1 Logique

Exercice **de base.**
P : le nombre 91 est un multiple de 7.
Traduction : $\exists k \in \mathbf{N},\ \ 91 = 7 \times k$.
Négation : $\forall k \in \mathbf{N},\ \ 91 \neq 7 \times k$.
La proposition P est vraie, en voici la preuve :
Posons $k = 13$.
Alors k est bien un entier naturel et $7 \times k = 91$.
Donc 91 est bien un multiple de 7.

Q : le tiers de 2 n'est pas un nombre entier.
Traduction : $\forall a \in \mathbf{Z},\ \ \frac{2}{3} \neq a$.
Négation : $\exists a \in \mathbf{Z},\ \ \frac{2}{3} = a$.
La proposition Q est vraie, en voici la preuve :
Supposons par l'absurde que la négation de Q est vraie.
Alors il existe $a \in \mathbf{Z}$ tel que $\frac{2}{3} = a$.
Donc $2 = 3a$.
Comme a est un entier, nous en déduisons que 2 est un multiple de 3.
Cela est absurde, donc la négation de Q ne peut pas être vraie.
Donc Q est vraie.

Autre preuve de Q plus directe :
Comme 2 et 3 sont des nombres strictement positifs, nous déduisons que $\frac{2}{3} > 0$.
De plus, comme $2 < 3$, nous déduisons $\frac{2}{3} < 1$.
Ainsi $\frac{2}{3}$ est un nombre rationnel compris strictement entre 0 et 1.
En particulier $\frac{2}{3}$ n'est pas un nombre entier.

Exercice **Opérations élémentaires**

1. Soient a et b des nombres. Démontrer l'identité remarquable : $(a+b)^2 = a^2 + 2ab + b^2$.
2. Quelles propriétés de l'addition et de la multiplication ont été utilisées ?
3. En utilisant l'identité, montrer que le polynôme $X^2 + 2X + 2$ n'a pas de racine réelle.
4. On considère les nombres écrits sous forme décimale, arrondis au dixième. Par exemple dans ce contexte, $1{,}4 \times 0{,}2 = 0{,}3$.
   L'identité est-elle alors satisfaite pour $a = 1{,}1$ et $b = 0{,}2$? Expliquer.

Justifions l'identité remarquable en précisant à chaque étape la propriété utilisée :

$$\begin{aligned}
(a+b)^2 &= (a+b) \times (a+b) && \text{définition de la puissance 2}\\
&= a \times (a+b) \ + \ b \times (a+b) && \text{distributivité}\\
&= (a \times a \ + \ a \times b) \ + \ (b \times a \ + \ b \times b) && \text{distributivité}\\
&= a \times a \ + \ (a \times b) \ + \ b \times a) \ + \ b \times b) && \text{associativité de l'addition}\\
&= a^2 \ + \ 2ab \ + \ b^2 && \text{commutativité de la multiplication}
\end{aligned}$$

Les nombres a et b pourraient en fait désigner n'importe quel objet mathématique (une fonction par exemple). Le résultat reste valable tant que l'addition et la multiplication utilisées sont associatives, commutatives et la seconde est distributive par rapport à la première.
Dans ce contexte, la notation $2ab$ est une abréviation de $a \times b + a \times b$.

Par exemple, l'identité est encore valable dans le monde des polynômes, dans lequel X n'est qu'un symbole abstrait. Ainsi, en faisant apparaître la **forme canonique** du polynôme, afin d'utiliser l'identité, nous obtenons :

$$X^2 + 2X + 2 = (X^2 + 2X + 1) + 1 = (X + 1)^2 + 1.$$

Écrit sous cette forme, il est facile de justifier le résultat attendu.
Soit $x \in \mathbf{R}$. Alors, par propriété du carré, $(x + 1)^2 \geqslant 0$.
Donc $(x + 1)^2 + 1 \geqslant 1$.
En particulier, $(x + 1)^2 + 1 \neq 0$.
Nous avons ainsi démontré que pour tout nombre réel x, $x^2+2x+2 \neq 0$: le polynôme X^2+2X+2 ne possède pas de racine réelle.

Posons $a = 1{,}1$ et $b = 0{,}2$ et effectuons tous les calculs en arrondissant chaque résultat au dixième près :

$$(a+b)^2 = 1{,}3^2 = 1{,}69 = 1{,}7$$

$$a^2 = 1{,}1^2 = 1{,}21 = 1{,}2 \qquad ab = 1{,}1 \times 0{,}2 = 0{,}22 = 0{,}2 \qquad b^2 = 0{,}2^2 = 0{,}04 = 0{,}0$$

$$\text{donc} \quad a^2 + 2ab + b^2 = 1{,}2 + 0{,}4 + 0{,}0 = 1{,}6.$$

Conclusion : dans ce contexte, $(a + b)^2 \neq a^2 + 2ab + b^2$. L'identité n'est pas satisfaite.
La raison est que la multiplication arrondie au dixième n'est ni associative, ni distributive par rapport à l'addition. C'est un mauvais cadre pour faire de l'algèbre ! Nous ne travaillons jamais en algèbre avec des nombres écrits sous forme décimale.

Exercice **Raisonnements algébriques**

1. Résoudre dans $\mathbf{R}$ l'équation : $\dfrac{\sqrt{2-x}}{x-1} = \dfrac{2}{3}$.

   Nous commençons par chercher les éventuelles solutions de l'équation. Nous partons pour cela de l'égalité, ce qui revient à supposer qu'il existe bien un réel x tel que $\dfrac{\sqrt{2-x}}{x-1} = \dfrac{2}{3}$.
   Nous allons ensuite manipuler algébriquement cette égalité afin de déduire les valeurs possibles de x.

   Premier réflexe : il faut supprimer les fractions. La fraction $\frac{a}{b}$ n'est qu'un symbole qui ne désigne rien de plus que le nombre qui, multiplié par b, est égal à a. La seule façon d'exploiter une fraction est, à un moment donné, de la multiplier par son dénominateur. Appliquons cela à notre équation et multiplions des deux côtés par $3(x-1)$. Nous obtenons :

   $$3\sqrt{2-x} = 2(x-1).$$

   Attention, soyons tout de même rigoureux ! Pour que cette nouvelle égalité soit équivalente à la première, il faut préciser que $x \neq 1$.

Continuons et attaquons désormais la racine carrée. De même qu'une fraction n'est qu'une expression symbolique, $\sqrt{c}$ n'est qu'un symbole qui désigne le nombre positif qui élevé au carré égale c. La seule façon d'exploiter cette définition est donc d'élever la racine au carré. Appliquons cela à notre égalité et élevons au carré des deux côtés :

$$9(2-x) = 4(x-1)^2.$$

Là encore, soyons rigoureux, cette égalité n'est équivalente à la précédente que si on précise que $2-x$ et $x-1$ doivent être positifs (si nous repassons en effet à la racine carrée dans cette dernière égalité, nous obtenons $3\sqrt{2-x} = 2|x-1|$).

Les étapes suivantes sont plus classiques : on développe les expressions et on passe tous les termes à gauche de l'égalité. On obtient ainsi : $-4x^2 - x + 14 = 0$. C'est une équation polynomiale de degré deux, de discriminant $\Delta := (-1)^2 - 4(-4)(14) = 225$. Les solutions de cette dernière équation sont donc $x_1 := \frac{1+\sqrt{225}}{-8}$ et $x_2 := \frac{1-\sqrt{225}}{-8}$. Les solutions obtenues sont des expressions algébriques, certes peu jolies, mais parfaitement exactes ! Cela étant dit, nous pouvons remarquer que $\sqrt{225} = 15$ et simplifier les expressions : $x_1 = -2$ et $x_2 = \frac{7}{4}$.

Avons-nous terminé la résolution ? Non ! D'après les remarques faites au cours de notre raisonnement, il nous reste des points à vérifier. Nous avons simplement démontré la chose suivante : si l'équation possède des solutions, il ne peut s'agir que de x_1 ou x_2. Vérifions alors :

$$\frac{\sqrt{2-x_1}}{x_1-1} = \frac{\sqrt{2-(-2)}}{-2-1} = -\frac{2}{3} \qquad \frac{\sqrt{2-x_2}}{x_2-1} = \frac{\sqrt{2-\frac{7}{4}}}{\frac{7}{4}-1} = \frac{2}{3}.$$

Nous constatons que x_1 n'est pas solution de l'équation. C'est cohérent avec nos remarques : x_1 ne satisfait en effet pas la condition $x - 1 \geqslant 0$ que nous avions établie.

Conclusion : l'équation a pour unique solution : $x_2 = \frac{7}{4}$.

2. Résoudre dans $\mathbf{R}$ l'inégalité : $\dfrac{2x+1}{x-1} < 1$.

Rappelons la règle de manipulation algébrique d'un produit dans une inégalité : si $c > 0$, $a < b \Leftrightarrow ac < ab$; si $c < 0$, $a < b \Leftrightarrow ac > ab$.

Partons de l'inégalité, distinguons des cas et raisonnons par équivalence :
Soit $x \in \mathbf{R}$.

Si $x - 1 > 0$, alors

$$\frac{2x+1}{x-1} < 1 \Leftrightarrow 2x + 1 < x - 1 \Leftrightarrow x < -2.$$

Or nous avons supposé $x > 1$ ce qui est incompatible avec cette dernière inégalité. Il n'existe donc pas de réel x tel que $x - 1 > 0$ et $\dfrac{2x+1}{x-1} < 1$.

Si $x - 1 < 0$, alors

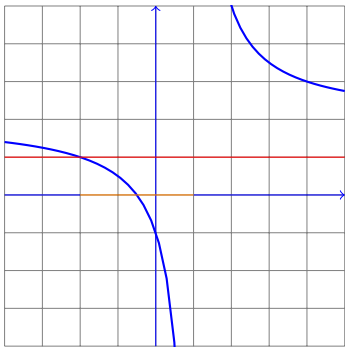
$$\frac{2x+1}{x-1} < 1 \Leftrightarrow 2x + 1 > x - 1 \Leftrightarrow x > -2.$$

Or $x < 1$ par hypothèse, donc nous concluons dans ce cas que les solutions sont les nombres de l'intervalle $]-2, 1[$.

Le cas $x = 1$ est immédiatement exclus par l'inégalité étudiée.

Conclusion : l'ensemble des solutions du problème est l'intervalle $]-2, 1[$.

Remarque : une méthode reposant sur l'analyse est possible. Il s'agit d'étudier la fonction $f : x \mapsto \frac{2x+1}{x-1}$. C'est facile si on la réécrit ainsi : $f(x) = \frac{2(x-1)+3}{x-1} = 2 + \frac{3}{x-1}$. Son graphe est l'hyperbole représentée ci-dessous :



Les valeurs de x pour lesquelles $f(x) < 1$ sont bien celles comprises dans l'intervalle $]-2, 1[$.

Exercice **Formulation mathématique**

• **L'entier n est un carré** : $\exists k \in \mathbf{N},\ \ n = k^2$.
Sa négation est $\forall k \in \mathbf{N},\ \ n \neq k^2$.

• **L'entier n n'est pas divisible par 7**. Il est plus facile de définir sa négation qui est que n est divisible par 7 : $\exists \ell \in \mathbf{Z},\ n = 7\ell$.
La proposition se traduit ainsi en prenant la négation de cette proposition : $\forall \ell \in \mathbf{Z},\ n \neq 7\ell$.

• **L'entier n est le minimum de la partie A**. Cette proposition dit deux choses : n est un élément de A et il en est le plus petit. On la traduit par : $n \in A$ et $\forall m \in A,\ m \geqslant n$.
Sa négation est : $n \notin A$ ou $\exists m \in A,\ m < n$.

