Dresser les tables d'addition et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 2$, $n = 4$, $n = 5$, $n = 6$. De manière générale, dans $\mathbb{Z}/n\mathbb{Z}$, peut-on « simplifier par x » dans l'équation $xa = xb$?

26. Résoudre les équations suivantes dans $\mathbb{Z}$.

$$\begin{aligned} 5x &\equiv 12 \quad (7), \\ 2x &\equiv 2 \quad (4), \\ 4x &\equiv 9 \quad (8). \end{aligned}$$

27. Donner une condition nécessaire et suffisante sur les entiers a, b et n pour que l'équation $ax \equiv b\ (n)$ ait des solutions.

28. Résoudre les systèmes suivants dans $\mathbb{Z}/7\mathbb{Z}$ puis dans $\mathbb{Z}/6\mathbb{Z}$.

$$\begin{cases} \dot{2}x + \dot{3}y = \dot{1} \\ x + \dot{4}y = \dot{4} \end{cases} \qquad \begin{cases} x + \dot{5}y = \dot{1} \\ \dot{4}x + \dot{2}y = \dot{3} \end{cases}$$

29. Résoudre les équations suivantes.

$$\begin{aligned} x^2 - \dot{2}x - \dot{2} &= \dot{0} && \text{dans } \mathbb{Z}/5\mathbb{Z}, \\ 2x^3 - 3x - 2 &\equiv 0 \quad (7) && \text{dans } \mathbb{Z}, \\ x^2 - x - \dot{1} &= \dot{0} && \text{dans } \mathbb{Z}/5\mathbb{Z}, \\ x^2 &= \dot{1} && \text{dans } \mathbb{Z}/18\mathbb{Z}, \\ x^2 - \dot{2}x + \dot{2} &= \dot{0} && \text{dans } \mathbb{Z}/5\mathbb{Z}, \\ x^2 - \dot{4}x + \dot{3} &= \dot{0} && \text{dans } \mathbb{Z}/143\mathbb{Z}, \\ x^2 - \dot{4}x + \dot{3} &= \dot{0} && \text{dans } \mathbb{Z}/(503 \times 509)\mathbb{Z}. \end{aligned}$$

Divers

30. Les assertions suivantes sont-elles exactes ?
« Si n divise un produit d'entiers, alors il divise l'un d'eux. »
« La relation “a et b sont premiers entre eux” est une relation d'équivalence. »
« $2\mathbb{Z} + 3\mathbb{Z} = 5\mathbb{Z}$. »

31. On veut résoudre $x^2 + y^2 = z^2$ dans $\mathbb{Z}^3$.
a. Trouver une solution particulière non nulle.
b. Montrer que l'on peut se ramener au cas où x, y et z sont premiers entre eux. Montrer qu'ils sont alors premiers deux à deux.
c. En raisonnant modulo 4, montrer que si (x, y, z) est une solution vérifiant l'hypothèse précédente, alors x et y sont de parités différentes. Montrer que l'on peut supposer x pair et y impair.
d. Sous les hypothèses précédentes, montrer que $(z + y)/2$ et $(z - y)/2$ sont des entiers, premiers entre eux. En déduire que ce sont des carrés parfaits, notés u^2 et v^2.
e. Conclure.

32. On cherche les triplets d'entiers (x, y, z) premiers deux à deux tels que
$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x}$$
soit un entier, noté m. Montrer que x, y et z sont tous égaux à 1 en valeur absolue. Montrer que l'on a nécessiarement $m = 3$. Conclure.

33. On cherche tous les couples d'entiers (n, p) tels que $3^n = p^2 + 8$. En raisonnant modulo 8, montrer que nécessairement n est pair et p impair. En déduire $(p+1)^2 \leqslant p^2 + 8$. Conclure.

34. (Théorème de Wilson) Montrer que si p est premier, alors $(p - 1)! \equiv -1 \ (p)$. (On pensera à regrouper chaque entier avec son inverse modulo p.)

35. (Théorème de Fermat) Montrer que pour tout nombre premier p et tout entier a premier à p, on a $a^{p-1} \equiv 1 \ (p)$. On pourra utiliser l'exercice 5 pour montrer que
$$(p-1)!a^{p-1} \equiv (p-1)! \quad (p).$$
L'un des algorithmes de cryptographie les plus simples est le suivant. On choisit un nombre premier p et un entier e premier à $p - 1$. Grace à l'algorithme d'Euclide, on peut trouver un inverse d de e modulo $p - 1$. Le cryptage s'effectue en remplaçant un entier T (inférieur à p) par $T^e \bmod p$ et le décryptage en remplaçant un entier C par $C^d \bmod p$. Vérifier que cela marche.
(On utilise aussi le théorème de Fermat pour concevoir des tests probabilistes de primalité : si $a^{p-1} \not\equiv 1 \ (p)$, alors p n'est pas premier. Réciproquement, si c'est congru à 1, il y a « des chances » pour que p soit premier.)

36. (Théorème de Fermat) **a.** Montrer que si p est premier et divise le produit ab, alors il divise a ou b.
b. Soit p un nombre premier et $1 \leqslant q < p$. Montrer que p et $q!$ sont premiers entre eux.
c. Montrer que $C_p^q = \binom{p}{q}$ est divisible par p.
d. En déduire que $(a+b)^p - a^p - b^p$ est divisible par p, pour tous entiers a et b.
e. Montrer que $2^p - 2$ est divisible par p.
f. Montrer que $k^p - k$ est divisible par p pour tout entier k. En déduire que $p \mid k^{p-1} - 1$ si $1 \leqslant k < p$.

37. (Théorème d'Euler) Notons $\varphi(n)$ le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Montrer que si les entiers a et n sont premiers entre eux, alors $a^{\varphi(n)} \equiv 1 \ (n)$. On pourra pour cela remarquer que
$$\prod_{b \wedge n = 1} ab \equiv \prod_{b \wedge n = 1} b \quad (n).$$
En prenant $n = pq$ un produit de deux nombres premiers, en déduire un algorithme de cryptographie à clef publique (RSA). On remarquera que $\varphi(n) = (p - 1)(q - 1)$.

38. Notons $\varphi(n)$ le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Montrer que si p est un nombre premier, alors $\varphi(p^k) = p^k - p^{k-1}$. Montrer que si m et n sont premiers entre eux, alors on a un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, puis montrer que $\varphi(mn) = \varphi(m)\varphi(n)$. En déduire l'expression de $\varphi(n)$ pour un entier n quelconque.

Groupes, anneaux, corps

À savoir

- Reconnaître un groupe, un sous-groupe, un morphisme de groupes ;
- « Faire des calculs » dans un groupe ;
- Décomposer une permutation en produit de cycles ;
- Connaître des exemples de groupes : $\mathfrak{S}_n$, $\mathfrak{S}(X)$, $\mathrm{GL}_n(k)$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{S}^1$;
- Connaître des exemples d'anneaux : $\mathbb{Z}/n\mathbb{Z}$, $k[X,Y,Z]$, $\mathscr{M}_n(k)$;
- Connaître des exemples de corps : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, $k(X)$.

Groupes

1. Montrer que l'intervalle $I =]-1;1[$ muni de la loi

$$* : \left\{ \begin{array}{ccc} I \times I & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x * y = \dfrac{x+y}{1+xy} \end{array} \right.$$

est un groupe abélien.

2. Montrer que l'on définit un groupe sur $E = \mathbb{R}^\times \times \mathbb{R}$ par

$$* : \left\{ \begin{array}{ccc} E \times E & \longrightarrow & E \\ ((a,b),(a',b')) & \longmapsto & (aa', ab'+b). \end{array} \right.$$

Est-il commutatif ? $\mathbb{R}^\times \times \{0\}$ est-il un sous-groupe ?

3. La loi de composition interne

$$* : \left\{ \begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (a,b) & \longmapsto & ab - 2(a+b) + 6 \end{array} \right.$$

est-elle commutative ? Associative ? Montrer qu'il existe un élément neutre. Quels sont les éléments qui possèdent un inverse ? Quels sont les éléments qui sont leur propre inverse ?

4. Montrer que $\mathbb{R}^2$ est un groupe si on le munit de la loi

$$\left\{ \begin{array}{ccc} \mathbb{R}^2 \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y,x',y') & \longmapsto & (x+x', ye^{x'} + y'e^{-x}). \end{array} \right.$$

5. Montrer que $E = \mathbb{R}^\times \times \mathbb{R}$ est un groupe si on le munit de la loi

$$\left\{ \begin{array}{ccc} E \times E & \longrightarrow & E \\ ((x,y),(x',y')) & \longmapsto & (xx', xy' + y'^n). \end{array} \right.$$

6. Donner une condition nécessiare et suffisante sur a, b et c pour que $\mathbb{R}$ soit un groupe si on le munit de la loi

$$\left\{ \begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & a(x+y) + bxy + c. \end{array} \right.$$

7. Obtient-on un groupe en munissant $\mathbb{Z}^3$ du produit

$$(a,b,c) * (x,y,z)) = (a + (-1)^b x, b + (-1)^c y, c + (-1)^a z)\ ?$$

8. Montrer que $(\mathbb{R}, \circ)$, où on note $x \circ y = \sqrt{x^5 + y^5}$, est un groupe isomorphe à $(\mathbb{R}, +)$.

Exemples de groupes

9. Soit $(G, \cdot, e)$ un groupe. Montrer que si $xy = z$ avec $x \neq e$ et $y \neq e$, alors $z \neq x$ et $z \neq y$. En déduire que la table de la loi d'un groupe contient dans chaque ligne et chaque colonne une fois et une seule tout élément de G. Écrire toutes les tables possibles pour un groupe à 3 et 4 éléments : montrer qu'il s'agit, à isomorphisme près, de $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Auquel de ces groupe $((\mathbb{Z}/5\mathbb{Z})^\times, \times)$ est-il isomorphe ?

10. Montrer que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Réciproquement, montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme. On pourra considérer le plus petit élément positif non nul n de ce sous-groupe et effectuer la division euclidienne par un élément quelconque a de ce sous-groupe.

11. Montrer que $\dot{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si il existe un entier q tel que $q\dot{k} = \dot{1}$. En déduire que $\dot{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.

12. **a.** Montrer que $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$ est un groupe. (On rapelle qu'il s'agit des éléments *inversibles* de $\mathbb{Z}/n\mathbb{Z}$.)
b. Plus généralement, monter que les éléments inversibles d'un anneau A forment un groupe $A^{\times}$.
c. Montrer que les nombres complexes de module un forment un groupe, que nous noterons $\mathbb{S}^1$.
d. Montrer que tout sous-groupe fini de $\mathbb{C}$ est un sous-groupe de $\mathbb{S}^1$.

13. **a.** Soient G et H deux groupes. Montrer que $G \times H$ devient un groupe si on le munit de la loi $(g,h) * (g',h') = (gg',hh')$.
b. Soit $(G,\cdot)$ un groupe, montrer que la loi

$$x * y = y \cdot x$$

fait de $(G,*)$ un groupe, isomorphe à $(G,\cdot)$.

14. **a.** Montrer que des morphismes $\varphi : G \longrightarrow H$ et $\psi . G \longrightarrow K$ permettent de définir un morphisme $\chi : G \longrightarrow H \times K$.
b. Montrer que $\operatorname{Ker}\chi = \operatorname{Ker}\varphi \cap \operatorname{Ker}\psi$.

15. Action d'un groupe. Définition. Exemples ?
a. Montrer qu'une action de G sur X induit une action de G sur $\mathscr{F}(X,Y)$ et sur $\mathscr{F}(Y,X)$.

16. **(Produit semi-direct)** Nous étudions le groupe G des isométries directes du plan, qui comporte les translations et les rotations.
a. Montrer que l'ensemble H des translations forme un sous-groupe distingué de G.
b. Montrer que l'ensemble K des rotations de centre O forme un sous-groupe de G. Est-il distingué ? Montrer que $H \cap K = \{\operatorname{Id}\}$.
c. Montrer que tout élément de G peut s'écrire de manière unique comme produit d'un élément de H et d'un élément de K. Peut-on dire que le groupe G est isomorphe à $H \times K$?
d. La bijection entre G et $H \times K$ induit une loi de groupe sur $H \times K$. La décrire.
e. Soient H et K des groupes et $\varphi : K \longrightarrow \operatorname{Aut} H$ un morphisme. Montrer que l'on définit bien une loi de groupe sur $H \times K$ par $(h,k)(h',k') = (h\sigma_k(h'),kk')$. Quel est le rapport avec les questions précédentes ?

Exemples géométriques

17. Montrer que les racines $n^{\text{ièmes}}$ de l'unité forment un sous-groupe de $(\mathbb{C}^{\times}, \times)$. Construire un morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans ce groupe. Montrer que c'est un isomorphisme.

18. Montrer que l'ensemble des applications de la forme

$$f_{a,b} : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax+b \end{array} \right.$$

forme un sous-groupe du groupe des bijections de $\mathbb{R}$. Montrer que les applications de la forme $f_{1,b}$ forment un sous-groupe du précédent.

19. Il n'y a que quatre isométries du plan qui fixent un ensemble de deux points distincts : lesquelles ? Montrer qu'elles forment un sous-groupe abélien du groupe des bijections du plan. Nous avons vu qu'il n'existe que deux groupes à quatre éléments : duquel s'agit-il ?

20. Il n'y a que six isométries du plan qui fixent un triangle équilatéral : lesquelles ? Montrer qu'elles forment un sous-groupe du groupe des bijections du plan. Donner sa table.

21. **a.** En remarquant qu'une isométrie du plan est entièrement déterminée par l'image de trois points non alignés, montrer qu'il n'y a que huit isométries du plan qui fixent un carré : lesquelles ?
b. Montrer qu'elles forment un sous-groupe G du groupe des bijections du plan. Donner sa table.
c. Montrer que la restriction des éléments de G aux coins du carré définit un morphisme de groupes injectif vers $\mathfrak{S}_4$.
d. Décrire l'ensemble ordonné (par l'inclusion) des sous-groupes de G. Quels sont les

sous-groupes abéliens ? Certains d'entre-eux ont quatre éléments : sont-ils isomorphes à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

22. Reprendre les exercices précédents dans l'espace, avec le tétraèdre puis le cube.

Calculs dans un groupe

23. Soit $(G, \cdot, e)$ un groupe tel que
$$\forall x \in G, \quad x \cdot x = e.$$
Montrer qu'il est commutatif.

24. Soient a, b des éléments d'un groupe $(G, \cdot, e)$.
a. Montrer que si $a^5 = b^4 = e$ et $ab = ba^3$, alors $a^2b = ba = et = ab^3 = b^3a^2$.
b. Montrer que si $(ab)^{-1} = a^{-1}b$ et $(ba)^{-1} = b^{-1}a$, alors $a^2 = b^2$ et $a^2b^2 = e$.
c. Montrer que si $b^6 = e$ et $ab = b^4a$, alors $b^3 = e$ et $ab = ba$. Pour cela, on pourra regarder $(aba^{-1})^3$.
d. Montrer que si $a^5 = e$ et $aba^{-1} = b^2$, alors $b^{31} = e$. On commencera par calculer b^{32}.

25. Soient a et b des éléments d'un groupe G. L'*ordre* de a est le plus petit entier (positif, non nul) n tel que $a^n = e$ ou l'infini.
a. Montrer que si a, b et ab sont d'ordre 2, alors a et b commutent.
b. Montrer que si a est d'ordre fini, alors a^{-1} et bab^{-1} le sont aussi, avec le même ordre que a.
c. Montrer que si ab est d'ordre fini, alors ba aussi, avec le même ordre.
d. Si a est d'ordre n et si $f : G \longrightarrow H$ est un morphisme de groupes, alors $f(a)$ est d'ordre fini divisant n.
e. Quels sont les morphismes de groupe $\mathbb{Z}/7\mathbb{Z} \longrightarrow \mathbb{Z}/13\mathbb{Z}$?

Sous-groupes

26. a. Décrire l'ensemble ordonné (par l'inclusion) des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.
b. Donner tous les sous-groupes de $\mathfrak{S}_4$ (?).
c. Donner tous les sous-groupes de $(\mathbb{Z}, +)$.
d. Donner tous les sous-groupes finis de $(\mathbb{C}^\times, \times)$.

27. Montrer que tout groupe G s'identifie à un sous-groupe de $\mathfrak{S}(G)$.

28. Montrer que tout élément d'un groupe fini est d'ordre fini.

29. Soit G un groupe et A une partie de G.
a. Montrer que le centre de G,
$$Z(G) = \{\, x \in G \;:\; \forall y \in G \;\; xy = yx \,\}$$
est un sous-groupe.
b. Montrer que le commutateur de A,
$$Z_A(G) = \{\, x \in G \;:\; \forall y \in A \;\; xy = yx \,\}$$
est un sous-groupe.
c. Montrer que le normalisateur de A,
$$N_A(G) = \{\, x \in G \;:\; xA = Ax \,\}$$
est un sous-groupe.
d. Montrer que si G est *abélien*, alors les éléments d'ordre fini
$$F(G) = \{\, x \in G \;:\; \exists n \in \mathbb{N}^\times \;\; x^n = e \,\}$$
forment un sous-groupe.
e. Montrer que l'image d'un sous-groupe par un morphisme de groupes est encore un sous-groupe. Montrer que l'image réciproque d'un sous-groupe par un morphisme de groupes est encore un sous-groupe.

30. (Sous-groupes distingués) Un sous-groupe H de G est *distingué* si pour tout $x \in H$, on a $xH = Hx$.
a. Montrer qu'un sous-groupe est dintingué si et seulement si il est stable par tous les automorphismes intérieurs.
b. Quels sont les sous-groupes distingués d'un groupe commutatif?
c. Montrer que si $xH \subset Hx$ pour tout $x \in G$, alors H est distingué.
d. Parmi les sous-groupes de l'exercice précédent, quels sont ceux qui sont distingués?
e. Montrer que le groupe dérivé
$$D(G) = \langle\, xyx^{-1}y^{-1} \;:\; x, y \in G \,\rangle$$
est un sous-groupe distingué.

f. Montrer que le noyau d'un morphisme de groupes, *i.e.*, l'image réciproque de l'élément neutre, est un sous-groupe distingué.
g. Réciproquement, soit H un sous-groupe distingué de G. Considérons la relation sur G définie par $x\mathscr{R}y$ si et seulement si $xy^{-1} \in H$. Montrer qu'il s'agit d'une relation d'équivalence. On notera G/H le quotient de G par $\mathscr{R}$: montrer que c'est un groupe. Vérifier que l'application $G \longrightarrow G/H$ est un morphisme de groupes, de noyau H.

31. Si H et K sont des sous-groupes de G, montrer que HK est un sous-groupe si et seulement si $HK = KH$. Montrer qu'il suffit en fait de demander que $HK \subset KH$.

32. Si A est une partie *finie* non vide de G stable par la loi, alors c'est un sous-groupe.

33. (Théorème de Lagrange) Si G est un groupe fini, on veut montrer que l'ordre d'un sous-groupe H divise celui de G.
a. Montrer que la relation sur G définie par $x\mathscr{R}y$ si $xy^{-1} \in H$ est une relation d'équivalence.
b. Montrer que les classes d'équivalence ont toutes le même cardinal.
c. En déduire que
$$\operatorname{Card} G = \operatorname{Card} H \times \operatorname{Card}(G/\mathscr{R}).$$
Conclure.
d. En utilisant le théorème de Lagrange, montrer que tout groupe fini d'ordre un nombre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
e. Soit G un groupe d'ordre impair, montrer (en utilisant le théorème de Lagrange) que l'application
$$f : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^2 \end{array} \right.$$
est bijective. Ce n'est pas un morphisme de groupes. Montrer que l'on définit une nouvelle loi de groupe par $x * y = f(f^{-1}(x)f^{-1}(y))$.
f. Soit p un nombre premier. Montrer, à l'aide du théorème de Lagrange, que tout groupe d'ordre p^n possède un élément d'ordre p.

34. Soient H et K des sous-groupes d'ordre fini d'un groupe G tels que $H \cap K = \varnothing$. Montrer que $\operatorname{Card}(HK) = \operatorname{Card} H \operatorname{Card} K$.

35. Soient p et q des nombres premiers entre eux et $n = pq$. Soit G un groupe fini tel que $\forall x \in G,\ x^n = 1$. On pose
$$H = \{\, x \in G \ :\ x^p = 1 \,\},$$
$$K = \{\, x \in G \ :\ x^q = 1 \,\}.$$
Montrer que ce sont des sous-groupes et que l'on a un isomorphisme
$$\varphi : \left\{ \begin{array}{ccc} H \times K & \longrightarrow & G \\ (x,y) & \longmapsto & xy. \end{array} \right.$$

Morphismes de groupes

36. (Transport de structure) Soit $(G, \cdot)$ un groupe, $(H, *)$ un ensemble muni d'une loi de composition interne et $\varphi : G \longrightarrow H$ une bijection telle que
$$\forall x, y \in G \qquad \varphi(x \cdot y) = \varphi(x) * \varphi(y).$$
Montrer que $(H, *)$ est un groupe.

37. a. Décrire $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z})$.
b. Décrire $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.
c. Décrire $\operatorname{Hom}(\mathbb{Z}/n, \mathbb{Z})$.
d. Décrire $\operatorname{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.
e. Décrire $\operatorname{Hom}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z})$.
f. Décrire $\operatorname{Hom}(\mathbb{Z}, G)$, où G est un groupe.
g. Décrire $\operatorname{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$.
h. Décrire $\operatorname{Hom}(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \mathbb{Z}/c\mathbb{Z})$.
i. Décrire $\operatorname{Hom}(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, G)$.

38. Soit $\varphi : G \longrightarrow G'$ un isomorphisme.
a. Montrer que G est fini si et seulement si G' l'est et qu'ils ont le même ordre.
b. Montrer que G est abélien si et seulement si G' l'est.
c. Montrer que G est monogène si et seulement si G' l'est.
d. Montrer que $x \in G$ est d'ordre fini si et seulement si $\varphi(x)$ l'est, et qu'ils ont alors le même ordre.
e. Montrer que l'ensemble (ordonné) des sous-groupes de G est en bijection avec l'ensemble (ordonné) des sous-groupes de G'.

f. Donner d'autres exemples de propriétés préservées par isomorphisme.

39. Les groupes suivants sont-ils isomorphes ?
a. $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
b. $\mathfrak{S}_3$ et $\mathbb{Z}/3\mathbb{Z}$.
c. $\mathfrak{S}_3$ et $\mathbb{Z}/6\mathbb{Z}$.
d. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.
e. $(\mathbb{R}, +)$ et $(\mathbb{R}_+^\times, \times)$.
f. Trouver deux groupes entre lesquels il existe *plusieurs* isomorphismes.

40. On dit qu'un groupe est *cyclique* s'il est isomorphe à un groupe de la forme $\mathbb{Z}/n\mathbb{Z}$. À quelle condition un produit de deux groupes cycliques est-il cyclique ?

41. Montrer que les notions suivantes, concernant un groupe G et des sous-groupes H et K, sont différentes. Y a-t-il quelques implications entre certaines d'entre-elles ?
a. Les sous-groupes H et K sont isomorphes.
b. Il existe un automorphisme de G induisant un isomorphisme entre H et K.
c. Les sous-groupes H et K sont conjugués, *i.e.*, il existe un automorphisme intérieur de G induisant un isomorphisme entre H et K.
d. Les sous-groupes H et K sont égaux.

42. Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes surjectif.
a. Montrer que si G est cyclique, alors il en va de même pour G'.
b. Montrer que si G est abélien, alors G' aussi.
c. Montrer que si N est un sous-groupe distingué de G, alors $\varphi(N)$ est un sous-groupe distingué de G'.
d. Montrer que l'on a une correspondance bijective entre les sous-groupes de G' et les sous-groupes de G qui contiennent le noyau de φ. Expliciter cette correspondance pour le morphisme canonique $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$. Montrer que l'on a une correspondance bijective entre les sous-groupes distingués de G' et les sous-groupes distingués de G qui contiennent le noyau de φ.

43. a. Si X est un ensemble, montrre que ses bijections forment un groupe. Si G est un groupe, montrer que ses automorphismes forment un sous-groupe du groupe de ses bijection, que nous noterons $(\operatorname{Aut} G, \circ)$.
b. Décrire le groupe des automorphismes de $(\mathbb{Z}, +)$.
c. Décrire $\operatorname{Aut} \mathbb{Z}/10\mathbb{Z}$.
d. Décrire $\operatorname{Aut} \mathfrak{S}_3$.
e. Déterminer $\operatorname{Aut} \mathbb{H}_8$.

44. Le groupe $\mathfrak{S}_3$ est-il isomorphe à un produit de deux groupes non triviaux ?

45. Soit G un groupe. Montrer que l'application

$$\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array} \right.$$

est bijective. À quelle condition sur G est-elle un automorphisme ?

46. Montrer que si G et H sont des groupes finis d'ordres permiers entre eux, alors $\operatorname{Hom}(G, H) = \{0\}$.

47. Montrer que le noyau d'un morphisme de groupes est réduit à l'élément neutre si et seulement si ce morphisme est injectif.

48. a. Montrer que les automorphismes de G forment un groupe $\operatorname{Aut} G$. Montrer qu'il s'agit d'un sous-groupe du groupe $\mathfrak{S}(G)$ des bijections de G.
b. Si a est un élément de G, on définit l'*automorphisme intérieur* associé à a par

$$i_a : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & axa^{-1}. \end{array} \right.$$

Vérifier que c'est bien un automorphisme de groupes.
c. Montrer que les automorphismes intérieurs forment un sous-groupe $\operatorname{Int} G$ du groupe des automorphismes de G.
d. Montrer que l'on a un morphisme de groupes $G \longrightarrow \operatorname{Int} G$. Quel est son noyau ?

49. Si G est un groupe abélien fini, on note $G' = \operatorname{Hom}(G, \mathbb{C}^\times)$. Montrer que c'est un groupe. Déterminer $(\mathbb{Z}/4\mathbb{Z})'$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})'$.

Groupe symétrique

50. Dans $\mathfrak{S}_9$, décomposer la permutation
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 6 & 2 & 4 & 1 & 5 & 9 \end{pmatrix}$$
en produit de cycles à support disjoint. Quel est son ordre? Calculer σ^{1998}.

51. Montrer que l'élévation au cube dans $\mathbb{Z}/11\mathbb{Z}$ en est une permutation. Quel est son ordre?

52. Montrer que $\mathfrak{S}_p$ est (isomorphe à) un sous-groupe de $\mathfrak{S}_q$ si $p \leqslant p$.

53. Montrer que le sous-groupe des bijections de $\mathbb{R} \cup \{\infty\}$ engendré par $x \longmapsto 1/x$ et $x \longmapsto (x-1)/x$ est isomorphe à $\mathfrak{S}_3$.

54. Montrer que l'ordre d'un produit de deux transpositions est inférieur à trois.

55. Donner deux 4-cycles de $\mathfrak{S}_4$ qui ne commutent pas.

56. Montrer que si $n \geqslant 3$, le centre de $\mathfrak{S}_n$ est trivial.

57. Montrer que deux cycles commutent si et seulement si leurs supports sont disjoints.

58. Quel est l'ordre maximal d'un élément de $\mathfrak{S}_5$?

59. (Signature) La *signature* d'une permutation $\sigma \in \mathfrak{S}_n$ est définie par
$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$
a. Montrer que l'on définit ainsi un morphisme de groupes vers $(\{\pm 1\}, \times)$.
b. Montrer que $\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$, où $\nu(\sigma)$ est le nombre d'inversions de σ, *i.e.*, le nombre de couples (i, j) avec $i < j$ et $\sigma(i) > \sigma(j)$.
c. Énumérer tous les éléments de $\mathfrak{S}_3$ et donner leur signature. Faire de même avec quelques éléments de $\mathfrak{S}_5$.
d. Montrer qu'un cycle est pair, *i.e.*, de signature égale à $+1$, si et seulement si il est de longueur impaire.
e. Montrer qu'une permutation est impaire si et seulement si sa décomposition en produit de cycles de supports disjoints contient un nombre impair de cycles de longueur paire.

60. Soit σ un cycle de longueur n dans $\mathfrak{S}_n$. Montrer que l'ensemble des permutations qui commutent avec σ est le sous-groupe engendré par σ. Que se passerait-il si σ était un cycle de longueur inférieure à n?

61. a. Montrer que $\mathfrak{S}_n$ est engendré par les transpositions (12), (23),...,$(n\ n-1)$.
b. Montrer que $\mathfrak{S}_n$ est engendré par les transpositions (12), (13),...,$(1\ n-1)$.
c. Montrer que $\mathfrak{S}_n$ est engendré par la transposition (12) et par le cycle $(123\cdots n)$.

Anneaux

62. Montrer que l'on peut munir $\mathscr{F}(\mathbb{R}, \mathbb{R})$ de deux structures d'anneau différentes, en prenant pour produit, la multiplication de $\mathbb{R}$ ou la composition des applications. Sont-ils commutatifs? Sont-ils intègres? Sont-ils isomorphes?
a. Donner un exemple d'anneau possédant des éléments a et b tels que $ab = 1$ et $ba \neq 1$.

63. a. Montrer que l'ensemble des endomorphismes d'un anneau A, avec pour addition et multipication celles induites par A, forment un anneau.
b. Montrer que l'ensemble des endomorphismes d'un anneau A, avec pour addition celle induite par A et pour multiplication la composition des morphismes, forment un anneau.

64. Montrer que les polynômes à trois indéterminées sur un corps k forment un anneau commutatif, noté $k[x, y, z]$. Est-il intègre?

65. Montrer que les nombres décimaux forment un anneau. Est-il intègre? Est-ce un corps? Quels sont ses éléments inversibles?

66. **a.** Montrer que
$$A = \mathbb{Z}[\sqrt{2}] = \{\, a + b\sqrt{2} \ : \ a, b \in \mathbb{Z} \,\}$$
est un anneau.
b. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que $N(0) = 0$ et que pour tous x, $y \in A$, on a $N(xy) = N(x)N(y)$.
c. Montrer que $a + b\sqrt{2} = 0$ si et seulement si $a = b = 0$. En déduire que A est intègre.
d. Montrer que x est inversible si et seulement si $N(x) = 1$. (On ne cherchera pas les éléments inversibles : il y en a une infinité.)
e. Montrer que pour tous $x, y \in A$, $x \neq 0$, il existe $q, r \in A$ tels que $x = qy + r$ et $|N(r)| < |N(y)|$. Définir une notion de pgcd dans A et calculer $\mathrm{pgcd}(3 + 2\sqrt{2}, 2 + \sqrt{2})$.