• **La partie A n'a pas de maximum**. Commençons par sa négation, la définition d'un maximum étant analogue à celle du minimum vu ci-dessus : $\exists p \in A,\ \forall m \in A, m \leqslant p$.
La proposition initiale se traduit alors en prenant la négation de celle-ci : $\forall p \in A,\ \exists m \in A,\ m < p$.
Autrement dit, pour tout élément de A, il est possible de trouver un autre élément de A qui lui est supérieur.

• **La fonction f est bornée** : il existe des valeurs réelles qui permettent d'encadrer toutes les valeurs de la fonction.

$$\exists a \in \mathbf{R}, \exists b \in \mathbf{R}, \forall x \in \mathbf{R}, a \leq f(x) \leq b$$

ou encore $\exists M \in \mathbf{R}, \forall x \in \mathbf{R}, |f(x)| \leq M$.
Prenons la négation : on applique bêtement les règles de la négation à chacune des parties de la proposition. Attention, $a \leq f(x) \leq b$ signifie $a \leq f(x)$ et $f(x) \leq b$, sa négation contiendra un

"ou".
Une fonction f n'est pas bornée si $\forall a \in \mathbf{R}, \forall b \in \mathbf{R}, \exists x \in \mathbf{R}, f(x) < a$ ou $f(x) > b$ (ou avec l'autre proposition $\forall M \in \mathbf{R}, \exists x \in \mathbf{R}, |f(x)| > M$).
Littéralement, cette proposition signifie que f n'est pas majoré ou n'est pas minoré.

• **Les courbes des fonctions f et g se rencontrent** : $\exists x \in \mathbf{R}, f(x) = g(x)$.
Négation : les courbes ne se croisent pas si $\forall x \in \mathbf{R}, f(x) \neq g(x)$.

• **La fonction réelle $x \mapsto x^2$ n'est pas bornée.** Il s'agit donc de démontrer la négation vue plus haut : $\forall M \in \mathbf{R}, \exists x \in \mathbf{R}, |x^2| > M$.
Soit $M \in \mathbf{R}$.
Posons $x = \sqrt{|M| + 1}$ *(obtenu après une recherche au brouillon basée sur le graphe de la fonction. Le "+1" est arbitraire, on aurait pu prendre n'importe quel nombre strictement positif).*
Alors $x^2 = |M| + 1$.
Donc $x^2 > M$.
On a bien démontré que la fonction $x \mapsto x^2$ est non bornée.

• **La fonction $x \mapsto \cos^2(x)+2$ est bornée.** Cela repose sur le fait (bien connu) que la fonction cosinus est bornée par -1 et 1. Passons à la démonstration :
Soit $x \in \mathbf{R}$. On sait que : $-1 \leq \cos(x) \leq 1$.
Donc $|\cos(x)| \leq 1$.
Donc $0 \leq \cos^2(x) \leq 1$. *(Attention, on ne peut pas passer au carré avec l'encadrement précédent car la fonction carré n'est pas croissante sur $\mathbf{R}$, seulement sur $\mathbf{R}_+$.)*
Donc $2 \leq \cos^2(x) + 2 \leq 3$.
Ceci étant vraie pour tout nombre réel x, on a bien démontré que la fonction considérée était bornée par les réels $a = 2$ et $b = 3$.

• **Leurs graphes s'intersectent.** Il s'agit de montrer que l'équation $x^2 = \cos^2(x) + 2$ admet une solution. Mais cette équation est impossible à résoudre explicitement. Nous allons donc chercher un argument général d'existence d'une solution sans la déterminer réellement.
Définissons la fonction $g : x \mapsto x^2 - (\cos^2(x) + 2)$.
Il s'agit d'une fonction continue sur $\mathbf{R}$.
De plus, $g(0) = -3$ et $g(\pi) = \pi^2 - 3 > 0$.
D'après le théorème des valeurs intermédiaires, la fonction g s'annule sur l'intervalle $]0, \pi[$: $\exists x \in]0, \pi[, g(x) = 0$.
On en déduit $\exists x \in]0, \pi[, x^2 = \cos^2(x) + 2$.
On a bien montré que les deux courbes s'intersectaient.

Exercice **Traductions et démonstrations**

— $\forall n \in \mathbf{N}, (6|n \wedge 4|n) \implies 24|n$: si un entier est divisible par 6 et par 4, alors il est divisible par 24.
Ce résultat est faux et il suffit de donner un contre-exemple pour l'infirmer. Prenons $n = 12$.
Alors n est bien divisible par 6 et 4 mais il n'est pas divisible par 24.
On a ainsi bien démontré la négation de la proposition :

$$\exists n \in \mathbf{N}, 6|n \text{ et } 4|n \text{ et } 24 \nmid n.$$

— $\forall n \in \mathbf{N}, (6|n \wedge n|40) \implies n \in \mathbf{P}$: si un entier est divisible par 6 et divise 40, alors il est premier.

Ce résultat est vrai. La première partie de l'implication étant toujours fausse (si un entier pouvait être divisible par 6 et diviser 40, alors 6 diviserait 40), l'implication est elle-même toujours vraie. Pour s'en convaincre, regardons la négation de la proposition :

$$\exists n \in \mathbf{N}, 6|n \text{ et } n|40 \text{ et } n \notin \mathbf{P}.$$

Comme il est impossible de trouver un entier vérifiant ces 3 conditions, cette proposition est clairement fausse. Donc la proposition initiale est bien vraie.

— $\forall p \in \mathbf{P}, \forall a \in \mathbf{N}, \forall b \in \mathbf{N},\ (p|a \text{ et } p|b \implies p|\frac{a+b}{2})$: si un nombre premier divise deux entiers, alors il divise leur moyenne.
Cette proposition est fausse. Pour le justifier, il suffit de donner un contre-exemple. Soit $p = 2$, $a = 4$ et $b = 6$. On a bien $p \in \mathbf{P}$, $p|a$ et $p|b$ mais la conclusion n'est pas satisfaite : p ne divise pas 5 qui est la moyenne de a et b.

— $\forall n \in \mathbf{N} \setminus \{0, 1\},\ \exists p \in \mathcal{P}, \exists q \in \mathcal{P}, 2n = p + q$: tout nombre pair supérieur à 4 peut s'écrire comme la somme de deux nombres premiers.
On pense fortement que ce résultat est vrai, mais il ne s'agit pour le moment que d'une conjecture.

— $\forall n \in \mathbf{N}, 2^n - 1 \in \mathbf{P} \implies n \in \mathbf{P}$: si l'entier $2^n - 1$ est premier, alors nécessairement, l'entier n est premier. Ou mieux : si le nombre précédent une puissance de 2 est premier, alors l'exposant de 2 est également premier.

Ce résultat est vrai. Montrons-le par contraposée : $\forall n \in \mathbf{N}, n \notin \mathbf{P} \implies 2^n - 1 \notin \mathbf{P}$.
Soit $n \in \mathbf{N}$.
Supposons que n n'est pas premier.
Remarquons déjà que le résultat est vérifié si $n = 0$ ou $n = 1$.
Supposons maintenant $n \neq 0$ et $n \neq 1$. Alors, comme n n'est pas un nombre premier, il existe des entiers r et s tels que $n = rs$ avec $r \neq 1$ et $s \neq 1$. Montrons alors que $2^n - 1$ n'est pas un nombre premier.
On a $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1$. Posons $a = 2^r$ pour faire apparaître une identité classique.
Ainsi $2^n - 1 = a^s - 1^s = (a - 1)(a^{s-1} + a^{s-2} + \cdots + a^2 + a + 1) = (a - 1)\sum_{i=0}^{s-1} a^i$.
Comme $r > 1$, $a \geq 4$ et en particulier $a - 1 > 1$. Comme $s \neq 1$, la somme ci-dessus contient au moins deux termes et en particulier elle est strictement supérieure à 1.
Ainsi, $2^n - 1$ est le produit de deux entiers différents de 1. Ce n'est donc pas un nombre premier.
Par contraposée, nous avons montré que si $2^n - 1$ est premier, alors n est premier.

— $\forall x \in \mathbf{R},\ x^2 \geq x$: tout nombre réel est inférieur à son carré.
Ce résultat est faux. En effet, pour $x = 1/2$ par exemple, $x^2 = 1/4$ est strictement inférieur à x. Ainsi $\exists x \in \mathbf{R},\ x^2 < x$.

— $\forall x \in \mathbf{R}, \exists! y \in \mathbf{R}, xy = 1$: tout nombre réel admet un unique inverse.
Ce résultat est faux : le nombre 0 n'admet pas d'inverse dans $\mathbf{R}$. C'est donc la négation de cette proposition qui est vraie : $\exists x \in \mathbf{R}, (\forall y \in \mathbf{R}, xy \neq 1)$ ou $(\exists y_1 \in \mathbf{R}, \exists y_2 \in \mathbf{R}, y_1 \neq y_2 \text{ et } xy_1 = xy_2 = 1)$. À noter que 0 permet de satisfaire la première partie de cette négation.
En revanche la proposition suivante est vraie : $\forall x \in \mathbf{R}^*, \exists! y \in \mathbf{R}, xy = 1$.

Exercice **Traductions et démonstrations : suite.**

$$\forall x \in \mathbf{R}, \exists a \in \mathbf{Z}^*, \exists b \in \mathbf{Z}, ax^2 = b$$

Traduction : tout nombre réel a pour carré un nombre rationnel.
Remarque : les nombres rationnels apparaissent lorsqu'on réécrit l'égalité ainsi : $x^2 = \frac{b}{a}$. Il est important de constater qu'il s'agit bien à droite d'un nombre rationnel car les nombres a et b sont des entiers relatifs. La condition $a \neq 0$ est nécessaire pour que la proposition ne soit pas stupide. Si a peut être nul, alors la proposition est trivialement vraie en prenant pour tout x : $a = b = 0$.

Si x est rationnel, la proposition $\exists a \in \mathbf{Z}^*, \exists b \in \mathbf{Z}, ax^2 = b$ est vraie. En effet, le carré d'un nombre rationnel est encore un nombre rationnel. Si x est irrationnel, cela semble faux. Il existe cependant des nombres irrationnels pour lesquels le résultat est juste.

Posons $y = \sqrt{2}$. Il s'agit bien d'un nombre irrationnel (démonstration par l'absurde vues en analyse). Alors $y^2 = 2$. Donc $1 \times y^2 = 2$. En posant $a = 1$ et $b = 2$, nous avons montré : $\exists a \in \mathbf{Z}^*, \exists b \in \mathbf{Z}, ay^2 = b$.

La proposition initiale est tout de même fausse. Nous allons en effet démontrer que sa négation est vraie.

$$\exists x \in \mathbf{R},\ \forall a \in \mathbf{Z}^*, \forall b \in \mathbf{Z},\quad ax^2 \neq b.$$

Reprenons le nombre y défini précédemment : c'est un nombre irrationnel tel que y^2 est rationnel.
Posons alors $x = y + 1$.
Soient $a \in \mathbf{Z}^*$ et $b \in \mathbf{Z}$, et montrons que $ax^2 \neq b$.
Supposons par l'absurde que $ax^2 = b$.
Alors $a(y+1)^2 = b$, donc $y^2 + 2y + 1 = b$.
Donc $y = \frac{1}{2}(b - y^2 - 1)$.
Or nous savons que y^2 est rationnel, ainsi que b puisque c'est un entier.
Comme une somme de nombres rationnels est encore un nombre rationnel, nous déduisons que $\frac{1}{2}(b - y^2 - 1)$ est encore un nombre rationnel.
Donc y est rationnel, ce qui est faux.
Nous concluons ainsi que $ax^2 \neq b$ et la négation de notre proposition est ainsi démontrée.
Donc la proposition initiale est fausse.