67. **a.** Reprendre l'exercice précédent avec A=$\mathbb{Z}[i]$ (ou $B = \mathbb{Z}[i\sqrt{5}]$), en changeant la définition de N. Quels sont les éléments inversibles?
b. On dit qu'un élément de B est premier s'il n'est pas inversible et s'il ne peut pas s'écrire comme produit de deux éléments non inversibles. Montrer que tout élément non inversible de B peut s'écrire comme produit d'éléments premiers. Cette décomposition est-elle unique?

68. Soit A un anneau. Montrer qu'il existe un unique morphisme d'anneaux $\mathbb{Z} \longrightarrow A$.

69. Dans $\mathbb{Z}/n\mathbb{Z}$, quels sont les éléments inversibles? réguliers? diviseurs de zéro? nilpotents?

70. **a.** Montrer que les séries formelles à une indéterminée sur un corps k commutatif forment un anneau $k[[x]]$. Quels sont ses éléments inversibles?
b. Reprendre la question si k n'est plus un corps mais simplement un anneau commutatif.

71. **(Multinôme)** **a.** Soient a et b des éléments *qui commutent* dans un anneau A. Montrer que pour tout entier n,
$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$
b. Soient $a_1, \ldots, a_p$ des éléments de A qui commutent. Montrer que
$$(a_1 + \cdots + a_p)^n = \sum_{k_1 + \cdots + k_p = n} \frac{n!}{k_1! \cdots k_p!} a_1^{k_1} \cdots a_p^{k_p}.$$

72. Soit A un anneau dont tout élément est égal à son carré. Montrer que le double de tout élément est égal à zéro. En déduire que l'anneau est commutatif.

73. **(Anneau produit)** Soient A et B des anneaux. Montrer que les deux lois sur $A \times B$ par
$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) * (a', b') = (aa', bb').$$
définissent bien une structure d'anneau.

74. Soit A un anneau commutatif. Notons $B = \{\, x \in A \ : \ x^2 = x \,\}$. Montrer que si $x \in B$, alors $1 - x \in B$. Montrer que $(B, \oplus, \cdot)$, où $x \oplus y = x + y - 2xy$, est un anneau commutatif (unitaire).

75. Montrer que tout anneau intègre *i.e.*, sans diviseur de zéro, *i.e.*, dans lequel
$$\forall a, b \in A \qquad ab = 0 \implies a = 0 \text{ ou } b = 0,$$
et *fini* est un corps. On pourra pour cela remarquer que les applications
$$\begin{cases} A & \longrightarrow & A \\ x & \longmapsto & xy \end{cases}$$
sont bijectives.

76. **a.** Montrer qu'il n'existe pas de morphisme d'anneaux $\mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}]$.
b. Montrer que si les anneaux A et B sont isomorphes, alors il en va de même des anneaux de polynômes $A[X]$ et $B[X]$.
c. Soit $P \in \mathbb{R}[X]$ un polynôme ; montrer que l'application $\mathbb{R}[X, Y] \longrightarrow \mathbb{R}[X, Y]$ définie par $\varphi(X) = X + P(Y)$ et $\varphi(Y) = Y$ est un automorphisme.

d. Soient A et B des anneaux. Les applications suivantes sont-elles des morphismes ?

$$\begin{array}{ll} A \longrightarrow A\times B & a \longmapsto (a,0) \\ A \longrightarrow A\times A & a \longmapsto (a,a) \\ A\times A \longrightarrow A & (a,b) \longmapsto a+b \\ A\times A \longrightarrow A & (a,b) \longmapsto ab \end{array}$$

e. Les anneaux $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ sont-ils isomorphes ? Et les anneaux $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$?

f. Soit p un nombre premier et A un anneau commutatif dans lequel $p1 = 1+\cdots+1 = 0$. Montrer que l'application $A\longrightarrow A$ définie par $\varphi(x) = x^p$ est un morphisme.

g. Décrire le groupe des automorphismes de l'anneau $\mathbb{Z}[X]$.

77. Vérifier que les applications suivantes sont des morphismes d'anneaux et trouver leur noyau.

a. $\left\{\begin{array}{ccc} \mathbb{R}[X,Y] & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(0,0). \end{array}\right.$

b. $\left\{\begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ f & \longmapsto & f(2+i). \end{array}\right.$

c. $\left\{\begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(\sqrt{2}). \end{array}\right.$

d. L'application $\mathbb{C}[X,Y,Z]\longrightarrow\mathbb{C}[T]$ définie par $\varphi(X)=T$, $\varphi(Y)=T^2$ et $\varphi(Z)=T^3$.

e. L'application $\mathbb{C}[X,Y]\longrightarrow\mathbb{C}[T]$ définie par $\varphi(X)=T^2$ et $\varphi(Y)=T^3$.

78. (Idempotents) Un élément *idempotent* d'un anneau est un élément égal à son carré. On remarque que dans un produit d'anneau $A\times B$, l'élément $(1,0)$ est idempotent. Démontrons la réciproque.

a. Montrer que si e est idempotent, alors $e' = 1-e$ aussi.

b. Montrer que (e) est un anneau. Est-ce un sous-anneau de A ?

c. Montrer que $A\simeq (e)\times(e')$.

79. (Idéaux) On dit qu'une partie I d'un anneau A est un *idéal* si c'est un sous-groupe additif et si

$$\forall x\in I \qquad \forall y\in A \qquad xy\in A.$$

a. Soit x un élément d'un anneau A. Montrer que l'ensemble (x) de xy, où $y\in A$ est un idéal. Montrer que c'est le plus petit idéal de A contenant x.

b. Quels sont les idéaux de l'anneau $\mathbb{Z}$?

c. Quels sont les idéaux de l'anneau $\mathbb{R}[X]$?

d. Montrer que les éléments *nilpotents* d'un anneau commutatif, *i.e.*, les éléments dont une puissance est nulle, forment un idéal.

e. Montrer qu'un idéal contenant l'unité est l'anneau tout entier.

f. Montrer qu'un idéal contenant un élément inversible est l'anneau tout entier.

g. Montrer si x est nilpotent dans l'anneau A, alors $1-x$ est inversible.

h. Montrer que le noyau d'un morphisme d'anneaux est un idéal.

i. Réciproquement, soit I un idéal d'un anneau A. Montrer que la relation sur A définie par $x\mathscr{R}y \equiv x-y\in I$ est une relation d'équivalence. Montrer que le quotient $A/\mathscr{R}$ est un anneau, et que l'application $A\longrightarrow A/\mathscr{R}$ est un morphisme d'anneaux de noyau I.

j. Soient I et J des idéaux de A. Montrer que $I\cup J$ n'est pas un idéal. Montrer que

$$I+J = \{\, x+y,\ \text{où } x\in I \text{ et } y\in J \,\}$$

est un idéal.

k. Montrer que $I\cap J$ est un idéal.

l. On suppose désormais A commutatif, jusqu'à la fin de l'exercice. Montrer que $\{xy, x\in I, y\in J\}$ n'est pas un idéal. Monter que l'ensemble IJ des sommes de produits d'un élément de I et d'un élément de J est un idéal.

m. Montrer que $IJ\subset I\cap J$. Montrer qu'il n'y a pas égalité en général.

n. Décrire les idéaux $n\mathbb{Z}\cap m\mathbb{Z}$, $n\mathbb{Z}+m\mathbb{Z}$ et $(n\mathbb{Z})(m\mathbb{Z})$ de $\mathbb{Z}$.

80. Soit A un anneau contenant $\mathbb{Q}$ comme sous-anneau et $x\in A$ un élément nilpotent, *i.e.*, dont une puissance est nulle ; on définit

$$\exp(x) = \sum_{n\geqslant 0}\frac{x^n}{n!}.$$

(On remarquera que comme x est nilpotent, la somme est finie.) Montrer que si x et y sont nilpotents et *commutent*, alors $\exp(x+y) = \exp(x)\exp(y)$. En déduire que $\exp x$ est inversible.

Corps

81. Montrer que $\mathbb{R}$ muni des lois

$$x \oplus y = x + y - 1$$
$$x \otimes y = x + y - xy.$$

est un corps.

82. Montrer que si p est un nombre premier, alors $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, que nous noterons $\mathbb{F}_p$.

83. (Quaternions) De même que l'on définit le corps des complexes comme $\mathbb{C} = \{\, a + ib \ : \ a, b \in \mathbb{R}\,\}$, avec $i^2 = -1$, posons

$$\mathbb{H} = \{a + ib + jc + kd \ : \ a, b, c, d \in \mathbb{R}\}$$

avec $i^2 = j^2 = k^2 = -1$ et $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Montrer que cela définit un corps non commutatif.

84. a. Soit α un rationnel positif non nul dont la racine carrée n'est plus rationnelle. Montrer que $\mathbb{Q}(\sqrt{\alpha}) = \{\, a + b\sqrt{\alpha} \ : \ a, b \in \mathbb{Q}\,\}$ est un corps.
b. Montrer que les anneaux $\mathbb{Q}^2$ et $\mathbb{Q}(\sqrt{\alpha})$ ne sont pas isomorphes.
c. Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ sont-ils isomorphes ?
d. Si α et β sont des rationnels, donner une condition nécessaire et suffisante pour que les corps $\mathbb{Q}(\sqrt{\alpha})$ et $\mathbb{Q}(\sqrt{\beta})$ soient isomorphes. Montrer qu'ils sont alors égaux, en tant que sous-corps de $\mathbb{C}$.
e. Quels sont les automorphismes de $\mathbb{Q}$? de $\mathbb{Q}(\sqrt{2})$?

85. Montrer que les séries de Laurent à coefficients dans un corps commutatif k, *i.e.*, les séries formelles

$$\sum_{n \geqslant N} a_n x^n$$

où N est un entier *relatif*, forment un corps.

86. a. Montrer que le noyau d'un morphisme d'anneaux est un idéal.
b. Montrer qu'un anneau est un corps si et seulement si (0) est son seul idéal.
c. En déduire qu'un morphisme de corps est toujours injectif.

Espaces vectoriels

À savoir

- Reconnaître un espace vectoriel, un sous-espace vectoriel ;
- Connaître les principaux exemples : $\mathbb{R}^n$ et des espaces de fonctions ;
- Reconnaître si une famille libre ou liée ;
- Savoir transformer une famille liée en une famille libre ;
- Savoir compléter une famille libre en une base ;
- Comprendre les deux descriptions d'un sous-espace, par une famille génératrice ou par un système d'équations, savoir passer de l'un à l'autre.

Définitions

1. a. Soit X un ensemble. Montrer que l'ensemble des fonctions de X vers $\mathbb{R}$ forme un espace vectoriel.
b. Soit V un espace vectoriel. Montrer que l'ensemble des fonctions de X vers V forme un espace vectoriel.

2. L'ensemble dont le seul élément est la lune, muni de la loi interne lune+lune = lune et de la loi externe $\lambda \cdot$ lune = lune est-il un espace vectoriel ?

3. L'ensemble des fonctions $f \in \mathscr{F}(\mathbb{R}, \mathbb{R})$ vérifiant les propriétés suivantes forment-elles un espace vectoriel ?
a. Les fonctions de classe $\mathscr{C}^\infty$.
b. Les fonctions s'annulant en une infinité de points.
c. Les fonction s'annulant sur une partie donnée de $\mathbb{R}$.
d. Les fonctions périodiques de période T.
e. Les fonctions périodiques de période quelconque.
f. Les fonctions périodiques de période rationnelle.
g. Les fonctions périodiques de période un multiple rationnel de π.
h. Les fonctions s'annulant sur un intervalle non vide centré en zéro.
i. les fonctions croissantes sur $\mathbb{R}$.
j. Les fonctions pouvant s'écrire comme différence de deux fonctions croissantes.
k. Les solutions de l'équation différentielle $y''' - y'' + y' - y = 0$.
l. Les fonctions dont l'image est finie.
m. Les fonctions f telles que

$$\exists A_f \qquad \forall x \in \mathbb{R} \qquad |f(x)| \leqslant A_f\,|x|\,.$$

4. Montrer que $\mathbb{Q}(\sqrt{2})$ est un espace vectoriel de dimension deux sur $\mathbb{Q}$. Que peut-on dire de $\mathbb{Z}[\sqrt{2}]$?

Sous-espaces vectoriels

5. Montrer que les fonctions paires et impaires sont des sous-espaces vectoriels P et I de $E = \mathscr{F}(\mathbb{R}, \mathbb{R})$. En remarquant que pour tout $f \in E$ et tout $x \in \mathbb{R}$,
$f(x) = \frac{1}{2}(f(x) + f(-x)) + \frac{1}{2}(f(x) - f(-x))$,
montrer que $E = P \oplus I$.

6. Vérifier que $A + B = \operatorname{Vect} A \cup B$.

7. Soient A, B et C trois sous-espaces vectoriels tels que $A \cap B = A \cap C$, $A + B = A + C$ et $B \subset C$. Montrer que $B = C$.

8. Soient $E_1, \ldots, E_n$ des sous-espaces vectoriels de E tels que $E = \bigoplus_{i=1}^n E_i$ et F_i des sous-espaces de E_i. Montrer que la somme des F_i est directe. Déterminer $(\bigoplus_j F_j) \cap E_i$.

9. Soient E un espace vectoriel et A et B des sous-espaces. Montrer que $A \cup B$ est un sous-espace si et seulement si $A \subset B$ ou $B \subset A$.

10. Soient A, B et C des sous-espaces vectoriels d'un espace vectoriel E. Pour chacune

des assertions suivantes, montrer qu'en général il n'y a qu'une inclusion et donner une condition sous laquelle l'égalité est vérifiée.
a. $A \cap B \subset A + B$.
b. $(A \cap B) + (A \cap C) \subset A \cap (B + C)$.
c. $A + (B \cap C) \subset (A + B) \cap (A + C)$.

11. Soient A, B et C des sous-espaces d'une espace vectoriel E. Montrer les assertions suivantes.

$$\begin{gathered}(A \cap B) + (B \cap C) + (C \cap A) \subset \\ (A + B) \cap (B + C) \cap (C + A), \\ A + (B \cap (A + C)) = (A + B) \cap (A + C), \\ A \cap (B + (A \cap C)) = (A \cap B) + (A \cap C),\end{gathered}$$

12. a. Soient A et B des sous-espaces de E et C un supplémentaire de $A \cap B$ dans B. Montrer que $A + B = A \oplus C$.
b. Soient A et B des sous-espaces de E et A' et B' des supplémentaires de $A \cap B$ dans A et B. Montrer que $A + B = A \cap B \oplus A' \oplus B'$.
c. Montrer que si $E = A \oplus B$ et $A \subset C$, alors $C = A \oplus (B \cap C)$.

13. Montrer que la somme $A+B+C+D$ est directe si et seulement si $(A+B) \cap (C+D) = (A+C) \cap (B+D) = (A+D) \cap (B+C) = 0$.

14. Montrer que $\mathbb{R}^n$ est somme directe des sous-espaces suivants.

$$E = \operatorname{Vect}\{\,(1, \dots, 1)\,\}$$
$$F = \{\,(x_i)_i \;:\; \sum x_i = 0\,\}$$

15. Soient A et B des sous-espaces d'un espace vectoriel de dimension n. Montrer que si $\dim A + \dim B > n$, alors $A \cap B \neq 0$.

16. Soient A, B et C des sous-espaces d'un espace vectoriel E de dimension finie.
a. Monter que

$$\begin{aligned}\dim(A + B + C) &\leqslant \dim A + \dim B + \dim C \\ &- \dim(A \cap B) - \dim(B \cap C) \\ &- \dim(C \cap A) + \dim(A \cap B \cap C).\end{aligned}$$

b. Donner un exemple de sous-espaces de $\mathbb{R}^2$ pour lequel l'inégalité est stricte.

17. Soient $U_1, \dots, U_k$ des sous-espaces vectoriels de dimension $n - 1$ dans un espace vectoriel E de dimension n. Montrer que

$$\dim(U_1 \cap \dots \cap U_k) \geqslant n - k.$$

Familles libres, liées, bases

18. Démontrer que les vecteurs $(1, 0, 1, 0)$, $(1, -1, 2, 1)$, $(-1, 1, -1, -2)$ et $(0, -1, -1, 1)$ forment une base de $\mathbb{R}^4$. Exprimer le vecteur $(1, 2, 2, -3)$ dans cette base.

19. Montrer que les vecteurs $(1, -1, 1)$, $(-1, 2, 1)$ et $(1, 0, 3)$ sont liés. Trouver une relation entre eux. Quelle est la forme générale d'un élément du sous-espace vectoriel qu'ils engendrent ? En donner une base. En utilisant le théorème de la base incomplète, donner un supplémentaire de ce sous-espace.

20. a. Montrer que les vecteurs $(1, 1, 1)$ et $(1, -1, -1)$ sont indépendants dans $\mathbb{R}^3$. Compléter cette famille pour obtenir une base de $\mathbb{R}^3$. En déduire une représentation cartésienne du sous-espace engendré par ces deux vecteurs.
b. Donner une représentation cartésienne de $\operatorname{Vect}\{\,(1, 0, 1)\,\}$.

21. a. Pour quelle valeur de a les vecteurs $(a, 1, 1)$, $(1, a, -1)$ et $(1, -1, 0)$ sont-ils liés dans $\mathbb{R}^3$? Donner une base du sous-espace E qu'ils engendrent. Trouver un supplémentaire de E et donner une représentation cartésienne de E.
b. Donner une base du sous-espace F défini par l'équation $x+y+z = 0$. Déterminer $E \cap F$ et $E + F$; donner leurs dimensions.

22. a. Multiplier les exemples d'exercices comme les trois précédents.
b. Seriez-vous capable d'expliquer à un ordinateur comment résoudre ce genre de problèmes dans $\mathbb{R}^n$?

23. On considère le sous-espace E engendré par $(1, 1, -1, 0)$, $(0, 1, 1, -1)$, $(1, 0, -2, 1)$ et $(1, 2, 0, -1)$ et le sous-espace F engendré par

$(1,-1,-3,2)$, $(1,1,0,-1)$ et $(2,0,-3,1)$. Déterminer une base et la dimension de E, F, $E\cap F$ et $E+F$.

24. a. Montrer que les (x,y,z) tels que
$$x+y+z=y-2z=0$$
forment un sous-espace vectoriel de $\mathbb{R}^3$. Quelle est sa dimension ? En donner une base.
b. Donner une base et la dimension du sous-espace G engendré par $(2,3,1)$, $(1,2,0)$, $(1,0,2)$. En donner une équation.
c. Les sous-espaces F et G sont-ils supplémentaires ?

25. Comparer le sous-espace engendré par $(2,3,-1)$ et $(1,-1,2)$ avec celui engendré par $(3,7,0)$ et $(5,0,-7)$.

26. a. Montrer que $\mathbb{R}$ est un espace vectoriel sur $\mathbb{Q}$.
b. En comparant le cardinal de $\mathbb{Q}$, celui d'un espace vectoriel de dimension finie n sur $\mathbb{Q}$ et celui de $\mathbb{R}$, montrer que $\mathbb{R}$ est un espace vectoriel de dimension infinie sur $\mathbb{Q}$.
c. Montrer que la famille $(2^{1/n})_{n\in\mathbb{N}^\times}$ est libre sur $\mathbb{Q}$. En déduire que $\mathbb{R}$ est de dimension infinie sur $\mathbb{Q}$.
d. Les familles suivantes sont-elles libres sur $\mathbb{Q}$? $(1,\sqrt{2})$, $(1,\sqrt{2},\sqrt[3]{2})$, $(1,\sqrt{2},\sqrt{3})$, $(1,\sqrt{2},\sqrt{3},\sqrt{6})$.

27. Soient $f_1,\dots,f_n$ des fonctions de classe $\mathscr{C}^{n-1}$. Montrer que si les vecteurs $(f_i^{(k)}(x))_k$ sont linéairement indépendants, alors les f_i sont aussi linéairement indépendantes.

28. Soit E un espace vectoriel et $(x_1,\dots,x_n)$ une famille de vecteurs. On définit une autre famille par $y_i=\sum_{j=1}^{i} x_j$. Montrer que l'une est libre si et seulement si l'autre l'est.

29. Soient j et k des entiers et λ un réel. Montrer que la famille $(x_i)_{1\leqslant i\leqslant n}$ est libre si et seulement si la famille $(y_i)i$ l'est, où $y_i=x_i$ si $i\neq j$ et $y_j=x_j+\lambda x_k$.

Exemples de sous-espaces

30. Montrer que
$$E=\{P\in\mathbb{R}_3[X]\ :\ \int_0^1 P(x)\,dx=0\}$$
est un sous-espace vectoriel de $\mathbb{R}_3[X]$. En donner une base. Quelle est sa dimension ? Trouver un supplémentaire de E. Donner une représentation cartésienne de E.

31. Montrer que
$$P_i=\sum_{k=0}^{i}(-1)^k X^k,\qquad 0\leqslant i\leqslant 3$$
forme une base de $\mathbb{R}_3[X]$. Quelles sont les coordonnées du polynôme $3X^3-2X^2+X-1$ dans cette base ?

32. Quelle est la dimension de l'espace des polynômes homogènes de degré d à n indéterminées ?

33. Soit $a\in\mathbb{R}$. Montrer que $((X-a)^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{R}_3[X]$. Quelles sont les coordonnées d'un polynôme P dans cette base.

34. Soit F l'ensemble des suites $(u_n)_{n\in\mathbb{N}}$ telles que $\forall n\in\mathbb{N}$, $u_{n+2}=3u_{n+1}-2u_n$.
a. Montrer que c'est un sous-espace vectoriel de l'espace $\mathscr{S}(\mathbb{R})$ des suites réelles.
b. En cherchant les suites géométriques qui sont dans F et en remarquant que toute suite de F est entièrement déterminée par ses deux premiers termes, donner une base et la dimension de F. Quelles sont les coordonnées de la suite de F définie par $u_0=a$ et $u_1=b$?

35. Montrer que les fonctions définie par e^x, $\ln(1+x^2)$, $\sin x$ et $2x/(1+x^2)$ forment une famille libre de $\mathscr{F}(\mathbb{R},\mathbb{R})$.

36. La famille $(f,f^2,\dots,f^n)$, où la fonction f est définie par $x\longmapsto\ln(1+x)$ et $f^n=f\circ\cdots\circ f$ est-elle libre ?

37. La famille $(\varphi_a,\varphi_b,\varphi_c)$, où on définit φ_a : $x\longmapsto\sin(x+a)$, est-elle libre ?

38. Montrer que les fonctions de la forme $f:x\longmapsto a\cos(x-\varphi)$, où a et φ sont des réel, forment un sous-espace de $\mathscr{F}(\mathbb{R},\mathbb{R})$. Quelle est sa dimension ?

39. Montrer que les familles suivantes sont libres dans $\mathscr{F}(\mathbb{R},\mathbb{R})$.
a. $(f_n(t) = \cos nt)_{n\in\mathbb{N}^\times}$.
b. $(f_n(t) = \sin nt)_{n\in\mathbb{N}^\times}$.

40. Montrer que le sous-espace de $\mathscr{F}(\mathbb{R},\mathbb{R})$ engendrés par les $x \longmapsto \cos nx$ coïncide avec celui engendré par les $x \longmapsto \cos^n x$.

41. Soit $(a_i)_{i\in I}$ une famille de réels distincts. Montrer que la famille $x \longmapsto |x - a_i|$ est libre dans $\mathscr{F}(\mathbb{R},\mathbb{R})$.

Applications linéaires

À savoir

- Déterminer le noyau et l'image d'un morphisme ;
- Appliquer le théorème du rang ;
- Reconnaître et décrire une projection, une réflexion.

Exemples et calculs

1. a. Montrer que l'application

$$f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y) & \longmapsto & (x+y,y) \end{array} \right.$$

est linéaire. Dessiner les ensembles

$$A = \{ (x,y) \in \mathbb{R}^2 \ : \ \max(|x|,|y|) = 1 \}$$
$$B = \{ (x,y) \in \mathbb{R}^2 \ : \ |x| + |y| = 1 \}$$
$$C = \{ (x,y) \in \mathbb{R}^2 \ : \ x^2 + y^2 = 1 \}$$

ainsi que leur image par f.

b. Montrer que l'application

$$f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y) & \longmapsto & (3x+2y,x+4y) \end{array} \right.$$

est linéaire. Dessiner l'image par f, f^2 et f^3 des vecteurs de la base canonique.

c. Reprendre la question précédente avec les vecteurs $(-2,1)$ et $(1,1)$. Que remarque-t-on ?

2. Donner un exemple d'application $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ telle que $\forall x \in \mathbb{R}^2$, $\forall \lambda \in \mathbb{R}$, $f(\lambda x) = \lambda f(x)$ mais qui ne soit pas linéaire.

3. Déterminer toutes les applications linéaires $\mathbb{R} \longrightarrow \mathbb{R}$.

4. Déterminez le rang, le noyau et l'image des applications linéaires suivantes. Quand il s'agit d'un automorphisme, donner son inverse.

a. $\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \longmapsto \begin{pmatrix} 2x+3y+7z+2t \\ 3x+6y+18z+4t \\ -3x-2y-2z-2t \\ 4x+5y+7z+3t \end{pmatrix}$.

b. $\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \longmapsto \begin{pmatrix} y+z \\ z+x \\ x+y \end{pmatrix}$.

c. $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} y+z \\ z+x \\ x+y \end{pmatrix}$.

d. $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} \frac{1}{2}(x-y+z) \\ \frac{1}{2}(-x+y+z) \\ z \end{pmatrix}$.

e. $\left\{ \begin{array}{ccc} \mathbb{R}_2[X] & \longrightarrow & \mathbb{R}_2[X] \\ P & \longmapsto & XP' - 3P. \end{array} \right.$

f. $\left\{ \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R}[X] \\ P & \longmapsto & P(X+1) - P(X). \end{array} \right.$

g. $D : \left\{ \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R}[X] \\ P & \longmapsto & P'. \end{array} \right.$

h. $\mathrm{Id} - D$.

5. a. Considérons l'endomorphisme

$$A : \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} \longmapsto \begin{pmatrix} a+b \\ 2a+b+4d+3e \\ c+2d+3e \\ a+-c+2d \\ 0 \end{pmatrix}$$

Donner une base de $\mathrm{Ker}\, A$, $\mathrm{Im}\, A$, $\mathrm{Ker}\, A + \mathrm{Im}\, A$, $\mathrm{Ker}\, A \cap \mathrm{Im}\, A$. Donner un sous-espace de dimension maximale sur lequel A est injective.

b. Considérons les morphismes

$$A : \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} \longmapsto \begin{pmatrix} a-2b+c+3d+2f \\ -2a+5b-3c-3d-f \\ 3a-8b+5c+11d+3f \\ -a+2b-c+3d+f \end{pmatrix}$$

$$B : \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \longmapsto \begin{pmatrix} a+2d \\ 2a \end{pmatrix}.$$

Décrire image et noyau de A, B et $B \circ A$.

6. Montrer que l'application
$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R}_3[X] & \longrightarrow & \mathbb{R}_3[X] \\ P & \longmapsto & P + (1-X)P' \end{array} \right.$$
est linéaire. Donner une base de son noyau et de son image. Montrer que
$$\operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi = \mathbb{R}_3[X].$$
Donner un endomorphisme de $\mathbb{R}_3[X]$ dont le noyau et l'image ne sont pas en somme directe.

7. Soit $E = \mathscr{C}^1([-1,1], \mathbb{R})$ l'espace des fonctions dérivables et $F = \{ f \in E \ : \ f(0) = 0 \}$.
a. Montrer que E est un sous-espace-vectoriel.
b. Montrer que $\varphi \ : \ E \longrightarrow E$ définie par $\varphi(f)(t) = \int_0^t f(u)\,du$ est un endomorphisme de E. Déterminer son noyau et son image.

8. Montrer que l'espace des suites arithmétiques réelles est isomorphe à $\mathbb{R}^2$.

9. Soient a et b des réels (on demande que b soit non nul) et E l'ensemble des suites réelles vérifiant $\forall n \in \mathbb{N}$, $u_{n+2} = au_{n+1} + bu_n$.
a. Montrer que E est un espace vectoriel de dimension 2.
b. Supposons $a^2 - 4b \neq 0$. En cherchant les suites géométriques dans E, trouver une base de E et l'expression générale d'un élément de E.
c. Supposons $a^2 - 4b = 0$. En cherchant les suites de la forme $(r^n)_n$ ou $(nr^n)_n$ dans E, trouver une base de E et l'expression générale d'un élément de E.
d. Généraliser pour les suites vérifiant
$$u_{n+k} = a_{k-1}u_{n+k-1} + \cdots + a_0 u_n.$$

10. a. Notons $U_k = X(X-1)\cdots(X-k+1)$. Montrer que l'application
$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R}_n[X] & \longrightarrow & \mathbb{R}_n[X] \\ X^k & \longmapsto & U_k \end{array} \right.$$
est un automorphisme.
b. Considérons l'application
$$\delta : \left\{ \begin{array}{ccc} \mathbb{R}_n[X] & \longrightarrow & \mathbb{R}_n[X] \\ P & \longmapsto & P(X+1) - P(X). \end{array} \right.$$
Vérifier que c'est une application linéaire. Calculer $\Delta(U_k)$. Déterminer le noyau et l'image de δ.
c. Décrire $d = \varphi^{-1} \circ \delta \circ \varphi$.

11. (Distributions) Notons $\mathscr{C}_c^\infty$ l'ensemble des fonctions indéfiniment dérivables $\mathbb{R} \longrightarrow \mathbb{R}$ nulle en dehors d'un intervalle borné.
a. Montrer que c'est un espace vectoriel.
b. Soit $f \in \mathscr{C}_c^\infty$. Montrer que l'application
$$\varphi_f : \left\{ \begin{array}{ccc} \mathscr{C}_c^\infty & \longrightarrow & \mathbb{R} \\ g & \longmapsto & \displaystyle\int_{-\infty}^{\infty} fg \end{array} \right.$$
est bien définie et linéaire.
c. Montrer que l'application
$$\left\{ \begin{array}{ccc} \mathscr{C}_c^\infty & \longrightarrow & \operatorname{Hom}(\mathscr{C}_c^\infty, \mathbb{R}) \\ f & \longmapsto & \varphi_f \end{array} \right.$$
est linéaire et injective.
d. Est-elle surjective ?