Remarque : nous n'avons pas utilisé le fait que y est égal à $\sqrt{2}$. Nous avons seulement utilisé le fait que c'est un nombre irrationnel dont le carré est rationnel.
Le choix de $x = y + 1$ est arbitraire, bien d'autres nombres permettent d'infirmer la proposition. Par exemple, si le nombre y est positif, on peut poser $x = \sqrt{y}$. Alors $x^2 = y$ n'est pas un nombre rationnel et on obtient un nouveau contre-exemple.

Il existe une fonction définie sur $\mathbf{R}$ dont le graphe intersecte toutes les droites du plan.

— $\exists x \in \mathbf{R},\ f(x) = 2x + 3$.
— On veut que la proposition précédente soit vérifiée pour toute droite du plan. Il s'agit donc de faire varier les deux coefficients permettant de définir la droite. On peut ainsi écrire :

$$\exists f : \mathbf{R} \to \mathbf{R}, \forall a \in \mathbf{R}, \forall b \in \mathbf{R}, \exists x \in \mathbf{R}, f(x) = ax + b$$

(Notons que les droites verticales du plan ne se définissent pas par une équation de la forme $y = ax + b$ mais de la forme $x = c$. Cela n'est pas très important ici, car de toute façon, le graphe de n'importe quelle fonction réelle intersecte naturellement toutes ces droites verticales.)

— Il s'agit d'un résultat d'existence. Pour le démontrer il faut idéalement trouver une fonction satisfaisant la propriété. Un travail d'analyse n'est ici pas simple et on ne peut guère faire mieux que de deviner graphiquement une fonction pouvant faire l'affaire en testant les quelques fonctions usuelles que l'on connaît. L'une des plus simples est la fonction cube.

Soit f la fonction définie sur $\mathbf{R}$ par $\forall x \in \mathbf{R}, f(x) = x^3$.
Montrons $\forall a \in \mathbf{R}, \forall b \in \mathbf{R}, \exists x \in \mathbf{R}, f(x) = ax + b$.
Soient donc $a \in \mathbf{R}$ et $b \in \mathbf{R}$.
Le polynôme $X^3 - aX - b$ étant de degré impair, on sait qu'il possède une racine réelle x (cela repose sur le TVI).
Ainsi $x^3 - ax - b = 0$ et donc $f(x) = ax + b$.
Ceci étant vrai pour tous réels a et b, la proposition est bien démontrée.

Remarque : le deuxième résultat d'existence de la proposition (celui du point d'intersection) a été justifié par un argument général.

Exercice **Équivalences**

1. $\forall f \in E,\ f$ paire $\Leftrightarrow f'$ impaire : cette proposition est vraie. Démontrons la par double implication.

Soit $f \in E$.
Première implication : Supposons f paire. Montrons que f' est impaire.
On a $\forall x \in \mathbf{R}, f(x) = f(-x)$.
Dérivons les deux termes de l'égalité : $\forall x \in \mathbf{R}, f'(x) = -f'(-x)$.
On retrouve la caractérisation d'une fonction impaire. Donc f' est impaire.

Réciproque :
Supposons que f' est impaire.
Montrons que f est paire.
On a $\forall x \in \mathbf{R}, f'(x) = -f'(-x)$.
Notons h la fonction définie par $h(x) = f(-x)$.
Alors h est une fonction dérivable et sa dérivée est définie par $h'(x) = -f'(-x)$.
Ainsi notre hypothèse s'écrit : $\forall x \in \mathbf{R}, f'(x) = h'(x)$.
Or on sait que si deux fonctions ont la même dérivée, alors elles sont égales à une constante près.
Donc $\exists c \in \mathbf{R},\ \forall x \in \mathbf{R}, f(x) = h(x) + c$.
Donc $\forall x \in \mathbf{R}, f(x) = f(-x) + c$.
En particulier, pour $x = 0$, on obtient $f(0) = f(0) + c$.
On en déduit que $c = 0$ et donc finalement : $\forall x \in \mathbf{R}, f(x) = f(-x)$.
La fonction f est paire.

par double implication, on a bien démontré l'équivalence.

Remarque importante : il faut absolument raisonner par double implication. On constate que la deuxième preuve est bien plus subtile que la première. Si on essaie de raisonner directement par équivalence, on risque de passer à côté du problème de la constante d'intégration et d'écrire une preuve qui ne marche en fait que dans un sens.

2. $\forall f \in E,\ f$ impaire $\Leftrightarrow$ f' paire : ce résultat est faux. Plus précisément, l'implication f impaire $\Longrightarrow$ f' paire est vraie mais sa réciproque f' paire $\Longrightarrow$ f impaire est fausse.
La preuve de la première implication est essentiellement la même que dans la question précédente. Si on voulait démontrer la réciproque comme dans la preuve précédente, on aboutirait à $\exists c \forall x \in \mathbf{R}, f(x) = -f(-x) + c$, mais il est ensuite impossible d'en déduire $c = 0$.

   Pour infirmer la réciproque (et donc l'équivalence toute entière), il suffit d'exhiber un contre-exemple : soit f la fonction définie par $f(x) = x^3 + 1$. Alors $f'(x) = 3x^2$ est une fonction paire, mais pourtant f n'est pas une fonction impaire.
3. $\exists! f \in E,\ f' = f$: ce résultat est faux. Il y a bien existence mais pas unicité. La fonction nulle et la fonction exponentielle vérifient toutes les deux l'équation différentielle $f' = f$. Il y a en fait une infinité de solutions. Les fonctions satisfaisant $f' = f$ sont les fonctions de la forme $f(x) = \lambda e^x$ où λ est une constante quelconque.
4. $\forall f \in E, \forall g \in E,\ f$ paire $\Longrightarrow$ $g \circ f$ paire : ce résultat est vrai.
   Soit $f \in E$ une fonction paire. Montrons que $g \circ f$ est paire.
   Soit $x \in \mathbf{R}$. Alors $g \circ f(-x) = g(f(-x)) = g(f(x))$ car f est paire.
   Ainsi $\forall x \in \mathbf{R}, g \circ f(-x) = g \circ f(x)$.
   La fonction $g \circ f$ est paire.
5. $\forall f \in E, \forall g \in E,\ f$ paire $\Longrightarrow$ $f \circ g$ paire : ce résultat est faux.
   Donnons un contre-exemple. Soit f la fonction définie par $f(x) = x^2$ et g la fonction définie par $g(x) = x + 1$. Alors $f \circ g(-1) = f(g(-1)) = f(0) = 0$ et $f \circ g(1) = f(g(1)) = f(2) = 4$. Donc $f \circ g(-1) \neq f \circ g(1)$: $f \circ g$ n'est pas paire.

Exercice **Quantificateurs**

Pour cet exercice, le mieux est de commencer par traduire les propositions proposées. Il faut bien comprendre que pour chaque proposition, l'entier n est fixé. On cherche à savoir pour quelles valeurs de n la proposition est vraie.

1. $\exists k \in \mathbf{N}, k \geq 2$ et $k^2 | n$: n est divisible par un carré (autre que 0 ou 1). Les solutions $\leqslant 30$ sont les multiples de 4, 9 et 25 : 0,4,8,9,12,16,18,20,24,25,27,28.
2. $\forall k \in \mathbf{N}, k | n \Longrightarrow k^2 | n$: si un nombre divise n, alors son carré aussi. Cette proposition est difficile à satisfaire. En effet, on a toujours $n | n$. Si la proposition est vraie, on doit alors avoir aussi $n^2 | n$ ce qui est impossible si $n^2 > n$. Les seules solutions sont 0 et 1 : 0 est divisible par tout le monde et 1 n'est divisible que par 1 (et par 1^2 donc).
3. $\forall k \in \mathbf{P}, k | n \Longrightarrow k^2 | n$: c'est la même proposition que la précédente mais avec une condition sur les diviseurs considérés. Si un nombre premier divise n, alors son carré aussi. On peut l'interpréter ainsi : tout facteur premier de n apparaît au moins deux fois dans sa décomposition en facteurs premiers. Les solutions sont : 0, 1, 4, 8, 9, 16, 25, 27. Les suivants seraient 32 et 36.
4. $\exists k \in \mathbf{P}, \exists j \in \mathbf{P}, n = kj$: le nombre n est le produit de deux nombres premiers. Attention à ne pas exclure les cas $k = j$. Les solutions sont : 4, 6, 9, 10, 14, 15, 21, 22, 25, 26.
5. $\forall k \in \mathbf{N}, \exists j \in \mathbf{N}, n | k$ ou $n | (k + j)$: plus difficile à interpréter simplement. L'important est de bien noter que j dépend de k. Ainsi $k + j$ peut être n'importe quel entier supérieur à k. La proposition peut alors s'interpréter ainsi : pour tout entier k, n divise k ou un entier supérieur à k. Cette proposition est alors vraie pour tous les entiers sauf 0 qui ne divise que lui-même. Par exemple, pour $n = 11$ et $k = 18$, on peut prendre $j = 4$ et on obtient bien $11 | 18$ ou $11 | 22$ (ceci n'est en rien une preuve !).

6. $\exists j \in \mathbf{N}, \forall k \in \mathbf{N}, n|k$ ou $n|(k+j)$: on a juste inversé les quantificateurs. Le nombre j ne peut plus dépendre de l'entier k considéré. La proposition devient plus difficile à satisfaire. Il y a cependant des solutions. Comme $n = 1$ divise tous les entiers, il est solution. On peut prendre $j = 0$ et on a bien : $\forall k \in \mathbf{N},\ 1|k$ ou $1|k$.
$n = 2$ est également solution. Il faut pour cela prendre $j = 1$. On a en effet bien $\forall k \in \mathbf{N},\ 2|k$ ou $2|(k+1)$: pour tout entier, lui ou son successeur est pair.
Il est possible de montrer qu'à partir de $n = 3$, la proposition devient fausse. Cela repose sur le fait qu'il y a plus de 3 restes différents possible pour la division euclidienne d'un entier par n.

Exercice **Par l'absurde**

Montrons par l'absurde que le nombre réel $\log_{10}(2)$ est irrationnel.
Supposons donc qu'il soit rationnel. Alors il existe $p \in \mathbf{Z}$ et $q \in \mathbf{N}^*$ tels que $\log_{10}(2) = \frac{p}{q}$. *(On pourrait préciser que la fraction est irréductible mais c'est inutile dans cette preuve.)*
Donc $10^{\log_{10}(2)} = 10^{\frac{p}{q}}$,
donc $2 = 10^{\frac{p}{q}}$,
donc $2^q = 10^p$,
et finalement $2^q = 2^p 5^p$.

(Nous ne savons pas vers où nous allons mais nous essayons de nous ramener à des problèmes connus. Ici, nous avons commencé par faire disparaître le log *puis par faire disparaître la fraction. Nous aboutissons ainsi à une égalité ne faisant intervenir que des entiers (à moins que p ne soit négatif mais ce cas est facile à écarter). Notre problème est désormais un problème d'arithmétique, un domaine que nous maîtrisons assez bien.)*

Comme $q \geq 1$, on a nécessairement $p \geq 1$. Ainsi les termes de l'égalité sont des entiers. Et comme $p \geq 1$, $5|2^p 5^p$. Donc $5|2^q$ ce qui est impossible. Nous avons donc abouti à une contradiction. Nous pouvons donc conclure que $\log_{10}(2)$ est un nombre irrationnel.
(On aurait aussi pu conclure ainsi : Dans l'égalité $2^q = 2^p 5^p$, les deux nombres sont décomposés en facteurs premiers. D'après l'unicité de ces décompositions, on doit avoir $p = q$ et $p = 0$. Or q est non nul et on retrouve une contradiction.)

Exercice **Récurrences**

2. Montrons par récurrence sur n que $\forall n \in \mathbf{N},\ 3$ divise $4^n + 5$.
Initialisation : pour $n = 0$, on a $4^0 + 5 = 6$ qui est bien divisible par 3. La propriété est donc vraie au rang 0. Par acquis de conscience, regardons aussi $n = 1$: $4^1 + 5 = 9$ est bien divisible par 3.
Hérédité : soit $n \in \mathbf{N}$ et supposons que 3 divise $4^n + 5$. Montrons que 3 divise $4^{n+1} + 5$. Par hypothèse, on peut écrire $4^n + 5 = 3k$ avec $k \in \mathbf{N}$. Donc $4^n = 3k - 5$ et :

$$4^{n+1} + 5 = 4 \cdot 4^n + 5 = 4(3k - 5) + 5 = 4 \cdot 3k - 15 = 3(4k - 5).$$

On en déduit bien que $4^{n+1} + 5$ est divisible par 3.
Cela achève notre récurrence.

3. Montrons par récurrence sur n que $\forall n,\ 2^n \leqslant n!$.
Initialisation : pour $n = 0$, $2^0 = 1$ et $0! = 1$, donc on a bien $2^0 \leqslant 0!$ et la propriété est vraie au rang 0.

Regardons aussi le cas $n = 1$: $2^1 = 2$ et $1! = 1$. Or $2 > 1$: la propriété n'est pas valable au rang 1 ! Autrement dit, la propriété annoncée est fausse.
Essayons tout de même d'en préciser la validité.

Regardons l'hérédité : soit $n \in \mathbf{N}$ et supposons que $2^n \leqslant n!$. Alors en multipliant par 2, on obtient $2^{n+1} \leqslant 2 \cdot n!$. Or $(n+1)! = (n+1) \cdot n!$. Donc si $n + 1 \geqslant 2$, on peut affirmer que

$$2^{n+1} \leqslant 2 \cdot n! \leqslant (n+1) \cdot n! = (n+1)!.$$

Ainsi, l'hérédité est démontrée pour $n \geqslant 1$. Mais elle n'est pas démontrée pour $n = 0$. C'est cohérent avec le résultat précédent : même si la propriété est vraie au rang 0, on ne peut pas garantir qu'elle l'est encore au rang 1.

Pour le moment, nous ne pouvons pas déduire grand chose. Il nous manque une initialisation permettant de faire démarrer notre propriété d'hérédité. reprenons les premières valeurs de n. Pour $n = 2$: $2^2 = 4$ et $2! = 2$, ça ne marche pas. Pour $n = 3$: $2^3 = 8$ et $3! = 6$, ça ne marche pas. Pour $n = 4$: $2^4 = 16$ et $4! = 24$, ça marche !

Conclusion : la propriété est vraie pour $n = 4$ et nous avons démontré que pour $n \geqslant 4$, si $2^n \leqslant n!$, alors $2^{n+1} \leqslant (n+1)!$. On en déduit par récurrence que la propriété est satisfaite pour tout $n \geqslant 4$. Et d'après ce qui précède, elle l'est également pour $n = 0$ mais pas pour $n = 1$, 2 et 3.

Exercice **Coefficients binomiaux**

1. Soit $n \in \mathbf{N}^*$ et $k \in 0, \ldots, n-1$. Alors $\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!} = n! \frac{k+1)+(n-k)}{(k+1)!(n-k)!} = n! \frac{n+1}{(k+1)!(n+1-(k+1))!} = \binom{n+1}{k+1}$.
2. En utilisant la propriété précédente, on peut construire rapidement le triangle de Pascal qui donne la liste des coefficients binomiaux. La construction du triangle a pour but de bien comprendre comment se rédigera la preuve suivante. On voit en effet clairement pourquoi les coefficients binomiaux sont bien entiers : on construit la triangle ligne par ligne. À partir du moment où une ligne est composée d'entiers, on voit bien que la suivante le sera aussi. Mais attention, cela n'est pas valable pour les 1 situés en bouts de ligne. Ceux-ci sont des entiers par définition et non pour une raison récursive.
   La preuve suivante reposera donc sur une récurrence par lignes du triangle et sur le fait que les extrémités des lignes valent toujours 1.
3. Pour $n \in \mathbf{N}$, notons P_n la propriété $\forall k \in \{0, \ldots, n\}$, $\binom{n}{k}$ est un entier (autrement dit, la ligne n du triangle est composée d'entiers). Montrons ce résultat par récurrence sur n.

   Si $n = 0$, on a $\binom{0}{0} = \frac{0!}{0!0!} = 1$. C'est un entier et la propriété P_0 est donc vraie.

   Soit $n \in \mathbf{N}$. Supposons que la propriété P_n est vraie. Montrons alors que la propriété P_{n+1} est vraie.
   Soit donc $k \in \{0, \ldots, n+1\}$.
   Si $k = 0$, $\binom{n+1}{0} = \frac{(n+1)!}{0!(n+1)!} = 1$. C'est un entier. Si $k = n+1$, $\binom{n+1}{n+1} = \frac{(n+1)!}{(n+1)!0!} = 1$. C'est encore un entier.
   Si $k \in \{1, \ldots, n\}$, on peut utiliser le résultat de la question 1 : $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. Or par hypothèse de récurrence, $\binom{n}{k}$ et $\binom{n}{k-1}$ sont des entiers. Donc $\binom{n+1}{k}$ est un entier.

On a ainsi montré $\forall k \in \{0, \dots, n+1\}$, $\binom{n+1}{k}$ est un entier. La propriété P_{n+1} est donc vraie.

Ainsi, par récurrence, nous avons démontré que tous les coefficients binomiaux sont des entiers.

4. Soit $p \in \mathbf{P}$ et $k \in \{1, \dots, p-1\}$. Montrons que $p|\binom{p}{k}$. Notons déjà que la question posée a du sens car on a bien démontré que $\binom{p}{k}$ était un entier.
On a $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Donc $p! = \binom{p}{k}k!(p-k)!$ (on se ramène à une égalité d'entiers). Comme $p|p!$, $p|\binom{p}{k}k!(p-k)!$. Or p est un nombre premier ; d'après le lemme d'Euclide, on déduit que p divise l'un des 3 facteurs : $p|\binom{p}{k}$ ou $p|k!$ ou $p|(p-k)!$.
Or $k < p$, donc p n'apparaît pas dans le produit $k!$. Toujours d'après le lemme d'Euclide, on en déduit que p ne divise pas $k!$. De même, comme $k > 0$, $p - k < p$ et p ne divise pas $(p-k)!$.
On peut finalement conclure que p divise $\binom{p}{k}$.

Remarque : toutes les hypothèses ont bien été utilisées dans cette preuve. Le résultat est faux si p n'est pas premier, $k = 0$ ou $k = p$.

5. Soit $p \in \mathbf{P}$. Montrons le résultat par récurrence sur a que $p|a^p - a$.
Si $a = 0$, $a^p - a = 0$ qui est clairement divisible par p. La propriété est donc vraie pour $a = 0$.
Soit $a \in \mathbf{N}$. Supposons la propriété vraie au rang a : $p|a^p - a$. Montrons qu'elle est vraie au rang $a+1$. D'après la formule du binôme de Newton, $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k}a^k$ Donc $(a+1)^p - (a+1) = 1 + a^p + \sum_{k=1}^{p-1} \binom{p}{k}a^k - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k}a^k$. Par hypothèse de récurrence, $p|(a^p - a)$ et d'après la question précédente, p divise chacun des coefficients binomiaux $\binom{p}{k}$ de la somme. On en déduit que p divise $(a+1)^p - (a+1)$ et la propriété est vraie au rang $a+1$.
Le petit théorème de Fermat est ainsi démontré par récurrence.

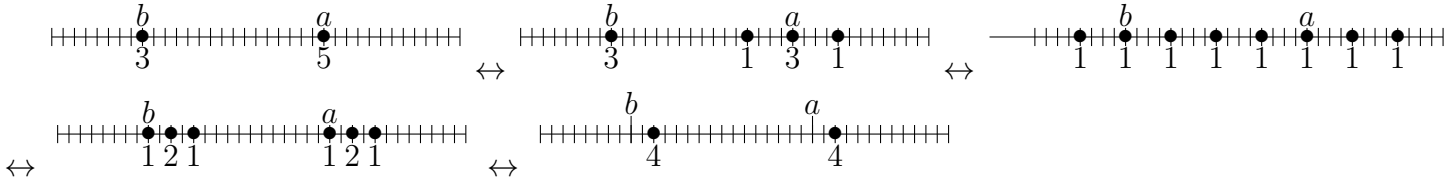
Exercice **Principe des tiroirs**

1. Soient m et n des nombres entiers non nuls. On souhaite démontrer que si $m > n$, alors toute répartition de m chaussettes parmi n tiroirs implique qu'un tiroir contienne au moins deux chaussettes. Montrons ce résultat par récurrence sur n :
Initialisation : soit $n = 1$ et $m > 1$. Alors, comme il n'y a qu'un seul tiroir et plusieurs chaussettes, il est évident que ce tiroir contiendra plusieurs chaussettes.
Hérédité : Supposons le résultat vrai pour n tiroirs et $m > n$ chaussettes. Montrons qu'il reste valable pour $n+1$ tiroirs. Soit maintenant $m > n+1$. Considérons l'un des tiroirs. Alors soit il contient plusieurs chaussettes et il n'y a rien à démontrer, soit il n'en contient qu'une, soit il n'en contient pas. Dans les deux derniers cas, on peut considérer les n tiroirs restants. Ils contiennent alors $m-1$ ou m chaussettes. Or, comme $m > n+1$, on a $m-1 > n$ et aussi $m > n$. Ainsi, par hypothèse de récurrence, l'un des n tiroirs contient au moins deux chaussettes. Nous en déduisons finalement que dans tous les cas, l'un des $n+1$ tiroirs contient plusieurs chaussettes.
Le résultat est donc démontré par récurrence.

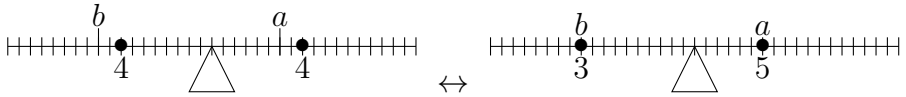
2. Soient $n+1$ nombres réels dans l'intervalle $[0, 1]$. Considérons les n intervalles de la forme $[\frac{k}{n}, \frac{k+1}{n}]$ pour $k = 0, 1, \dots n-1$. Nos $n+1$ nombres sont répartis dans ces n intervalles. D'après le principe des tiroirs, l'un de ces intervalles contient au moins deux nombres. Comme leur longueur est égale à $\frac{1}{n}$, on déduit qu'il existe bien au moins deux de nos nombres situés à une distance l'un de l'autre inférieure à $\frac{1}{n}$.

Exercice **Axiomatique**

Déterminons le point d'équilibre de deux poids de masses $a = 5$ et $b = 3$ en utilisant les deux axiomes autorisés. L'idée est de se ramener, en utilisant l'axiome 2, à une situation où les masses sont égales puis d'appliquer l'axiome 1. Sur la figure, l'intervalle $[a, b]$ a été divisée en 8 parties égales. Le symbole $\leftrightarrow$ signifiera que les configurations ont le même point d'équilibre.