Noyau et image

12. Si f et g sont des applications linéaires, montrer $\operatorname{Ker}(g \circ f) = f^{-1}(\operatorname{Ker} g \cap \operatorname{Im} f)$.

13. Monter que si les endomorphismes f et g commutent, alors ils laisent stable le noyau et l'image l'un de l'autre.

14. Soit f un endomorphisme d'un espace de dimension finie. Montrer que les assertions suivantes sont équivalentes.
(i) $E = \operatorname{Ker} f + \operatorname{Im} f$;
(ii) $E = \operatorname{Ker} f \oplus \operatorname{Im} f$;
(iii) $\operatorname{Im} f = \operatorname{Im} f \circ f$;
(iv) $\operatorname{Ker} f = \operatorname{Ker} f \circ f$;
(v) il existe un endomorphisme g tel que $fgf = f$ et $\operatorname{Im} gf = \operatorname{Im} f$.
Que peut-on alors dire de f ?

15. Soit T un endomorphisme d'un espace de dimension finie. Montrer qu'il existe un entier n tel que $\operatorname{Ker} T^n \cap \operatorname{Im} T^n = 0$.

Endomorphismes remarquables

16. a. Montrer que
$$(x, y, z) \longmapsto (2y + z, y + z - x, 2y + z)$$
est une projection de $\mathbb{R}^3$. Donner les sous-espaces qui la définissent.
b. Décrire analytiquement la projection de $\mathbb{R}^3$ sur $\mathrm{Vect}\{(-1, 1, 1), (-1, 1, 2)\}$ le long de $\mathrm{Vect}(0, 1, 1)$.
c. Décrire analytiquement la réflexion de $\mathbb{R}^3$ par rapport à $\mathrm{Vect}\{\,(1, 1, -1), (0, 1, 1)\,\}$ le long de $\mathrm{Vect}(-1, 0, 1)$.

17. Soit p un projecteur de E et f un endomorphisme. Montrer qu'ils commutent si et seulement si le noyau et l'image de p sont stables par f.

18. a. Montrer que si p et q sont des projecteurs de E, alors les assertions suivantes sont équivalentes.
(i) $p + q$ est un projecteur ;
(ii) $p \circ q + q \circ p = 0$;
(iii) $p \circ q = q \circ p = 0$.
(Pour les deux derniers points, on pourra considérer $p \circ q(p \circ q + q \circ p)$.)(???)
b. Démontrer qu'alors $\mathrm{Im}\, p \cap \mathrm{Im}\, q = 0$ et $\mathrm{Ker}(p + q) = \mathrm{Ker}\, p \cap \mathrm{Ker}\, q$.

19. Soit $V = A \oplus B$ un espace vectoriel et p la projection sur A le long de B. Soit f un endomorphisme.
a. Montrer que A est f-invariant si et seulement si $fp = pfp$.
b. Montrer que A et B sont f-invariant si et seulement si $fp = pf$.

20. Soient p et q des endomorphismes.
a. Montrer que les assertions suivantes sont équivalentes.
(i) p et q sont des projecteurs complémentaires ;
(ii) $p + q = 1$, $p^2 = p$ et $q^2 = q$;
(iii) $p + q = 1$ et $pq = qp = 0$.
b. Montrer que les assertions suivantes sont équivalentes.
(i) p et q sont des réflexions complémentaires ;
(ii) $p + q = 1$, $p^2 = \mathrm{Id}$ et $q^2 = \mathrm{Id}$;
(iii) $p + q = 0$ et $pq = qp = -\mathrm{Id}$.

21. a. On dit qu'un endomorphisme T de E est une *réflexion* si on peut écrire $E = A \oplus B$, avec $T|_A = \mathrm{Id}_A$ et $T|_B = -\mathrm{Id}_B$. Montrer qu'alors $E = \mathrm{Ker}(T + \mathrm{Id}) \oplus \mathrm{Ker}(T - \mathrm{Id})$.
b. Soit T un endomorphisme. Montrer que les assertions suivantes sont équivalentes.
(i) T est involutive, *i.e.*, $T^2 = T$;
(ii) $p = \frac{1}{2}(1 - T)$ et $q = \frac{1}{2}(1 + T)$ sont des projecteurs complémentaires ;
(iii) $\mathrm{Ker}(T + 1) = \mathrm{Im}(T - 1)$;
(iv) $\mathrm{Ker}(T - 1) = \mathrm{Im}(T + 1)$;
(v) T est une réflexion.

22. Soit f un endomorphisme de E. Montrer que $f^2 = 0$ et $\dim E = 2 \,\mathrm{rang}\, f$ si et seulement si $\mathrm{Im}\, f = \mathrm{Ker}\, f$.

23. Soit T un endomorphisme nilpotent de V.
a. Montrer que si $T^k v \neq 0$, alors $(v, Tv, T^2 v, \dots, T^k v)$ est libre.
b. Montrer que si $T^k = 0$, alors
$$\dim \mathrm{Ker}\, T \geqslant \frac{1}{k} \dim V.$$
c. Soit T un endomorphisme d'un espace V de dimension deux. Montrer que $\mathrm{Ker}\, T = \mathrm{Im}\, T$ si et seulement si T est non nul et de carré nul. Quels sont les endormophismes nilpotents de V ?
d. notons $W_i = \mathrm{Im}\, T^i$. Montrer que si $W_i \neq 0$, alors $\dim W_{i+1} < \dim W_i$.
e. Montrer que si $\dim V = n$, alors $T^n = 0$.

Théorème du rang

24. Existe-t-il une application linéaire $\mathbb{R}^5 \longrightarrow \mathbb{R}^2$ dont le noyau soit
$$\{\,(a, b, c, d, e) \ : \ a = b \text{ et } c = d = e\,\}\,?$$

25. Montrer qu'une application linéaire de $\mathbb{R}^4$ dans $\mathbb{R}^2$ dont le noyau est
$$\{\,(a, b, c, d) \ : \ a = b \text{ et } c = d\}$$
est surjective.

26. Soient V et W des espaces vectoriels de dimension finie. Montrer qu'il existe un morphisme surjectif $V \longrightarrow W$ si et seulement si $\dim V \geqslant \dim W$.

27. Soient V et W des espaces vectoriels de dimension finie et U un sous-espace de V. Montrer que un morphisme $V \longrightarrow W$ de noyau U si et seulement si $\dim U \geqslant \dim V - \dim W$.

28. Soit $T : V \longrightarrow W$ une application linéaire. Montrer qu'il existe un sous-espace U de V tel que $\operatorname{Ker} T \cap U = 0$ et $\operatorname{Im} T = \operatorname{Im} T|_U$.

29. Soient f et g des endomorphismes d'un espace de dimension finie. Montrer

$$\operatorname{rang} g \circ f = \operatorname{rang} f - \dim \operatorname{Im} f \cap \operatorname{Ker} g.$$

30. **a.** Montrer que donner une représentation cartésienne d'un sous-espace revient à l'exprimer comme noyau d'une application linéaire.
b. Quel est le nombre minimal d'équations nécessaire pour définir un sous-espace de dimension n dans un espace de dimension m ? Ce nombre est-il suffisant ?

31. Soit $T : V \longrightarrow k$ une application linéaire. Montrer que si $v \in V$ n'est pas dans le noyau de T, alors on a $V = \operatorname{Ker} T \oplus \operatorname{Vect}\{v\}$.

Sous-espaces propres

32. En déterminant le noyau, l'image et les points fixes des morphismes suivants, puis éventuellement en les exprimant dans une autre base, décrire géométriquement les endomorphismes suivants de $\mathbb{R}^3$.

a. $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ \frac{1}{2}(y+z) \\ \frac{1}{2}(y-z) \end{pmatrix}$

b. $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} 3x - z \\ 6x + 4y + 5z \\ -3x + 3y + 2z \end{pmatrix}$

33. Soit f un endomorphisme d'un espace vectoriel E.

a. Montrer qu'une somme de sous-espaces invariants l'est encore.

b. Montrer qu'une intersection de sous-espaces invariants l'est encore.

34. Soit E un espace vectoriel de dimension 2 et f un endomorphisme tel que $f \circ f = \operatorname{Id}$, différent de $\pm \operatorname{Id}$. Notons

$$E_1 = \{\, x \in E \;:\; f(x) = x \,\},$$
$$E_2 = \{\, x \in E \;:\; f(x) = -x \,\}.$$

a. Montrer que E_1 et E_2 sont des sous-espaces vectoriels.

b. Calculer $f(x + f(x))$ et $f(x - f(x))$. En déduire que $E = E_1 \oplus E_2$.

c. Déterminer $\dim E_1$ et $\dim E_2$.

35. Cet exercice généralise le précédent. Soit f un endomorphisme tel que

$$f \circ f + af + b \operatorname{Id} = 0,$$

avec $a^2 - 4b > 0$. Notons α et β les racines distinctes du polynôme $X^2 + aX + b$ et $E_1 = \operatorname{Ker}(f - \alpha \operatorname{Id})$ et $E_2 = \operatorname{Ker}(f - \beta \operatorname{Id})$.

a. Montrer $E_1 \cap E_2 = 0$.

b. Montrer que si $E = E_1 + E_2$, alors tout vecteur x s'écrit de manière unique $x = x_1 + x_2$, avec

$$x_1 = \frac{f(x) - \alpha x}{\beta - \alpha}, \qquad x_1 = \frac{f(x) - \beta x}{\alpha - \beta}.$$

c. Montrer $E = E_1 \oplus E_2$. Examiner le cas $\alpha = -1$, $\beta = 0$.

d. Que se passe-t-il si $a^2 - 4b < 0$? et si $a^2 - 4b = 0$?

36. Soit f un endomorphisme de E.

a. Montrer que $E_\lambda = \operatorname{Ker}(f - \lambda \operatorname{Id})$ est un sous-espace vectoriel stable par f.

b. On dit que λ est une *valeur propre* de f s'il existe un vecteur non nul u tel que $f(u) = \lambda u$. On dit alors que u est un *vecteur propre* de f. Montrer que λ est une valeur propre si et seulement si $f - \lambda \operatorname{Id}$ n'est pas injectif.

c. Considérons
$$f : \begin{cases} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} & \longmapsto & \begin{pmatrix} 4z \\ x + 2y + z \\ 2x + 4y - 2z \end{pmatrix} \end{cases}.$$
Trouver une base puis une représentation cartésienne du noyau et de l'image de f. Montrer que $-4, 0, 4$ sont valeurs propres de f. Donner une base de $\mathbb{R}^3$ constituée de vecteurs propres de f. Décrire le morphisme f dans cette base.

d. Considérons
$$f : \begin{cases} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} & \longmapsto & \begin{pmatrix} 6x - 5y + z \\ 9x - 8y + z \\ 5x - 5y + 2z \end{pmatrix} \end{cases}.$$
Quelles sont les valeurs propres de f ? Donner une base de $\mathbb{R}^3$ constituée de vecteurs propres de f. Décrire le morphisme f dans cette base.

e. Si f est un endormophisme d'un espace vectoriel E, existe-t-il toujours une base de E constituée de vecteurs propres de f ?

37. a. Soit φ un endomorphisme d'un espace vectoriel E tel que $\varphi^2 - 5\varphi + 6\,\mathrm{Id}_E = 0$. Montrer que
$$E = \mathrm{Ker}(\varphi - 2\,\mathrm{Id}_E) \oplus \mathrm{Ker}(\varphi - 3\,\mathrm{Id}_E).$$
b. Généraliser à un polynôme quelconque.

38. Soit T un endomorphisme d'un espace vectoriel V.

a. Montrer que des vecteurs propres de T associés à des valeurs propres distinctes sont linéairement indépendants.

b. En déduire que si T possède $\dim V$ valeurs propres distinctes, alors il possède une base de vecteurs propres.

39. a. Trouver les valeurs propres de l'application $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ définie par $\varphi(e_i) = (1, \dots, 1)$, où $(e_i)_i$ est la base canonique.

b. Trouver les valeurs propres de l'application $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ définie par $\varphi(x_1, \dots, x_n) = (x_2, \dots, x_n, 0)$.

40. a. Trouver tous les sous-espaces invariants de l'application linéaire
$$(x, y) \longmapsto (x + y, y).$$
b. Même question pour l'application linéaire
$$(x, y, z) \longmapsto (x, 2y, 3z).$$

Divers

41. Soit $f : E \longrightarrow F$ un morphisme et X et Y des parties de E et F. Les assertions suivantes sont-elles exactes ?

« Si $f(X)$ est libre, alors X aussi. »
« Si X est libre, alors $f(X)$ aussi. »
« Si $f(X)$ est génératrice, alors X aussi. »
« Si X est génératrice, alors $f(X)$ aussi. »
« Si $f^{-1}(Y)$ est libre, alors Y aussi. »
« Si Y est libre, alors $f^{-1}(Y)$ aussi. »
« Si $f^{-1}(Y)$ est génératrice, alors Y aussi. »
« Si Y est génératrice, alors $f^{-1}(Y)$ aussi. »

42. a. Montrer qu'un endomorphisme f tel que pour tout $x \in E$, la famille $(x, f(x))$ soit liée est une homothétie.

b. Quels sont les endomorphismes de E qui commutent avec tous les autres ? (Si f est un tel endomorphisme, on pourra considérer, pour $x \in E$, une projection g sur $\mathrm{Vect}\, x$, montrer que $f(x) \in \mathrm{Vect}\, x$ et conclure.)

43. a. Montrer qu'une application linéaire est injective si et seulement si elle possède un inverse à gauche.

b. Montrer qu'une application linéaire est surjective si et seulement si elle possède un inverse à droite.

44. Si S et T sont des applications linéaires entre des espaces vectoriels de dimension finie, montrer que le composé ST est un isomorphisme si et seulement si S et T sont des isomorphismes. Que se passe-t-il en dimension infinie ?

45. Soit $f : V \longrightarrow W$ un morphisme. Notons
$$R(f) = \{\, g \in \mathrm{Hom}(W, V) \ : \ f \circ g = 0 \,\}.$$
a. Montrer que $R(f) \simeq \mathrm{Hom}(W, \mathrm{Ker}\, f)$.

b. Montrer que si h_1 et h_2 sont des inverses à droite de f, alors $h_1 - h_2 \in R(f)$.

Matrices

À savoir

- Multiplier des matrices ;
- Utiliser le pivot de Gauss pour inverser une matrice ;
- Utiliser le pivot de Gauss pour résoudre un système dépendant d'un paramètre ;
- Dans certains cas particuliers, calculer les puissances d'une matrice ;
- Donner la matrice d'un morphisme par rapport à des bases ;
- Effectuer un changement de base.