Avec l'axiome 1, on connaît le point d'équilibre de cette dernière configuration et c'est donc le même que celui de la configuration initiale :



On peut alors conclure : si on note 1 la distance entre a et b, le point d'équilibre des poids $a = 5$ et $b = 3$ est situé à une distance $3/8$ de a et à une distance $5/8$ de b.

Exercice **Démonstrations erronées**

— Le résultat est faux. Contre-exemple : la fonction constante égale à 1. En effet, pour tout entier n, on peut prendre $x = n$ et on a alors $f(x) = 1 \leq x/n = 1$.
L'erreur dans la preuve est d'avoir considéré que x était indépendant de n. Réécrivons-la correctement : soit $n \in \mathbf{N}^*$. D'après l'hypothèse faite, il existe $x_n \in \mathbf{R}$ tel que $|f(x_n)| \leq \frac{x_n}{n}$. N'ayant a priori aucune information sur les nombres x_n, il est impossible de déterminer la limite de la suite (x_n/n).

— Le résultat est juste mais la preuve n'est pas valable pour $p = 2$. Les nombres x proposés ne sont en effet pas des entiers si b est impair. Et de plus on ne peut pas déduire $2|P(x)$ de $2|4P(x)$.
Pour rendre la preuve valable, il suffit de traiter le cas $p = 2$ à part.

— La preuve de l'hérédité n'est pas valable pour $n = 2$. Dans ce cas, on considère 3 points A_1, A_2 et A_3. D'après l'hypothèse de récurrence, on sait que A_1, A_2 sont alignés et A_2, A_3 sont alignés (ce qui est juste). Mais il est impossible d'en déduire que A_1, A_2, A_3 sont alignés. Les deux droites n'ayant qu'un seul point d'intersection a priori n'ont aucune raison d'être égales.
À noter qu'à partir de $n = 3$, la preuve de l'hérédité est valable. Mais comme ça coince pour $n = 2$, tout l'édifice de la preuve s'écroule.

— Toute la démonstration semble juste. En fait, la principale erreur vient de la figure. Le point O ne peut pas se trouver à l'intérieur du triangle. Et le point P ne se trouve alors pas entre A et B. Dans la preuve, cela se traduit vers la fin par le fait qu'on a écrit $AB = AP + PB$ alors qu'on devrait avoir $AB = AP - PB$.

2 Arithmétique

Exercice **Racines dans $\mathbf{Z}/n\mathbf{Z}$** Pour résoudre les équations demandées, on teste toutes les valeurs possibles dans $\mathbf{Z}/13\mathbf{Z}$ et dans $\mathbf{Z}/12\mathbf{Z}$ (en dressant des tableaux de congruences).

Les solutions dans $\mathbf{Z}/13\mathbf{Z}$ de l'équation $x^2 + x + \bar{7} = \bar{0}$ sont $x = \bar{2}$ et $x = \bar{10}$.

Les solutions dans $\mathbf{Z}/12\mathbf{Z}$ de l'équation $x^2 + \bar{4}x + \bar{3} = 0$ sont $x = \bar{3}$, $x = \bar{5}$, $x = \bar{9}$ et $x = \bar{11}$.

Remarques : quand on considère un polynôme de degré 2, on s'attend d'habitude à trouver au plus deux racines. Nous verrons plus tard que cette assertion est vraie dans $\mathbf{Z}/n\mathbf{Z}$ si n est premier (ce qui est le cas de 13) mais qu'elle ne l'est pas forcément si n n'est pas premier (ce qui est le cas de 12).

On peut déjà remarquer que la factorisation dans $\mathbf{Z}/n\mathbf{Z}$ fonctionne comme dans $\mathbf{R}$: dans $\mathbf{Z}/13\mathbf{Z}$

$$x^2 + x + \bar{7} = x^2 + \bar{14}x + \bar{7} = (x + \bar{7})^2 - \bar{42} = (x + \bar{7})^2 - \bar{3}.$$

Or, dans $\mathbf{Z}/13\mathbf{Z}$, $\bar{3}$ est le carré de $\bar{4}$, donc

$$x^2 + x + \bar{7} = (x + \bar{7})^2 - \bar{4}^2 = (x + \bar{3})(x + \bar{11}) = (x - \bar{10})(x - \bar{2}).$$

On retrouve bien les racines $\bar{10}$ et $\bar{2}$. Ce raisonnement ne permet néanmoins pas d'assurer qu'on a trouvé toutes les racines.

Exercice **Équations diophantiennes**

Supposons par l'absurde que $(x, y) \in \mathbf{Z}^2$ est solution de l'équation $x^2 - 2y^6 = 17$.
Alors en particulier, $x^2 - 2y^6 = 17 \mod 7$, *i.e.* $\bar{x}^2 - \bar{2}\bar{y}^6 = \bar{17} = \bar{3}$ dans $\mathbf{Z}/7\mathbf{Z}$.
Or les valeurs possibles de $\bar{x}^2$ dans $\mathbf{Z}/7\mathbf{Z}$ sont $\bar{0}, \bar{1}, \bar{4}$ et $\bar{2}$ et les valeurs possibles de $\bar{y}^6$ sont $\bar{0}$ et $\bar{1}$.
Ainsi les valeurs possibles de $\bar{x}^2 - \bar{2}\bar{y}$ sont $\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}$ et $\bar{6}$.
Comme $\bar{3}$ n'apparaît pas dans cette liste, on déduit que la relation $\bar{x}^2 - \bar{2}\bar{y}^6 = \bar{3}$ est impossible.
On a ainsi obtenu une contradiction et l'équation étudiée n'a donc pas de solution dans $\mathbf{Z}^2$.

Supposons par l'absurde que $(x, y) \in \mathbf{Z}^2$ est solution de l'équation $x^2 + y^2 = 9z + 6$.
Alors en particulier, $x^2 + y^2 = 0 \mod 3$, *i.e.* $\bar{x}^2 + \bar{y}^2 = \bar{0}$ dans $\mathbf{Z}/3\mathbf{Z}$.
On peut vérifier que la seule possibilité est que $\bar{x} = \bar{0}$ et $\bar{y} = \bar{0}$.
Cela signifie que x et y sont des multiples de 3. Donc x^2 et y^2 sont des multiples de 9.
Or d'après notre relation initiale $6 = x^2 + y^2 - 9z$. On en déduit donc que 6 est un multiple de 9 ce qui est absurde.
On peut donc conclure que notre équation n'a pas de solution dans $\mathbf{Z}^2$.

Exercice **Équations diophantiennes**

On cherche à résoudre dans $\mathbf{Z}$ l'équation $2x + 3y = 7$.
Soit $(x, y) \in \mathbf{Z}^2$ une solution.
Remarquons déjà que si y est pair, $2x + 3y$ est pair et ne peut être égal à 7.
Ainsi, y est nécessairement un entier impair.
Alors $7 - 3y$ est un entier pair et on doit donc avoir $x = \frac{7-3y}{2}$.
Nous avons donc montré que si (x, y) est solution alors il peut s'écrire sous la forme $(\frac{7-3y}{2}, y)$ avec y impair.

Réciproquement, on peut vérifier que tous ces couples sont bien solutions de l'équation : $2\frac{7-3y}{2} + 3y = 7$.

L'ensemble des solutions est donc $S = \{(\frac{7-3y}{2}, y); y \text{ impair}\}$. (On peut l'écrire aussi $S = \{(2-3k, 2k+1); k \in \mathbf{Z}\}$ ou $S = \{(x,y) \in \mathbf{Z} \mid y \text{ impair et } x = \frac{7-3y}{2}\}$.)

Proposons une seconde preuve, basée sur un argument plus général.
Commençons par résoudre l'équation diophantienne $2x+3y=0$ (il s'agit de l'équation homogène associée à notre problème).
Un couple d'entiers (x,y) est solution ssi $2x = -3y$. Comme 2 et 3 sont premiers entre eux, on en déduit que 2 divise y et 3 divise x. On peut donc écrire y sous la forme $y = 2k$ avec $k \in \mathbf{Z}$ et il en découle que $x = -3k$.
Réciproquement, tout couple de la forme $(-3k, 2k)$ est trivialement solution de l'équation homogène.
Ainsi l'ensemble des solutions de cette première équation est $S_0 = \{(-3k, 2k); k \in \mathbf{Z}\}$.

Passons maintenant à notre équation $2x + 3y = 7$. Nous remarquons déjà que le couple $(x,y) = (2,1)$ en est une solution. Considérons maintenant une autre solution (x,y). Alors $2x + 3y = 7$ et nous venons de voir que $2 \cdot 2 + 3 \cdot 1 = 7$. En soustrayant ces égalités, on obtient $2(x-2) + 3(y-1) = 0$.
Ainsi le couple $(x-2, y-1)$ est solution de notre équation homogène. On en déduit qu'il peut s'écrire sous la forme $(x-2, y-1) = (-3k, 2k)$ avec $k \in \mathbf{Z}$. Autrement dit, $(x,y) = (2-2k, 1+2k)$.
Finalement on retrouve notre ensemble de solutions : $S == \{(2-3k, 1+2k); k \in \mathbf{Z}\}$.

Passons à l'autre équation : $15x - 6y = 14$.
Soit (x,y) dans $\mathbf{Z}^2$. Alors $15x - 6y$ est un multiple de 3. En particulier $15x - 6y$ ne peut pas être égal à 14. L'équation n'a donc pas de solutions dans $\mathbf{Z}^2$. L'ensemble des solutions est vide.

Exercice **Nombres premiers entre eux**

Soient a et b des entiers premiers entre eux. Montrons que $a+b$ et ab sont premiers entre eux.
Soit p un nombre premier divisant ab.
Alors, d'après le lemme d'Euclide, p divise a ou p divise b.
S'il divise a il ne peut diviser b puisque a et b sont premiers entre eux.
Alors il ne divise pas $a+b$.
De même s'il divise b, il ne divise pas a et ne divise donc pas $a+b$.
Nous avons donc montré qu'aucun diviseur premier de ab n'est un diviseur de $a+b$.
On en déduit qu'aucun diviseur de ab, sauf 1, ne divise $a+b$.
Ces deux nombres n'ont donc aucun diviseur en commun et sont premiers entre eux.

La réciproque est vraie.
Soient a et b des entiers tels que $a+b$ et ab soient premiers entre eux. Montrons que a et b sont premiers entre eux.
Soit d un diviseur de a et b.
Alors il divise $a+b$ et ab.
Ces deux nombres étant premiers entre eux, cela implique $d = 1$.
Ainsi le seul diviseur commun à a et b est 1.
Donc a et b sont premiers entre eux.

Exercice **Diviseurs consécutifs**

Soit $n \in \mathbf{N}^*$.
Considérons les n entiers consécutifs $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$. On rappelle

que $k!$ désigne le produit $1 \times 2 \times 3 \times \cdots \times k$.
Montrons qu'aucun de nos n entiers n'est premier.
Comme $n+1 \geq 2$, $(n+1)!$ est pair.
Donc $(n+1)!+2$ est un nombre pair différent de 2. En particulier ce n'est pas un nombre premier.
Plus généralement, soit $2 \leq k \leq n+1$.
Le nombre $(n+1)!$ est un multiple de k.
Donc k divise $(n+1)!+k$. Comme ce nombre est différent de k, on en d'eduit qu'il possède un diviseur autre que 1 et lui-même et qu'il n'est pas premier.
Ainsi chacun de nos n nombres entiers admet un diviseur non trivial.
On a donc bien trouvé n nombres entiers consécutifs tels qu'aucun d'entre eux ne soit premier.

Exercice **Nombres premiers ?**

Notons n le nombre $101\cdots101$ formé de $k+1$ uns et k zéros disposés alternativement.
Notons $m = 11n = 10n+n$. Alors m est égal au nombre $11\cdots11$ formé de $2k+2$ uns.
Notons $r = 1\cdots1$ formé de $k+1$ uns. Alors $m = 10^{k+1}r + r$.
Ainsi $11n = r(10^{k+1}+1)$.
Comme 11 est premier, on sait qu'il divise r ou $10^{k+1}+1$.
Si $k > 1$, ces deux nombres sont des nombres distincts de 11.
On peut déduire de tout cela que le nombre $r(10^{k+1}+1)$ possède au moins trois diviseurs autres que 1 (dont l'un est 11) dans sa décomposition en nombres premiers.
Mais alors n possède au moins deux facteurs et n'est donc pas premier.
Si $k = 1$ ces arguments ne fonctionnent pas. On peut en fait montrer que le nombre 101 est un nombre premier.

Conclusion : le nombre $101\cdots101$ est premier si et seulement si $k = 1$.

Exercice **Système de congruences**

Résolvons le système $\begin{cases} \bar{3}x - y &= \bar{2} \\ x + \bar{2}y &= \bar{1} \end{cases}$ dans $\mathbf{Z}/10\mathbf{Z}$.
Effectuons l'opération $2L_1 + L_2$: on obtient $\bar{7}x = \bar{5}$.
En considérant toutes les valeurs possibles de x dans $\mathbf{Z}/10\mathbf{Z}$, on trouve que la seule possibilité est $x = \bar{5}$ (en effet, $7 \times 5 = 35 = 5 \mod 10$).
Dans la première équation on obtient alors $\bar{3} \times \bar{5} - y = \bar{2}$, donc $y = \bar{15} - \bar{2} = \bar{3}$.
L'unique solution du système est donc $(x, y) = (\bar{5}, \bar{3})$.
Passons au système $\begin{cases} \bar{2}x + \bar{3}y &= \bar{1} \\ x - y &= \bar{0} \end{cases}$. Effectuons l'opération $L_1 - 2L_2$: on obtient $\bar{5}y = \bar{1}$.
Or dans $\mathbf{Z}/10\mathbf{Z}$, quelque soit la valeur de y, le produit $\bar{5}y$ ne peut valoir que $\bar{0}$ ou $\bar{5}$.
L'équation ci-dessus n'a donc pas de solution, et par conséquent, le système n'en a pas non plus.

3 Ensembles et Applications

Exercice **Ensembles particuliers**

L'ensemble E_1 est constitué de 6 points disposés en rectangle.

L'ensemble E_2 est la parabole d'équation $y = x^2$.

L'ensemble E_3 est la portion de la parabole d'axe Ox, d'équation $x = y^2$, délimitée en ordonnée par $y = 1$ et $y = -1$.

L'ensemble E_4 est la portion de plan délimitée par les droites d'équations $x = 0$ et $y = 1 - x$, contenant le point $(1, -4)$.

L'ensemble E_5 est une demi-couronne délimitée par les cercles de centre $(0, 0)$ de rayons 1 et $\sqrt{5}$ et l'axe Oy. On peut le paramétrer sous la forme

$$E_5 = \{(r\cos(\theta), r\sin(\theta)) \ ; \ r \in]1, \sqrt{5}[, \theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]\}.$$

L'ensemble E_6 est le cercle de centre $(2, 0)$ de rayon 1. Il est défini par l'équation cartésienne $(x-2)^2 + y^2 = 1$.

Exercice **Étude d'un ensemble paramétré**

Le but de cet exercice est de représenter dans le plan l'ensemble

$$S = \{(r\cos(r\theta), r\sin(r\theta)) \ ; \ r \in [0, 1], \theta \in [0, \pi]\}.$$

Montrons que S est inclus dans le disque unité $D = \{(x, y) \ ; \ x^2 + y^2 \leqslant 1\}$.
Soit $(x, y) \in S$. Alors il existe $r \in [0, 1]$ et $\theta \in [0, \pi]$ tels que $(x, y) = (r\cos(r\theta), r\sin(r\theta))$. Donc

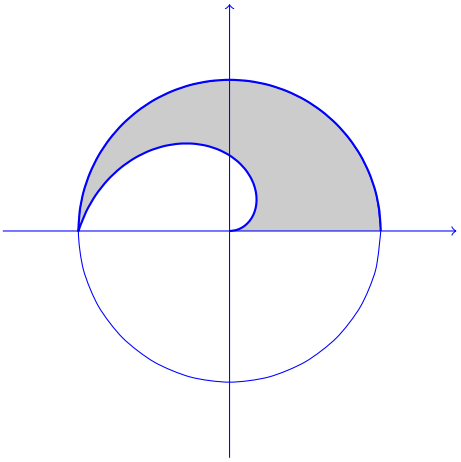
$$x^2 + y^2 = r^2\cos^2(r\theta) + r^2\sin^2(r\theta) = r^2 \leqslant 1.$$

Ainsi (x, y) satisfait l'inégalité définissant D, donc $(x, y) \in D$.
Ainsi $S \subset D$.

Montrons de même que S est inclus dans le demi-plan défini par $y \geqslant 0$. Reprenons notre couple (x, y) de S. Alors $y = r\sin(r\theta)$. Comme $r \in [0, 1]$ et $\theta \in [0, \pi]$, on déduit $0 \leqslant r\theta \leqslant \pi$. En particulier, $\sin(r\theta) \geqslant 0$. Et donc $r\sin(r\theta) \geqslant 0$. Ainsi $y \geqslant 0$ et nous pouvons conclure.

Montrons que le couple $(-\frac{1}{4}, \frac{1}{4})$ n'est pas élément de S. Supposons par l'absurde qu'il en est un élément. Alors il existe $r \in [0, 1]$ et $\theta \in [0, \pi]$ tels que $(-\frac{1}{4}, \frac{1}{4}) = (r\cos(r\theta), r\sin(r\theta))$. Alors $(-\frac{1}{4})^2 + (\frac{1}{4})^2 = r^2\cos^2(r\theta) + r^2\sin^2(r\theta)$, donc $\frac{1}{8} = r^2$ et $r = \frac{1}{2\sqrt{2}}$. De plus $r\cos(r\theta) = -\frac{1}{4}$, donc $\cos(\frac{\theta}{2\sqrt{2}}) = -\frac{\sqrt{2}}{2}$. On en déduit $\frac{\theta}{2\sqrt{2}} = \frac{3\pi}{4}$ (en tenant compte du fait que $\theta \in [0, \pi]$). Donc $\theta = \frac{3\pi}{\sqrt{2}}$. En particulier $\theta > \pi$ ce qui est contradictoire. Donc le couple $(-\frac{1}{4}, \frac{1}{4})$ n'est pas élément de S.

Fixons $r \in [0, 1]$. L'ensemble $S_r = \{(r\cos(r\theta), r\sin(r\theta)) \ ; \ \theta \in [0, \pi]\}$ ne dépend plus que d'un seul paramètre, il s'agit d'une courbe. Et on reconnaît une portion de cercle : le cercle de centre $(0, 0)$, de rayon r. La portion de cercle est décrite par un angle variant de 0 à $r\pi$. Cette portion est donc d'autant plus grande que r est grand. L'ensemble S est l'union de ces portions de cercles pour r variant de 0 à 1. On peut représenter S par l'ensemble ci-dessous.

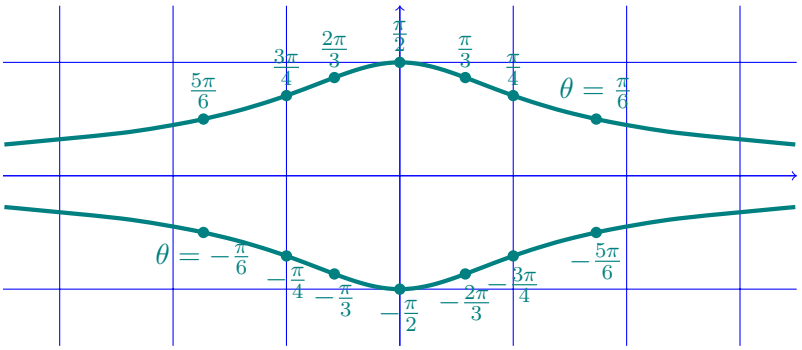


Exercice **Égalité d'ensembles**

Montrons $\{(x,y) \in \mathbf{R}^2 \mid x^2y^2 + y^2 = 1\} = \left\{(\frac{\cos(\theta)}{\sin(\theta)}, \sin(\theta)) \ ; \ \theta \in]-\pi, 0[\cup]0, \pi[\right\}$.
Notons A le premier ensemble et B le second et raisonnons par double inclusion.
Commençons par montrer $B \subset A$ (c'est le sens facile).
Soit $(x,y) \in B$. Par définition de B, on peut l'écrire $(x,y) = (\frac{\cos(\theta)}{\sin(\theta)}, \sin(\theta))$ pour un certain angle $\theta \in]-\pi, 0[\cup]0, \pi[$. Alors $x^2y^2 + y^2 = \frac{\cos(\theta)}{\sin(\theta)} \times \sin^2(\theta) + \sin^2(\theta) = \cos^2(\theta) + \sin^2(\theta) = 1$. Ainsi $x^2y^2 + y^2 = 1$: (x,y) satisfait la propriété définissant l'ensemble A. Donc $(x,y) \in A$. Nous avons montré $B \subset A$.

Montrons $A \subset B$.
Soit $(x,y) \in A$. Alors $x^2y^2 + y^2 = 1$. Donc $(xy)^2 + y^2 = 1$. Ainsi (xy, y) satisfait l'équation du cercle unité. D'après un exemple du cours, on en déduit qu'il existe $\theta \in]-\pi, \pi]$ tel que $(xy, y) = (\cos(\theta), \sin(\theta))$. D'autre part, $y \neq 0$ sinon $x^2y^2 + y^2 = 0 \neq 1$. Donc $\sin(\theta) \neq 0$, donc $\theta \in]-\pi, 0[\cup]0, \pi[$. Finalement, $y = \sin(\theta)$ et $xy = \cos(\theta)$ donc $x = \frac{\cos(\theta)}{\sin(\theta)}$. Le couple (x,y) est bien un élément de B et $A \subset B$.

Par double inclusion, nous avons montré $A = B$. Pour représenter cet ensemble, le plus simple est d'utiliser la version paramétrée B. On prend plusieurs valeurs de θ et on représente pour chacune le point correspondant.



Montrons $\{(x,y) \in \mathbf{R}^2 \mid (x-1)^2 + y^2 = 1 \text{ et } x \neq 0\} = \{(\frac{2}{1+t^2}, \frac{2t}{1+t^2}) \mid t \in \mathbf{R}\}$.
Notons A l'ensemble de gauche et B celui de droite. On reconnaît pour A l'équation du cercle de centre $(1,0)$ et de rayon 1, privé du point $(0,0)$.
Montrons que $B \subset A$: soit $t \in \mathbf{R}$ et posons $(x,y) = (\frac{2}{1+t^2}, \frac{2t}{1+t^2})$ l'élément de B correspondant.