Calculs Numériques

1. Calculer ABC et CAB, où

$$A = \begin{pmatrix} 3 & -2 & 1 \\ 1 & 2 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \ C = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

2. a. Calculer, si possible, AB et BA avec

$$A = \begin{pmatrix} 1 & -1 \\ 2 & 2 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & 1 \\ -4 & 4 \end{pmatrix}.$$

b. Existe-t-il une matrice C telle que $CA = B$? Laquelle ?
c. Existe-t-il une matrice D telle que $AD = B$? Laquelle ?

3. Vérifier que les matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 2 & 2 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

sont égales à leur carré.

4. a. Trouver deux matrices A et B telles que $AB \neq BA$.
b. Trouver deux matrices carrées A et B non nulles telles que $AB = 0$. En d'autres termes, l'anneau $\mathscr{M}_n$ n'est pas intègre.
c. Trouver deux matrices A et B telles que $AB = I$ et $BA \neq I$.
d. Trouver des matrices A et B telles que $(A+B)^2 \neq A^2 + 2AB + B^2$.
e. Trouver des matrices A et B telles que $(A-B)(A+B) \neq A^2 - B^2$.
f. Trouver une matrice A non nulle telle que $A^2 = 0$.
g. Trouver une matrice A telle que $A^2 = -\operatorname{Id}$.

5. Soit E l'ensemble des matrices carrées d'ordre deux égales à leur carré.
a. Déterminer toutes les matrices de E.
b. Quelles sont les matrices inversibles de E ?
c. Retrouver ce résultat sans aucun calcul.

6. Trouver toutes les matrices qui commutent avec

$$\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \text{ puis avec } \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

7. Quelles sont les matrices de taille deux de carré nul ?

8. Quelles sont les matrices A de taille deux telles que $A^2 = I$?

9. Vérifier que les matrices A de taille deux telles que ${}^tAA = I$ sont exactement les

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \qquad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

10. Résoudre les équations matricielles suivantes.

a. $X \begin{pmatrix} -1 & 0 & 1 \\ 1 & 1 & 0 \\ 3 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ -3 & 1 & 5 \end{pmatrix}.$

b. $X \begin{pmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -5 & -1 & 0 \\ 6 & -3 & 7 \end{pmatrix}.$

c. $\begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix} X - X \begin{pmatrix} 1 & 4 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -2 \\ 5 & 4 \end{pmatrix}.$

11. Montrer qu'il existe une matrice P inversible telle que

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = P^{-1} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} P$$

si et seulement si $a \neq d$ ou $b = 0$.

Calculs

12. **a.** Vérifier que multiplier une matrice ligne par une matrice A revient à faire une combinaison linéaire sur les lignes de A.
b. Vérifier que multiplier une matrice A par une matrice colonne revient à faire une combinaison linéaire sur les colonnes de A.

13. Montrer que des matrices diagonales de même taille commutent.

14. On dit qu'une matrice est *stochastique* si ses coefficients sont positifs et si la somme des éléments de chaque ligne est égale à un. Montrer qu'un produit de matrices stochastiques l'est encore.

15. Si les coefficients d'une matrice A sont des fonctions dérivables, $a_{i,j}(t)$, on note

$$\frac{dA}{dt} = \left(a'_{i,j}(t)\right)_{i,j}.$$

Si A et B sont de telles matrices, f une fonction dérivable et λ un scalaire, calculer la dérivée de $A+B$, λA, fA, et AB.

16. Soit $u \in \mathbb{R}^n$ tel que ${}^tuu = 1$. Posons $H = I - 2u{}^tu$. Montrer que $H = {}^tH$ et ${}^tHH = I$.

17. **a.** Si A et B sont des matrices carrées de même taille, on définit $A * B = \frac{1}{2}(AB + BA)$. Vérifier que ce produit est commutatif. Est-il associatif ? Vérifier qu'il est distributif par rapport à l'addition. Montrer que

$$A * (B * A^2) = (A * B) * A^2.$$

b. On note maintenant $[A, B] = AB - BA$. Montrer que $[A, B] = -[B, A]$. Ce produit est-il associatif ? Montrer que

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0.$$

Montrer que $AB = A * B + \frac{1}{2}[A, B]$.

Pivot de Gauss

18. **a.** Trouver le polynôme f de degré trois tel que

$$f(0) = 10,\ f(1) = 7,\ f(3) = 11,\ f(4) = -14.$$

b. Trouver le polynôme de degré deux dont le graphe passe par le point $(-1, 0)$ et possède une tangente horizontale au point $(2, -9)$.
c. Trouver l'équation du cercle passant par les points $(-2, 7)$, $(-4, 5)$ et $(4, -3)$.
d. Trouver des réels a, b et c tels que

$$\frac{x^2 + x - 2}{(3x-1)(x^2+1)} = \frac{a}{3x-1} + \frac{bx+c}{x^2+1}.$$

19. **(Interpolation de Lagrange)** Soient x_1, x_2 et x_3 trois réels distincts.
a. Montrer que le morphisme

$$T : \left\{ \begin{array}{ccc} \mathbb{R}_2[X] & \longrightarrow & \mathbb{R}^3 \\ P & \longmapsto & (P(x_1), P(x_2), P(x_3)) \end{array} \right.$$

est injectif, puis que c'est un isomorphisme.
b. Calculer les image réciproques P_i des vecteurs de la base canonique de $\mathbb{R}^3$.
c. Quel rapport y a-t-il entre le graphe de $a_1P_1(x) + a_2P_2(x) + a_3P_3(x)$ et les points (x_i, a_i) ?
d. Généraliser à des polynômes de degré quelconque.

20. Résoudre le système

$$\begin{aligned} mx + (m-1)y + z &= 0 \\ 2mx + my + (4-m)z &= 0 \\ mx + y + z &= 0. \end{aligned}$$

21. **a.** Rappeler (et justifier) la méthode de calcul de l'inverse d'une matrice à l'aide du pivot de Gauss.
b. Posons

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Trouver une matrice inversible B telle que BA soit triangulaire supérieure. Cette matrice est-elle unique ?
c. Expliquer comment on procèderait pour obtenir une matrice B inversible telle que AB soit triangulaire supérieure. Même question avec triangulaire inférieure.

22. Montrer que l'on peut passer de la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ à la matrice $\left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right)$ par des opérations élémentaires sur les lignes et les colonnes à moins que $b = c = 0$ et $a = d$. On fera attention au cas où b ou c est nul.

23. (Décomposition LU) Certaines matrices inversibles peuvent s'écrire sous la forme LU, où L est une matrice triangulaire inférieure et U une matrice triangulaire supérieure dont les éléments diagonaux sont égaux à un.

a. Montrer qu'une telle décomposition, si elle existe, est unique.

b. Expliquer comment la trouver.

c. Une matrice de permutaion est un produit de matrices élémentaires correspondant à l'interversion de deux lignes (ou colonnes). Montrer que toute matrice inversible peut s'écrire LPU, où P est une matrice de permutation et L et U sont comme ci-dessus.

24. Donner des systèmes linéaires dépendant d'un paramètre.

Puissances d'une matrice

25. Calculer $J = P^{-1}AP$ puis J^n où

$$A = \begin{pmatrix} 0 & 2 & -3 \\ 1 & 1 & 1 \\ 2 & -2 & 5 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}.$$

En déduire A^n.

26. Calculer $J = P^{-1}AP$ puis J^n où

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 3 & 1 \\ -1 & -1 & 2 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}.$$

En déduire A^n.

27. Calculer A^n, où

$$A = \begin{pmatrix} 4 & 3 & 3 \\ 3 & 4 & 3 \\ 3 & 3 & 4 \end{pmatrix},$$

en écrivant $A = I_3 + J_3$.

28. Considérons les matrices

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

a. Calculer A^n par récurrence.

b. Calculer A^n en posant $A = I_3 + N$.

c. Calculer AB et BA. Que peut-on en déduire? Que représente B^n?

29. Posons

$$M = \begin{pmatrix} 2 & -2 & 1 \\ 2 & -3 & 2 \\ -1 & 2 & 0 \end{pmatrix}.$$

a. Vérifier que $M^2 + 2M - 3I_3 = 0$.

b. En déduire que M est inversible et déterminer M^{-1}.

c. Montrer que

$$\forall n \in \mathbb{N}, \ M^n = u_n M + v_n I_3,$$

où les suite u et v sont définies par

$$\begin{aligned} u_0 &= 0 \qquad & u_{n+1} &= -2u_n + v_n \\ v_0 &= 1 \qquad & v_{n+1} &= 3u_n. \end{aligned}$$

d. Vérifier que $\forall n \in \mathbb{N}, \ u_n + v_n = 1$. En déduire que $\forall n \in \mathbb{N}, \ u_{n+1} = -3u_n + 1$. (On parle de suite arithmético-géométrique.)

e. Déterminer $\alpha \in \mathbb{R}$ tel que la suite w définie par $w_n = u_n - \alpha$ pour tout entier n soit géométrique. En déduire, en fonction de n, l'expression de w_n, u_n, v_n et M^n.

f. Généraliser.

30. Considérons

$$A = \begin{pmatrix} 2 & 1 & -4 \\ 0 & 1 & -2 \\ 1 & 1 & -3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 2 & -4 \\ 1 & 1 & -2 \end{pmatrix}$$

et pour $x, y \in \mathbb{R}$, notons $M = xA + yB$.

a. Calculer A^2, A^3, A^n. La matrice A est-elle inversible?

b. Calculer B^2, B^n. La matrice B est-elle inversible?

c. Calculer AB et BA. En déduire M^n.

31. Montrer que si $a \neq b$, alors

$$a^n + a^{n-1}b + \cdots + ab^{n-1} + b^n = \frac{a^{n+1} - b^{n+1}}{a - b}.$$

En déduire

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 1 & 0 & c \end{pmatrix}^n.$$

32. Trouver un polynôme de degré deux annulant
$$B = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}.$$
En déduire $I + B + B^2 + \cdots$.

33. Montrer les égalités suivantes, en supposant que les inverses qui interviennent existent.
a. $(C^{-1} + D^{-1})^{-1} = C(C + D)^{-1}D$.
b. $(I + CD)^{-1}C = C(I + DC)^{-1}$.
c. $(C + D^tD)^{-1}D = C^{-1}D(I + {}^tDC^{-1}D)^{-1}$.

L'anneau/espace vectoriel des matrices

34. a. Montrer que si $A^2 = I$, alors $B = \frac{1}{2}(I + A)$ est égale à son carré.
b. Montrer que si $AB = A$ et $BA = A$, alors $A^2 = A$ et $B^2 = B$.
c. Montrer que $A^2 = A$ si et seulement si $(I - A)^2 = I - A$.

35. a. Les matrices inversibles forment-elles un sous-espace vectoriel ?
b. Les matrices non inversibles forment-elles un sous-espace vectoriel ?

36. On dit qu'une matrice $A \in \mathscr{M}_n$ est *nilpotente* s'il existe un entier p tel que $A^p = 0$.
a. Montrer que si A et B sont nilpotentes et commuttent, alors $A + B$ et AB sont aussi nilpotentes.
b. Calculer $(I - A)(I + A + \cdots + A^k)$. En déduire l'inverse de $I - A$ si A est nilpotente.
c. L'exponentielle d'une matrice nilpotente.
d. Les matrices nilpotentes forment-elles un sous-anneau ? un idéal ?

37. La transposition est-elle un morphisme d'anneaux ?

38. Soient X, $Y \in \mathscr{M}_n$. Montrer que pour tout entier $r \geqslant 1$,
$$X^r - Y^r = \sum_{j=0}^{r-1} Y^j(X - Y)X^{r-1+j}.$$

39. Notons T_n (respectivement T'_n) l'ensemble des matrices triangulaires supérieures (respectivement inférieures).
a. Montrer que ce sont des sous-espaces vectoriels de $\mathscr{M}_n$. Vérifier que $T_n + T'_n = \mathscr{M}_n$.
b. Cette somme est-elle directe ? Calculer la dimension de T_n et T'_n.
c. Les sous-espaces T_n et T'_n sont-ils aussi des sous-anneaux ?

40. On dit qu'une matrice carrée A est *symétrique* si $A = {}^tA$ et *antisymétrique* si $A = -{}^tA$.
a. Si A est une matrice carrée, montrer que A^tA et ${}^tAA$ sont symétriques et que leurs termes diagonaux sont posifits. Montrer que $A+{}^tA$ est symétrique et que $A-{}^tA$ est antisymétrique. Montrer que si A est symétrique ou antisymétrique et P quelconque, alors ${}^tPAP$ l'est aussi.
b. Notons S_n et A_n l'ensemble des matrices symétriques et antisymétriques de taille n. Montrer que ce sont des sous-espaces vectoriels de $\mathscr{M}_n$. Quelle est leur dimension ? Montrer que $\mathscr{M}_n = S_n \oplus A_n$.

41. Montrer que l'application
$$\begin{cases} \mathscr{M}_2 & \longrightarrow & \mathscr{M}_2 \\ X & \longmapsto & \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} X + X \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \end{cases}$$
est linéaire. Déterminer son noyau et son image.

42. Soit $M \in \mathscr{M}_n$ une matrice carrée. Si $P = \sum a_n X^n \in \mathbb{R}[X]$ est un polynôme, on note
$$P(M) = \sum_n a_n M^n.$$
a. Montrer qu'il existe un polynôme P qui annule M.
b. Montrer que les polynômes qui annulent M forment un idéal de $\mathbb{R}[X]$.
c. Trouver un polynôme de degré deux annulant $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

d. Trouver un polynôme *de degré minimal* annulant les matrices suivantes.

$$\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \quad \begin{pmatrix} -2 & 4 \\ 3 & 6 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & -c_0 \\ 1 & 0 & -c_1 \\ 0 & 1 & -c_2 \end{pmatrix}$$

Expliquer comment déduire la puissance 1998^e d'une matrice à partir d'un polynôme l'annulant.

43. a. Montrer que les matrices de la forme

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

forment un corps commutatif. Est-il isomorphe à un corps que l'on connait ?

b. Montrer que le sous-espace vectoriel *réel* de $\mathscr{M}_2(\mathbb{C})$ engendré par les matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

est un corps non commutatif.

Inverse et rang

44. À quelle condition la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est-elle inversible ? Quel est alors son inverse ?

45. Calculer l'inverse des matrices suivantes.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 \\ -1 & -1 & -1 & -1 & 0 \\ 1 & 1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 0 & -1 \end{pmatrix}$$

46. Inverser (si possible) les matrices suivantes.

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 0 & 7 \\ 0 & 0 & 9 \end{pmatrix}$$

$$C = \begin{pmatrix} -1 & 1 & -1 \\ 2 & -2 & -2 \\ 3 & -7 & -1 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

47. Discuter, en fonction de a et b, le rang des matrices suivantes. Donner éventuellement leur inverse.

$$A = \begin{pmatrix} a+b & a-b \\ a-b & a+b \end{pmatrix}, \qquad B = \begin{pmatrix} a & 0 & b \\ b & a & 0 \\ 0 & b & a \end{pmatrix}$$

48. Calculer l'inverse des matrices suivantes.

$$\begin{pmatrix} 1 & -1 & & \\ & \ddots & \ddots & \\ & & \ddots & -1 \\ & & & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & & & & \\ -2 & \ddots & & & \\ 1 & \ddots & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & -2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -1 & & \\ -1 & \ddots & \ddots & \\ & \ddots & \ddots & -1 \\ & & -1 & 2 \end{pmatrix}$$

49. Montrer qu'une matrice triangulaire est inversible si et seulement si ses termes diagonaux sont non nuls. Ce résultat reste-t-il vrai pour des matrices quelconques ?