Alors
$$(x-1)^2+y^2=(\frac{2}{1+t^2}-1)^2+(\frac{2t}{1+t^2})^2=(\frac{1-t^2}{1+t^2})^2+(\frac{2t}{1+t^2})^2$$
$$=\frac{1-2t^2+t^4+4t^2}{(1+t^2)^2}=\frac{(1+t^2)^2}{(1+t^2)^2}=1.$$
Ainsi le couple (x,y) satisfait l'équation définissant A. D'autre part, on a bien $x=\frac{2}{1+t^2}\neq 0$. Donc (x,y) est un élément de A. On en déduit $B\subset A$.

Montrons que $A\subset B$: soit $(x,y)\in A$. Alors $x\neq 0$ et $(x-1)^2+y^2=1$. Posons alors $t=\frac{y}{x}$ (cela est suggéré par l'énoncé, mais on peut en effet remarquer que les couples (x,y) de l'ensemble B satisfont la condition $y=tx$). Alors $y=tx$, et en remplaçant dans l'équation, on obtient $(x-1)^2+t^2x^2=1$, *i.e.* $(1+t^2)x^2-2x=0$. On en déduit $x=0$ ou $x=\frac{2}{1+t^2}$. Or $x\neq 0$, donc $x=\frac{2}{1+t^2}$ et $y=tx=\frac{2t}{1+t^2}$. Ainsi $(x,y)=(\frac{2}{1+t^2},\frac{2t}{1+t^2})$, donc (x,y) est un élément de B. On en déduit $A\subset B$.

Montrons $\{x\in\mathbf{R}\mid\exists a,b,c\in\mathbf{Z},a\neq 0,ax^2+bx+c=0\}=\{p\pm\sqrt{q}\mid p\in\mathbf{Q},q\in\mathbf{Q}_+\}$.
Notons A l'ensemble de gauche et B celui de droite.
Commençons par montrer $A\subset B$: soit $x\in A$.
Alors il existe des entiers relatifs a, b et c tels que x est racine du polynôme aX^2+bX+c.
Ce polynôme ayant une racine réelle, son discriminant est un entier positif et ses racines sont $r_1=\frac{-b+\sqrt{b^2-4ac}}{2a}$ et $r_2=\frac{-b-\sqrt{b^2-4ac}}{2a}$.
Comme x est l'une de ces deux racines, on a $x=\frac{-b}{2a}+\sqrt{\frac{b^2-4ac}{4a^2}}$ ou $x=\frac{-b}{2a}-\sqrt{\frac{b^2-4ac}{4a^2}}$.
Dans les deux cas, il s'écrit sous la forme $p\pm\sqrt{q}$ où p et q sont des nombres rationnels.
Donc $x\in B$. Donc $A\subset B$.

Montrons désormais $B\subset A$.
Soit $x\in B$. Alors il existe des nombres rationnels p et q non nuls (même si $x=0$) tels que $x=p+\sqrt{q}$ ou $x=p-\sqrt{q}$.
Cherchons un polynôme à coefficients entiers annulant ces deux nombres.
Remarquons pour cela que $x-p=\pm\sqrt{q}$, donc $(x-p)^2=q$.
Ainsi, le polynôme $(X-p)^2-q=X^2-2pX+p^2-q$ a pour racine x.
Cependant, ce polynôme est à coefficients rationnels mais pas nécessairement à coefficients entiers !
Notons d un dénominateur commun de p et q. Alors en multipliant par d^2 notre polynôme, nous éliminerons tous les potentiels dénominateurs et auront un polynôme à coefficients entiers : $d^2X^2-2d^2pX+d^2p^2-d^2q$.
Nous avons bien montré que x est racine d'un polynôme de degré 2 à coefficients entiers.
Donc $y\in A$. Donc $B\subset A$.

Par double inclusion on a bien montré $A=B$.

Exercice **Images et antécédents**

- Soit f l'application définie de $\mathbf{R}$ vers $\mathbf{R}$ par $f(x)=x^2$. Graphiquement, on conjecture que $f([-2,1])=[0,4]$. Démontrons-le.

Montrons que $f([-2,1])\subset[0,4]$.
Soit $x\in[-2,1]$, montrons que $f(x)\in[0,4]$.
On a $-2\leqslant x\leqslant 1$, donc $0\leqslant|x|\leqslant 2$.
Donc $0\leqslant x^2\leqslant 4$ et on obtient bien $f(x)\in[0,4]$.
Donc tous les éléments de $[-2,1]$ ont leur image par f dans $[0,4]$: $f([-2,1])\subset[0,4]$.

Montrons que $[0,4] \subset f([-2,1])$.
Soit $y \in [0,4]$. Posons $x = -\sqrt{y}$ (bien défini car $y \geqslant 0$).
Comme $0 \leqslant y \leqslant 4$, on a $-2 \leqslant -\sqrt{y} \leqslant 0$.
Donc $x \in [-2,1]$.
De plus $f(x) = (-\sqrt{y})^2 = y$. Donc y est l'image d'un élément de $[-2,1]$: $y \in f([-2,1])$.
Donc $[0,4] \subset f([-2,1])$.

Par double inclusion on a montré $f([-2,1]) = [0,4]$.

- Démontrons maintenant que $f^{-1}([-2,1]) = [-1,1]$.

Montrons d'abord $f^{-1}([-2,1]) \subset [-1,1]$.
Soit $x \in f^{-1}([-2,1])$. Par définition cela signifie que $f(x) \in [-2,1]$.
Donc $-2 \leqslant x^2 \leqslant 1$.
Donc en fait $0 \leqslant x^2 \leqslant 1$ et on en déduit $x \in [-1,1]$.
Donc $f^{-1}([-2,1]) \subset [-1,1]$.

Montrons maintenant $[-1,1] \subset f^{-1}([-2,1])$.
Soit $x \in [-1,1]$.
Alors $x^2 \in [0,1]$. Donc a fortiori, $f(x) \in [-2,1]$.
Cela signifie que $x \in f^{-1}([-2,1])$.
Donc $[-1,1] \subset f^{-1}([-2,1])$ et le résultat est finalement démontré par double inclusion.

- Démontrons que $\exp(]-\infty,0]) =]0,1]$.
On sait que la fonction exponentielle est strictement croissante.
Or $\lim_{x \to -\infty} e^x = 0$ et $e^0 = 1$.
Donc pour tout $x \in]-\infty,0]$, $e^x \in]0,1]$.
De plus la fonction exponentielle est continue sur $\mathbf{R}$.
Donc d'après le théorème des valeurs intermédiaires, toutes les valeurs situées entre 0 et 1 sont prises par la fonction entre $-\infty$ et 0.
On déduit de ces deux résultats que $exp(]-\infty,0]) =]0,1]$.

- Soit h définie sur $\mathbf{R}^2$ par $h(x,y) = (x+y, y)$. Pour trouver l'image du carré $[0,1]^2$ par h, on peut commencer par regarder les images des sommets du carré puis d'autres points du carré. On peut alors conjecturer que l'image du carré est le parallélogramme de sommets $(0,0)$, $(1,0)$, $(2,1)$ et $(1,1)$.
Mathématiquement, montrons $h([0,1] \times [0,1]) = \{(x,y) \in \mathbf{R}^2 \mid y \in [0,1], x \in [y, y+1]\}$. Notons B l'ensemble de droite et raisonnons par double inclusion.

Soit $(x,y) \in [0,1] \times [0,1]$.
En particulier $y \in [0,1]$.
De plus comme $x \in [0,1]$, $x + y \in [y, y+1]$.
Ainsi $(x+y, y)$ est bien un élément de la forme (x', y') avec $y' \in [0,1]$ et $x' \in [y', y'+1]$.
Donc $h(x,y) \in B$ et $h([0,1] \times [0,1]) \subset B$.

Soit maintenant $(x', y') \in B$.
Posons $y = y'$ et $x = x' - y'$.
Comme $y' \in [0,1]$, on a aussi $y \in [0,1]$.
De plus, comme $x' \in [y', y'+1]$, on a $x' - y' \in [0,1]$.

Ainsi $(x,y) \in [0,1] \times [0,1]$.
De plus $h(x,y) = (x+y, y) = (x'-y'+y', y') = (x', y')$.
Donc $(x', y') \in h([0,1] \times [0,1])$ et $B \subset h([0,1] \times [0,1])$.
L'égalité est donc bien montrée par double inclusion.

- On peut montrer de manière analogue que $h^{-1}([0,1] \times [0,1]) = \{(x,y) \in \mathbf{R}^2 \mid y \in [0,1], x \in [-y, 1-y]\}$. C'est le parallélogramme de sommets $(0,0)$, $(1,0)$, $(0,1)$ et $(-1,1)$.

Exercice **Injectivité et surjectivité**

On considère les fonctions définies de $\mathbf{R}$ vers $\mathbf{R}$ par

$$\forall x \in \mathbf{R}, \quad f(x) = x^3 + 2, \quad g(x) = \ln(x^2+1), \quad h(x) = 5 - 2e^{-x}, \quad \ell(x) = x + e^x.$$

La fonction f est bijective. Proposons deux démonstrations.
Montrons que f est injective : soient x_1 et x_2 des réels tels que $f(x_1) = f(x_2)$.
Montrons que nécessairement $x_1 = x_2$.
On a $x_1^3 + 2 = x_2^3 + 2$, donc $x_1^3 = x_2^3$.
En passant à la racine cubique, on déduit $x_1 = x_2$. La fonction est bien injective.

Montrons qu'elle est surjective : soit $y \in \mathbf{R}$.
Montrons qu'il existe $x \in \mathbf{R}$ tel que $f(x) = y$. (La résolution au brouillon de l'équation $x^3 + 2 = y$ permet de trouver x.)
Posons $x = \sqrt[3]{y-2}$.
Alors $f(x) = x^3 + 2 = y - 2 + 2 = y$.
Ainsi, tout élément de $\mathbf{R}$ est l'image par f d'un réel : f est surjective.

Seconde démonstration : nous allons montrer que f admet une fonction réciproque. Nous pourrons en déduire que f est bijective.

Posons $\tilde{f}(y) = \sqrt[3]{y-2}$ pour y dans $\mathbf{R}$.
Alors, pour tout $x \in \mathbf{R}$, $\tilde{f} \circ f(x) = \tilde{f}(x^3+2) = \sqrt[3]{x^3+2-2} = x$.
Donc $\tilde{f} \circ f = id_{\mathbf{R}}$.
De même, $\forall y \in \mathbf{R}, f \circ \tilde{f}(y) = f(\sqrt[3]{y-2}) = (\sqrt[3]{y-2})^3 + 2 = y - 2 + 2 = y$.
Donc $f \circ \tilde{f} = id_{\mathbf{R}}$.
La fonction $\tilde{f}$ est donc la fonction réciproque de f. On en déduit que f est bijective et $f^{-1} = \tilde{f}$.

La fonction g est n'est ni surjective ni injective. En effet, $g(1) = g(-1)$, donc 1 et -1 ont la même image par g : g n'est pas injective.
Pour tout réel x, $x^2+1 \geq 1$. Comme ln est croissante, on en déduit : $\forall x \in \mathbf{R}, \ln(x^2+1) \geq \ln(1) = 0$.
En particulier $\forall x \in \mathbf{R}, g(x) \neq -3$.
Ainsi -3 n'est pas dans l'image de g et g n'est pas surjective.

Si on considère la fonction g comme étant définie de $\mathbf{R}_+$ vers $\mathbf{R}_+$, on obtient alors une bijection. Autrement dit, la fonction $\tilde{g}$ définie de $\mathbf{R}_+$ vers $\mathbf{R}_+$ par $\tilde{g}(x) = \ln(x^2+1)$ est une bijection. On peut, pour le démontrer, vérifier qu'elle est bien injective et surjective. On peut également montrer qu'elle admet une bijection réciproque, à savoir la fonction définie de $\mathbf{R}_+$ vers $\mathbf{R}_+$ par $y \mapsto \sqrt{e^y - 1}$.