50. Montrer qu'une matrice contenant une ligne ou une colonne de zéros n'est pas inversible.

51. Montrer que si A, $B \in \mathscr{M}_n$, alors $\operatorname{rang}(A+B) \leqslant \operatorname{rang} A + \operatorname{rang} B$.

52. a. Si $u \in \mathbb{R}^n$, montrer que le rang de $u\,{}^t u$ est égal à un.

b. Réciproquement, montrer que toute matrice carrée de rang un peut s'écrire $u\,{}^t u$, où u est un vecteur colonne.

53. (Trace) La *trace* d'une matrice carrée est la somme de ses éléments diagonaux.

a. Montrer que la trace est une application linéaire $\mathscr{M}_n \longrightarrow \mathbb{R}$.

b. Montrer que $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$. A-t-on $\operatorname{Tr}(AB) = \operatorname{Tr} A \operatorname{Tr} B$?

c. Montrer que $\operatorname{Tr}(ABC) = \operatorname{Tr}(BCA)$. A-t-on $\operatorname{Tr}(ABC) = \operatorname{Tr}(ACB)$?

d. Sans calcul, dire s'il existe une matrice inversible P telle que
$$P^{-1}\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}P=\begin{pmatrix}2 & 3\\ 1 & 4\end{pmatrix}.$$
e. En déduire la définition de la trace d'un *endomorphisme*.
f. Montrer que la trace d'un projecteur est un entier positif.
g. Montrer que les matrices de trace nulle forment un sous-espace vectoriel de $\mathscr{M}_n$. Quelle est sa dimension ? pouivez-vous en donner une base ?
h. Montrer que si un endomorphisme T possède une base de vecteurs propres (sur $\mathbb{R}$), alors $\mathrm{Tr}(T^2)\geqslant 0$.
i. Donner un exemple de matrice telle que $\mathrm{Tr}(T^2)<0$.
j. Montrer que
$$\forall T\ \mathrm{Tr}(ST)=0 \implies S=0.$$
k. Montrer que
$$\mathrm{Tr}(A^tA)=\mathrm{Tr}({}^tAA)=\sum_{i,j}a_{i,j}^2.$$

Groupes de matrices

54. a. Montrer que les matrices $\left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right)$ forment un groupe à quatre éléments. Est-il isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\times\mathbb{Z}/2\mathbb{Z}$?
b. Montrer que les matrices
$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\quad\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}\quad\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\quad\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$
et leurs inverses forment un groupe multiplicatif à huit éléments.
c. Montrer que le sous-groupe engendré par $\left(\begin{smallmatrix}1 & 1\\ -1 & 0\end{smallmatrix}\right)$ est d'ordre fini. Est-il abélien ? À quel groupe connu est-il isomorphe ?
d. Quel est le sous-groupe engendré par la matrice $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$? Est-il isomorphe à un groupe que l'on connait ?
e. Montrer que les matrices de la forme $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$ forment un sous-groupe. Est-il isomorphe à un groupe que l'on connait ?
f. Soit n un entier positif. Donner un sous-groupe de GL_2 isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
g. Quel est le sous-groupe engendré par
$$\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}\qquad\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}\ ?$$
Montrer qu'il est isomorphe à $\mathfrak{S}_3$.

55. (Matrices de permutations) Notons $(e_1,\dots,e_n)$ la base canonique de $\mathbb{R}^n$. Si $\sigma\in\mathfrak{S}_n$, montrer que l'on définit un automorphisme par $\varphi_\sigma(e_i)=e_{\sigma(i)}$. Quelle est sa matrice ? Montrer que cela définit un morphisme de groupes $\mathfrak{S}_n\longrightarrow\mathrm{GL}_n$.

56. a. Montrer que les matrices inversibles de taille n forment un groupe, noté GL_n.
b. Montrer que les matrices triangulaires supérieures dont les éléments diagonaux sont non nuls forment un groupe.
c. Montrer que les matrices triangulaires supérieures dont les éléments diagonaux sont égaux à un forment un groupe.
d. Montrer que
$$\mathrm{SO}_2=\left\{\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\right\}$$
est un sous-groupe de GL_n.
e. Montrer que les matrices A de taille n telles que $A^tA=I$ forment un sous-groupe de GL_n.
f. Soit J une matrice inversible. Montrer que les matrices inversibles A telles que ${}^tAJA=J$ forment un sous-groupe.
g. Une *affinité* de $\mathbb{R}^n$ est une application $x\longmapsto Ax+b$ où A est une matrice et b un vecteur. On peut dont identifier l'ensemble des affinités au produit $\mathscr{M}_n\times\mathbb{R}^n$. Montrer que la composition des applications en fait un groupe. Expliciter la loi de groupe sur $\mathscr{M}_n\times\mathbb{R}^n$. Montrer qu'on peut voir ce groupe comme un sous-groupe de GL_{n+1}, *i.e.*, qu'il est isomorphe à un sous-groupe de GL_{n+1}.

57. Pour les sous-groupes de GL_n apparaissant dans les exercices précédents : dire si ce sont des sous-groupes distingués, déterminer leur centre, etc. (peut-être aussi leur sous-groupe dérivé)

Matrice d'un endomorphisme

58. Interpréter géométriquement les endomorphismes de $\mathbb{R}^2$ ou $\mathbb{R}^3$ dont les matrices suivent.

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\ \begin{pmatrix}1&0\\0&0\end{pmatrix}\ \begin{pmatrix}0&0\\0&1\end{pmatrix}\ \begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

$$\begin{pmatrix}-1&0\\0&1\end{pmatrix}\ \begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}\ \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}\ \begin{pmatrix}1&0&0\\0&0&0\\0&0&1\end{pmatrix}\ \begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix}$$

$$\begin{pmatrix}-1&0&0\\0&1&0\\0&0&1\end{pmatrix}\ \begin{pmatrix}1&0&0\\0&-1&0\\0&0&-1\end{pmatrix}\ \begin{pmatrix}1&0&0\\0&0&0\\0&0&-1\end{pmatrix}$$

$$\begin{pmatrix}\cos\theta&-\sin\theta&0\\\sin\theta&\cos\theta&0\\0&0&1\end{pmatrix}\ \begin{pmatrix}\cos\theta&0&-\sin\theta\\0&1&0\\\sin\theta&0&\cos\theta\end{pmatrix}$$

$$\begin{pmatrix}2\cos\theta&0&-2\sin\theta\\0&0&0\\0&0&0\end{pmatrix}\ \begin{pmatrix}2\cos\theta&0&2\sin\theta\\0&0&0\\0&0&0\end{pmatrix}$$

59. On fait effectuer au vecteur $(-2, 1, 2)$ une rotation d'angle $-30°$ par rapport au premier axe de coordonnées puis une rotation d'angle $-45°$ par rapport au second puis d'angle $-90°$ par rapport au dernier : quel vecteur obtient-on ? Donner la matrice de la composition de ces trois rotations. Est-ce encore une rotation ?

60. Si A est la matrice d'une rotation de $\mathbb{R}^3$ d'angle θ, vérifier que $\cos\theta = \frac{1}{2}(\operatorname{Tr} A - 1)$ et que son axe est donné par

$$u = Ax + {}^tAx + (1 - \operatorname{Tr} A)x,$$

où x est un vecteur (non nul) quelconque de $\mathbb{R}^3$.

61. Trouver toutes les applications linéaires du plan qui transforment la ligne d'équation $y = x$ en la ligne d'équation $y = 3x$.

62. Soit A une matrice de taille $m \times n$. Montrer que les vecteurs-colonnes X tels que $AX = 0$ forment un espace vectoriel de dimension supérieure à $n - m$.

63. Soit f l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique (e_1, e_2, e_3) est

$$A = \begin{pmatrix}3&-1&1\\0&2&0\\1&-1&3\end{pmatrix}.$$

a. Montrer que f est un automorphisme.
b. Déterminer la matrice B de f dans la base $e'_1 = (1, 0, -1)$, $e'_2 = (0, 1, 1)$, $e'_3 = (1, 0, 1)$.
c. Calculer B^n. En déduire A^n pour $n \in \mathbb{Z}$.

64. Considérons l'endomorphisme

$$f : \left\{\begin{array}{ccc}\mathbb{R}4 & \longrightarrow & \mathbb{R}^4\\ \begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} & \longmapsto & \begin{pmatrix}-x_1\\x_1+2x_2\\x_1+x_2+x_3\\x_3+x_4\end{pmatrix}\end{array}\right. .$$

a. Donner la matrice M de f dans la base canonique. Quel est son rang ?
b. Trouver une base de $\operatorname{Im} f$ et une base de $\operatorname{Ker} f$.
c. Montrer que $\operatorname{Im} f \cap \operatorname{Ker} f = \{0\}$ et que $\operatorname{Im} f \oplus \operatorname{Ker} f = \mathbb{R}^4$. Cela reste-t-il vrai pour un endomorphisme quelconque ?

65. Soit E un espace vectoriel réel de dimension trois et u un endomorphisme non nul de carré nul.
a. Montrer que $\operatorname{Im} u \subset \operatorname{Ker} u$, $\operatorname{Im} u \neq \{0\}$ et $\operatorname{Ker} u \neq E$. En déduire les dimensions de $\operatorname{Im} u$ et $\operatorname{Ker} u$.
b. Soit e_2 un vecteur non nul de $\operatorname{Im} u$ et e_1 tel que $u(e_1) = e_2$. Justifier l'existence de e_1 et e_2. Montrer que (e_1, e_2) est libre.
c. Montrer que l'on peut choisir e_3 tel que (e_2, e_3) soit une base de $\operatorname{Ker} u$ et (e_1, e_2, e_3) une base de E. Quelle est la matrice de u dans cette base ?
d. Supposons maintenant $u^2 \neq 0$ et $u^3 = 0$. Soit e_1 tel que $u^2(e_1) \neq 0$. Montrer que $(e_1, u(e_1), u^2(e_1))$ est une base de E. Quelle est la matrice de u dans cette base ?

66. Soit (e_1, e_2) une base d'un espace vectoriel E et $v_1 = 2e_1 + 3e_2$, $v_2 = e_1 + 2e_2$.
a. Montrer que (v_1, v_2) est une base de E.
b. Montrer que l'endomorphisme de E défini par $f(e_1) = 2e_1 + e_3$ et $f(e_2) = e_1 + 2e_2$ est bijectif, de trois manières : en utilisant la question précédente, matriciellement, en regardant le noyau de f.
c. Calculer l'image de $xe_1 + ye_2$ par f. Vérifier le résultat matriciellement.
d. Expliciter f^{-1}.

67. Considérons
$$f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} x+y \\ x-y \\ 2x+y \end{pmatrix} \end{array} \right. .$$
a. Donner la matrice de f relativement aux bases canoniques de $\mathbb{R}^2$ et $\mathbb{R}^3$.
b. Le morphisme f est-il bijectif ?
c. Déterminer son noyau.
d. Déterminer son rang et son image.

68. Montrer que les polynômes $1 + X$, $X + X^2, \ldots, X^{n-1} + X^n$, X^n forment une base $\mathscr{B}'_n$ de $\mathbb{R}_n[X]$. Considérons
$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R}_2[X] & \longrightarrow & \mathbb{R}_3[X] \\ P & \longmapsto & XP + X^2P'. \end{array} \right.$$
a. Quelle est la matrice de φ relativement aux bases $(1, X, X^2)$ et $(1, X, X^2, X^3)$?
b. Quelle est la matrice de φ relativement aux bases $\mathscr{B}'_2$ et $\mathscr{B}'_3$?

69. Soient a, b et c des nombres complexes et φ l'endomorphisme de $\mathbb{C}^3$ de matrice
$$\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$$
dans la base canonique $\mathscr{B} = (e_1, e_2, e_3)$.
a. Notons $e'_1 = e_1 + e_2 + e_3$, $e'_2 = e_2$ et $e'_3 = e_3$. Montrer que c'est une base $\mathscr{B}'$ de $\mathbb{C}^3$. Quelle est la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$? de $\mathscr{B}'$ à $\mathscr{B}$?
b. Quelle est la matrice de f dans $\mathscr{B}'$?

70. **a.** Montrer que
$$f : P \longmapsto (4X+1)P - X^2P' - X^3P''$$
est un endomorphisme de $\mathbb{R}_2[X]$.
b. Quelle est la matrice de f dans la base canonique ?
c. Déterminer $f \circ f \circ f \circ f(1 + X + X^2)$.
d. Montrer que f est un automorphisme. Quelle est la matrice de f^{-1} ?
e. Trouver les polynômes P de $\mathbb{R}_2[X]$ tels que
$$(4X+1)P - X^2P' - X^3P'' = 2X^2 - X - 1.$$

71. Soit E un espace vectoriel de dimension trois, muni d'une base (e_1, e_2, e_3) et u un endomorphisme de E tel que $u(e_1) = 0$, $u(e_2) = e_1 + 2e_2 + 3e_3$ et $u(e_3) = e_1$.
a. Déterminer $\operatorname{Im} u$, $\operatorname{Im} u^2$, $\operatorname{Im} u^3$, puis, de manière plus générale, $\operatorname{Im} u^n$ pour $n \in \mathbb{N}^\times$.
b. Montrer que la restriction de u à $\operatorname{Im} u^2$ est une homothétie.
c. Montrer que $E = \operatorname{Im} u^2 \oplus \operatorname{Ker} u^2$.
d. Écrire la matrice de u dans una base constituée de vecteurs de $\operatorname{Im} u^2$ et $\operatorname{Ker} u^2$.

72. Soit $(e_1, \ldots, e_n)$ une base de $\mathbb{R}^n$ et f un endomorphisme. On suppose que $f(e_n) = 0$ et $\forall i \in [\![1, n]\!]$, $f(e_i) \in \operatorname{Vect}\{e_1, \ldots, e_{i-1}\}$.
a. Quelle est la forme de la matrice A de f dans $(e_1, \ldots, e_n)$.
b. Démontrer que $A^n = 0$.
c. Existe-t-il un vecteur x non nul et un réel non nul λ tel que $Ax = \lambda x$?

73. Soit $a \in \mathbb{R}$, considérons
$$f : \left\{ \begin{array}{ccc} \mathbb{R}_n[X] & \longrightarrow & \mathbb{R}_n[X] \\ P & \longmapsto & (X-a)P' + P(a) - P. \end{array} \right.$$
Donner la matrice de f dans la base canonique. Décrire le noyau et l'image de f.

74. **a.** Notons $f_1(x) = e^{-x}$, $f_2(x) = xe^{-x}$ et $f_3(x) = x^2e^{-x}$ et $E = \operatorname{Vect}\{f_1, f_2, f_3\}$ le sous-espace de $\mathscr{F}(\mathbb{R}, \mathbb{R})$. Quelle est la dimension de E ?
b. Montrer que la dérivation est un endomorphisme de E. Donner sa matrice dans la base (f_1, f_2, f_3).

c. Calculer A^n. En déduire la dérivée n^{e} de $g(x) = (3 - 2x + 8x^2)e^{-x}$.

75. Soit $f_a : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ l'endomorphisme dont la matrice dans la base canonique est
$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & a \\ 0 & 1 & 1 \end{pmatrix}.$$
a. Pour quelles valeurs de a l'application f_a est-elle bijective ? surjective ? injective ?
b. Lorsque f_a n'est pas bijective, donner une base de son noyau et de son image.

76. a. Donner la matrice de la dérivation $\mathbb{R}_n[X] \longrightarrow \mathbb{R}_n[X]$ dans une base de votre choix
b. Montrer qu'elle est nilpotente.
c. Trouver tous les sous-espaces invariants par cet endomorphisme.
d. Donner la matrice de la dérication dans la base $(X - a)^k/k!$.

77. a. Donner la matrice de l'application linéaire $(x, y) \longmapsto (x - 2y, -y)$ par rapport aux bases $B_1 = \{(1, 0), (0, 1)\}$ et $B_2 = \{(2, 1), (-3, 4)\}$.
b. Donner la matrice de l'application linéaire
$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x + 2y - z \\ -y \\ x + 7z \end{pmatrix}$$
par rapport à la base canonique $(e_i)_i$ (au départ) et la base $(e_1, e_1 + e_2, e_1 + e_2 + e_3)$ à l'arrivée.

78. Donner la matrice de la dérivation $D : \mathbb{R}_n[X] \longrightarrow \mathbb{R}_n[X]$ dans la base canoniques

79. Donner la matrice de l'opération « prendre la primitive qui s'annule en 0 », $\mathbb{R}_n[X] \longrightarrow \mathbb{R}_{n+1}[X]$ dans la base de votre choix.

80. a. Notons $A = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Montrer que $X \longmapsto AX{}^tA$ est un endomorphisme de l'espace de matrices symétriques. Donner sa matrice par rapport à une base de votre choix.
b. Soient A et B des matrices de taille deux. Donner la matrice de l'application linéaire $X \longmapsto AXB$ dans la base $(e_{11}, e_{12}, e_{21}, e_{22})$.
c. Soit A une matrice de taille $k \times m$ et B une matrice de taille $n \times p$.Montrer que $M \longmapsto AMB$ est une application linéaire $\mathscr{M}_{m,n} \longrightarrow \mathscr{M}_{k,p}$. Donner sa matrice dans une base de votre choix.

81. Soit T un endomorphisme d'un espace vcectoriel de dimension deux qui n'est pas une multiplication par un scalaire. Montrer qu'il existe un vecteur v tel que (Tv, v) soit une base. Donner la matrice de T dans cete base.

Divers

82. (Graphes) a. Soit M la matrice d'adjacence d'un graphe orienté. Montrer que le coefficient en position (i, j) de M^k est le nombre de chemins de i à j de longueur k.
b. Généraliser le résultat précédent aux graphes non orientés.
c. Montrer que le nombre de triangles dans un graphe non orienté de matrice d'adjacence M est $\frac{1}{6} \operatorname{Tr} M^3$.

83. (Chaînes de Markov) On remarque 3/5 des descendants de fumeurs sont eux-mêmes des fumeurs et que la proportion n'est que de 1/5 chez les descendants de non-fumeurs. On suppose que la moitié de la population fume. En effectuant toutes les hypothèses simplificatrices nécessaires, donner la proportion de fumeurs dans une génération, puis dans deux générations. Peut-on espérer une disparition des fumeurs ? En cas contraire, peut-on espérer une stabilisation de leur nombre ?

Polynômes et fractions rationnelles

À savoir

- Division euclidienne des polynômes ;
- Algorithme d'Euclide ;
- Décomposition en produit de facteurs irréductibles ;
- Formule de Taylor–Lagrange pour les polynômes ;
- Liens entre coefficients et racines d'un polynôme ;
- Décomposition d'une fraction rationnelle en éléments simples.

Polynômes

1. En utilisant le théorème de décomposition d'un polynôme à coefficients réels en produit de facteurs irréductibles, montrer que tout polynôme réel de degré impair possède une racine. Connaissez-vous une autre démonstration de ce résultat ?

2. a. Factoriser $X^4 + X^3 + 3X^2 - 5X$ sur $\mathbb{R}$ puis sur $\mathbb{C}$.
b. Montrer que $Q = X^5 + X^3 - 8X^2 - 8$ est divisible par $X^3 - 8$. Le factoriser sur $\mathbb{R}$ puis sur $\mathbb{C}$.

3. Notons $P = X^4 + 2X^3 + 3X^2 + 2X + 1$ et $j = e^{2\pi i/3}$. Calculer $P(j)$ et $P'(j)$ et en déduire la décomposition de P dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

4. Décomposer $P = X^5 - X^3 + 2X - 125$ selon les puissances de $X - 3$.

5. Pour quelles valeurs de n le polynôme $X^2 + X + 1$ divise-t-il $X^{2n} + X^n + 1$?

6. Que dire des coefficients, puis des racines, d'un polynôme pair ? d'un polynôme impair ?

7. Quels sont les polynômes multiples de leur dérivée ?

8. a. Quel est le degré d'un produit de polynôme ? Que dire du degré d'une somme de polynômes ?
b. La *valuation* d'un polynôme est le degré du monôme non nul de plus bas degré. Quel est la valuation d'un produit ? Que dire de la valuation d'une somme ?

9. Montrer qu'un polynôme P possède une racine multiple si et seulement si $P' \wedge P \neq 1$.

10. Trouver tous les polynômes P tels que $P(X^2) = P(X)P(X+1)$.

11. Développer
$$(1+X)(1+X^2)(1+X^4)\cdots(1+X)^{2^n}.$$

12. Montrer que pour tout n, il existe un polynôme P_n tel que
$$P_n\left(X + \frac{1}{X}\right) = X^n + \frac{1}{X^n}.$$

13. En considérant P'/P, montrer que les racines de P' sont contenues dans l'enveloppe convexe de celles de P. Que se passe-t-il si toutes les racines de P sont réelles ?

14. (Polynômes de Tchebychev) Pour $x \in [0,1]$, on pose $P_n(x) = \cos(n \arccos x)$.
a. Calculer P_1, P_2, P_3.
b. Calculer P_n.
c. Montrer $P_{n+1}(x) = 2xP_n(x) - P_{n-1}(x)$.
d. Montrer que P_n est un polynôme.
e. Quel est son degré ? Son terme dominant ? Calculer $P_n(1)$ et $P_n(-1)$.
f. Quelles sont les racines de P_n sur $[-1,1]$? Sur $\mathbb{R}$?
g. Quelles sont les racines de P'_n ?

Polynômes symétriques

15. Soient α, β et γ les racines du polynôme $X^3 + aX^2 + bX + c$.
a. Exprimer a, b et c en fonction de α, β et γ.

b. Exprimer $\alpha^2+\beta^2+\gamma^2$ en fonction de a, b et c.

16. a. Quelles sont les solutions complexes de $Y^n=1$? En déduire la factorisation du polynôme $Q(Y)=Y^n-1$ puis celle de $P(X)=(X+1)^n-1$.
b. Développer P à l'aide de la formule du binôme de Newton.
c. En déduire la valeur de

$$\prod_{k=1}^{n-1}\left(\exp\frac{2k\pi i}{n}-1\right)$$

puis celle de

$$\prod_{k=1}^{n-1}\sin\frac{k\pi}{n}.$$

17. Comme dans l'exercice précédent, calculer

$$\sum_{i=1}^{p}\cot^2\frac{k\pi}{2p+1} \text{ et } \prod_{i=1}^{p}\cot^2\frac{k\pi}{2p+1}$$

à l'aide du polynôme $(X-1)^n-(X+1)^n$.

Arithmétique de polynômes

18. Montrer que $X^4+X^2+r^2$ et X^2-X+r, où $r\in\mathbb{R}$, sont premiers entre eux dans $\mathbb{R}[X]$.

19. a. Quels sont les polynômes de degré quatre dont le reste de la division euclidienne par X^2+1 est égal à X ?
b. Trouver tous les polynômes de degré sept dont le reste de la division par $(X+2)^4$ est 2 et le reste de la division par $(X-2)^4$ est -2.

20. Soient a, b et c trois réels distincts.
a. Quel est le reste de la division euclidienne de P par $X-a$?
b. Quel est le reste de la division euclidienne de P par $(X-a)(X-b)(X-c)$?
c. Examiner le cas $a=b=c$?

21. Quel est le reste de la division euclidienne de $(X\cos t+\sin t)^n$ par X^2+1 ?

22. Déterminer tous les couples (U,V) de polynômes de $\mathbb{R}[X]$ tels que

$$(X^7+1)U+(X^3-1)V=X+1.$$

23. a. Notons $P_n=X^n+X^{n-1}+\cdots+1$. À l'aide de l'algorithme d'Euclide, montrer que $P_n\wedge P_m=P_{n\wedge n}$.
b. Idem pour $P_n=X^n-1$.

24. Soient f, g et h des polynômes.
a. Montrer que si f et g sont premiers entre eux, et $h\mid f$, alors $h\wedge g=1$.
b. Montrer que si f et g sont premiers entre eux, alors $(fh)\wedge g=h\wedge g$.

25. Trouver tous les polynômes P dont le reste de la division euclidienne par $(X-1)^3$ et par $(X+1)^3$ est égal à 1.

Fractions rationnelles

26. Décomposer en éléments simples.

$$\frac{X+1}{X^2(X-1)^2} \qquad \frac{X^2+9}{(X+2)(X^2+2X+5)}$$

$$\frac{1}{X^2(1+X^3)} \qquad \frac{X^6+1}{X^4-1}$$

$$\frac{1}{3X^4+10X^2+3} \qquad \frac{X+1}{X(X^2+X+1)^2}$$

27. En utilisant ses propriétés de parité, décomposer

$$\frac{16X}{(X-1)^3(X+1)^3}$$

en éléments simples. En déduire ses primitives sur $]-1,1[$.

28. On veut décomposer

$$F(X)=\frac{2X-1}{(X+2)(X+1)^4}$$

en éléments simples.
a. Effectuer le changement de variable $Y=X+1$ puis effectuer la division de $-3+2Y$ par $1+Y$ selon les puissances croissances, jusqu'à un reste d'ordre quatre. Conclure.
b. Retrouver cette décomposition en commençant par obtenir le terme en $1/(X+2)$ puis en utilisant la formule de Taylor–Lagrange.

29. etc.

Calculs d'intégrales et de primitives

À savoir

- Intégrer par parties, par exemple pour calculer des intégrales par récurence ;
- Intégrer des fracions rationnelles ;
- Intégrer des fracions rationnelles trigonométriques en faisant au changement de variables ;

Voir feuille manuscrite.

Intégrale de Riemann

À savoir

➠ Reconnaître une somme de Riemann et calculer sa limite ;
➠ Utiliser le théorème de la moyenne pour étudier certaines intégrales dépendant d'un paramètre ;
➠ Démontrer certaines inégalités à l'aide de celle de Cauchy–Schwartz.

Sommes de Riemann

1. Rappelons que si $f : [a, b] \longrightarrow \mathbb{R}$ est continue, alors

$$\lim_{n\to\infty} \frac{b-a}{n} \sum_{k=1}^{n} f\left(a + k\frac{b-a}{n}\right) = \int_a^b f(t)\,dt.$$

Calculer les limites suivantes.

a. $\displaystyle\lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{n+k}$.

b. $\displaystyle\lim_{n\to\infty} \sum_{k=1}^{n} \frac{n+k}{n^2+k^2}$.

c. $\displaystyle\lim_{n\to\infty} \sum_{k=1}^{n+1} \frac{k}{n^2} \sin\left(\frac{k\pi}{n+1}\right)$.

d. $\displaystyle\lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{n} \exp\left(\frac{k+n}{n}\right)$.

e. $\displaystyle\lim_{n\to\infty} \prod_{k=1}^{n} \left(2 + \frac{k}{n}\right)^{1/n}$.

f. $\displaystyle\lim_{n\to\infty} \left(\frac{(2n)!}{n!\,n^n}\right)^{1/n}$.

Inégalité de Cauchy–Schwartz

2. Soient f et g deux fonctions réelles continues sur $[a, b]$.

a. Montrer que $P(X) = \int_a^b (f(t) + Xg(t))^2\,dt$ est un polynôme du second degré. Quel est son discriminant ?

b. En déduire l'*inégalité de Cauchy–Schwartz*,

$$\left|\int_a^b fg\right| \leqslant \sqrt{\int_a^b f^2} \cdot \sqrt{\int_a^b g^2}.$$

c. Supposons que $f(x)g(x) > 1$ pour tout $x \in [a, b]$. Montrer que

$$\left(\int_a^b f\right)\left(\int_a^b g\right) \geqslant (b-a)^2.$$

Théorème de la moyenne

3. Considérons $\displaystyle f(x) = \int_x^{2x} \frac{dt}{\ln(1+t^2)}$.

a. Quel est le domaine de définition D_f de f ? Quelles sont ses limites aux bornes de D_f ?

b. Montrer que f est impaire.

c. Montrer que f est dérivable et calculer sa dérivée.

4. Considérons $\displaystyle f(x) = \int_x^{x^2} \frac{dt}{\ln t}$.

a. Quel est le domaine de définition de f ? Étudier le signe de f.

b. Montrer que l'on peut prolonger f par continuité en 0 et en 1. Notons $\tilde{f}$ ce prolongement.

c. Étudier la dérivabilité de f puis de $\tilde{f}$.

d. Dresser le tableau de variations de $\tilde{f}$.

e. Trouver le limite de f en $+\infty$ et la nature de la branche infinie.

5. Étudier $\displaystyle f(x) = \int_x^{2x} e^{t^2}\,dt$.

Divers

6. Soit $f : [-1, 1] \longrightarrow \mathbb{R}_+$ une fonction continue.

a. Rappeler pourquoi $\displaystyle M = \sup_{x\in[-1,1]} f(x)$ existe.

b. Montrer $\forall n$ $\displaystyle\left(\int_{-1}^{1} f(x)^n\,dx\right)^{1/n} \leqslant 2^{1/n} M$.

c. Montrer que pour tout $\varepsilon > 0$, il existe un intervalle $[a, b] \subset [-1, 1]$ sur lequel $f \geqslant M - \varepsilon$.

d. En déduire que pour tout n,

$$\left(\int_{-1}^{1} f(x)^n \, dx\right)^{1/n} \geqslant 2^{1/n}(M - \varepsilon).$$

e. Déterminer la limite de

$$\left(\int_{-1}^{1} f(x)^n \, dx\right)^{1/n}.$$

7. Si f est continue sur $[0, 1]$, calculer

a. $\displaystyle\lim_{n\to\infty} \int_0^1 x^n f(x) \, dx.$

b. $\displaystyle\lim_{n\to\infty} n \int_0^{1/n} f(x) \, dx.$

8. Calculer les limites suivantes.

$$\lim_{x\to 1} \frac{1}{x-1} \int_1^x \frac{t^2 \, dt}{1+t^8}, \qquad \lim_{x\to 0^+} \frac{1}{x} \int_0^x \frac{dt}{\ln t},$$

$$\lim_{n\to\infty} \frac{1}{n} \int_1^n \frac{1}{t} \sin\frac{n}{t} \, dt, \qquad \lim_{n\to\infty} \int_0^1 \sin^n t \, dt.$$