La fonction h est injective non surjective. Elle permet de définir une bijection de $\mathbf{R}$ vers son image $]-\infty, 5[$ dont la bijection réciproque est la fonction définie sur $]-\infty, 5[$ par $y \mapsto -\ln(\frac{5-y}{2})$.

La fonction ℓ est bijective. Le meilleur moyen de le démontrer est d'étudier ses variations.
Cette fonction est dérivable sur $\mathbf{R}$ et sa dérivée $x \mapsto 1 + e^x$ est strictement positive sur $\mathbf{R}$. On en déduit que ℓ est strictement croissante sur $\mathbf{R}$. En particulier elle est injective.
De plus, elle tend vers $-\infty$ en $-\infty$ et vers $+\infty$ en $+\infty$. Comme elle est continue, on en déduit, d'après le théorème des valeurs intermédiaires que $\forall y \in \mathbf{R}$, $\exists x \in \mathbf{R}, \ell(x) = y$: ℓ est surjective.

On peut ainsi conclure que ℓ est bijective. Elle admet donc une bijection réciproque. Il n'est cependant pas possible d'en donner l'expression. Pour cela, il faudrait pouvoir expliciter l'antécédent de chaque réel y. Cela revient à résoudre en x l'équation $x + e^x = y$. Or on ne sait pas résoudre explicitement cette équation.

Exercice **Injection, surjection, bijection**

Soit $f_8 : \mathbf{Q}^2 \to \mathbf{R},\ (a,b) \mapsto a + b\sqrt{2}$.
Montrons que f_8 est injective : soient (a,b) et (c,d) dans $\mathbf{Q}^2$ telles que $f_8(a,b) = f_8(c,d)$.
Alors $a + b\sqrt{2} = c + d\sqrt{2}$. Donc $a - c = \sqrt{2}(d - b)$.
Si $b \neq d$, alors $\sqrt{2} = \frac{a-c}{d-b}$.
Or a, b, c et d sont des rationnels, donc $\sqrt{2}$ serait aussi un rationnel.
Cela étant faux, on en déduit que $b = d$, puis que $a = c$. Ainsi $(a,b) = (c,d)$ et donc f_8 est injective.

Montrons que f_8 n'est pas surjective : soit $y = \sqrt{3} \in \mathbf{R}$.
Supposons par l'absurde que y est dans l'image de f_8.
Alors il existe $(a,b) \in \mathbf{Q}^2$ tel que $f_8(a,b) = \sqrt{3}$. Donc $a + b\sqrt{2} = \sqrt{3}$.
Élevons au carré : $a^2 + 2b^2 + 2ab\sqrt{2} = 3$.
Si $ab \neq 0$, on peut en déduire comme précédemment que $\sqrt{2}$ est irrationnel ce qui est faux. Donc $ab = 0$.
Donc $a = 0$ ou $b = 0$. On en déduit $a = \sqrt{3}$ ou $b = \sqrt{3/2}$.
Comme a et b sont rationnels, on obtient une contradiction dans les deux cas.
Donc $\sqrt{3}$ n'est pas dans l'image de f_8 et f_8 n'est donc pas surjective.

Proposons une autre preuve : l'ensemble $\mathbf{Q}$ est dénombrable. On peut en déduire que $\mathbf{Q}^2$ est également un ensemble dénombrable. Son image par f_8 est donc au plus dénombrable. En particulier elle ne peut pas être égale à $\mathbf{R}$ qui est indénombrable.

Soit $f_9 : \mathbf{R} \setminus \{1\} \to \mathbf{R},\ x \mapsto \frac{2x+1}{x-1}$.
Montrons que f_9 est injective : soient x et y dans $\mathbf{R} \setminus \{1\}$ tels que $f_9(x) = f_9(y)$.
Alors $\frac{2x+1}{x-1} = \frac{2y+1}{y-1}$.
Donc $(2x+1)(y-1) = (2y+1)(x-1)$, donc $2xy + y - 2x - 1 = 2xy + x - 2y - 1$.
Donc $3y = 3x$ et finalement $x = y$. Donc f_9 est injective.

Proposons une autre preuve : on peut récrire $f_9(x) = 2 + \frac{3}{x-1}$. Alors f_9 est la composée d'applications injectives bien connues : $x \mapsto x - 1$, $x \mapsto \frac{3}{x}$ et $x \mapsto 2 + x$. C'est donc une injection.

Montrons que f_9 n'est pas surjective : soit $y = 2 \in \mathbf{R}$. S'il existe $x \in \mathbf{R} \setminus \{1\}$ tel que $f_9(x) = y$, alors $2x + 1 = 2(x - 1)$, donc $1 = -2$ ce qui est absurde.
Donc 2 n'est pas dans l'image de f_9 qui n'est donc pas surjective.

Exercice **Composée d'injections, surjections, bijections**

Soient $f : E \to F$ et $g : F \to G$. Ainsi $g \circ f : E \to G$.

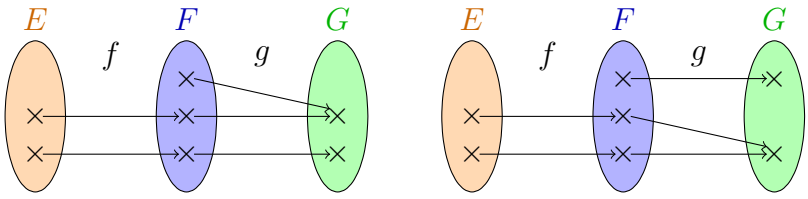
• Supposons f et g injectives et montrons que $g \circ f$ est aussi injective.
Soient x et x' dans E tels que $g \circ f(x) = g \circ f(x')$.
Cela signifie que $g(f(x)) = g(f(x'))$.
Or g est injective, donc si $g(X) = g(X')$ alors nécessairement $X = X'$.
On en déduit ici (avec $X = f(x)$ et $X' = f(x')$) que $f(x) = f(x')$.
Or f est injective. On en déduit donc que $x = x'$.
Nous avons ainsi montré : $g \circ f(x) = g \circ f(x') \implies x = x'$. Donc $g \circ f$ est injective.

• Supposons f et g surjectives et montrons que $g \circ f$ est surjective.
Soit $z \in G$ l'ensemble d'arrivée de $g \circ f$.
Comme g est surjective, il existe $y \in F$ tel que $g(y) = z$.
De même, comme f est surjective de E vers F, il existe $x \in E$ tel que $f(x) = y$.
Ainsi $g(f(x)) = g(y) = z$. Nous avons donc montré : $\forall z \in G, \exists x \in E,\ g \circ f(x) = z$. L'application $g \circ f$ est donc surjective sur G.

• On déduit des deux résultats précédents que si f et g sont bijectives, alors $g \circ f$ est bijective : une composée de bijections est encore une bijection.
• Supposons que $g \circ f$ est injective et montrons que f est injective.
Soient x et x' dans E tels que $f(x) = f(x')$.
Alors $g(f(x)) = g(f(x'))$.
Or $g \circ f$ est injective par hypothèse. Donc on déduit $x = x'$.
Ainsi si $f(x) = f(x')$, alors $x = x'$, donc f est injective.

• Supposons $g \circ f$ surjective et montrons que g est surjective.
Soit $z \in G$.
Comme $g \circ f$ est surjective de E vers G, il existe $x \in E$ tel que $g \circ f(x) = z$.
Posons $y = f(x) \in F$.
Alors $g(y) = g(f(x)) = z$.
Ainsi z admet un antécédent dans F par g. Cela étant vrai pour tout $z \in G$, on déduit que g est surjective.

• Les réciproques sont toutes fausses. Voici des contre-exemples sous forme de patates :



Sur le premier exemple, on voit que f est injective et g est surjective. Mais f n'est pas surjective sur F et g n'est pas injective. Pourtant $g \circ f$ définit une bijection entre les deux éléments de E et les deux éléments de G. On a ainsi un contre-exemple à nos deux premières propositions :
$g \circ f$ est injective mais g n'est pas injective.
$g \circ f$ est surjective mais f n'est pas surjective.

Sur le second exemple, f est toujours injective et g surjective. Mais $g \circ f$ est l'application qui envoie les deux éléments de E sur le second élément de G : elle n'est ni injective, ni surjective. Ainsi nous avons un contre-exemple pour les deux dernières propositions :

f est injective mais $g \circ f$ n'est pas injective.
g est surjective mais $g \circ f$ n'est pas surjective.

Il n'est pas difficile de définir des fonctions explicites sur $\mathbf{R}$ ou sur un autre ensemble classique, vérifiant ces propriétés.

Exercice **Réunion, intersection, etc**

Avant toute chose il faut faire des dessins pour visualiser les ensembles !

Montrons $\bar{A} \cap \bar{B} = \overline{A \cup B}$ par double inclusion.
Montrons $\bar{A} \cap \bar{B} \subset \overline{A \cup B}$.
Soit $x \in \bar{A} \cap \bar{B}$.
Alors $x \in \bar{A}$ ce qui signifie $x \notin A$.
De même, $x \in \bar{B}$, donc $x \notin B$.
Ainsi x n'est ni dans A, ni dans B et donc $x \notin A \cup B$.
Donc $x \in \overline{A \cup B}$ et $\bar{A} \cap \bar{B} \subset \overline{A \cup B}$.

Montrons $\overline{A \cup B} \subset \bar{A} \cap \bar{B}$.
Soit $x \in \overline{A \cup B}$.
Cela signifie $x \notin A \cup B$.
En particulier $x \notin A$, donc $x \in \bar{A}$.
De même $x \notin B$, donc $x \in \bar{B}$.
Ainsi, $x \in \bar{A} \cap \bar{B}$.
Donc $\overline{A \cup B} \subset \bar{A} \cap \bar{B}$.
Par double inclusion, le résultat est démontré.

Montrons $(A \cup B) \cap (\bar{A} \cup B) = B$. Développons l'expression de gauche : $(A \cup B) \cap (\bar{A} \cup B) = [(A \cup B) \cap \bar{A}] \cup [(A \cup B) \cap B] = [(A \cap \bar{A}) \cup (B \cap \bar{A})] \cup [(A \cap B) \cup (B \cap B)]$.
Or $A \cap \bar{A} = \emptyset$ et $B \cap B = B$.
De plus, $B \cap A$ et $B \cap \bar{A}$ sont incluse dans B.
Ainsi la réunion $(B \cap \bar{A}) \cup (A \cap B) \cup B = B$ et le résultat est démontré.

Exercice **Réunion, intersection bis**

On rappelle que A, B et C sont des parties d'un ensemble E. Avant de rédiger quoique ce soit, il est bon de faire un dessin pour visualiser le résultat.

Montrons $A = B \Leftrightarrow A \cap B = A \cup B$.
Montrons d'abord $A = B \implies A \cap B = A \cup B$. Supposons donc que $A = B$. Alors $A \cap B = A$ et $A \cup B = A$. Ainsi $A \cap B = A \cup B$.

Montrons maintenant $A \cap B = A \cup B \implies A = B$.
Supposons $A \cap B = A \cup B$.
Or $A \subset A \cup B$. Donc $A \subset A \cap B$.
Or $A \cap B \subset B$, donc $A \subset B$.
De même, $B \subset A \cup B$ et $A \cup B = A \cap B \subset A$.
Donc $B \subset A$. Par double inclusion, on obtient $A = B$.
Le résultat est donc démontré par double implication.

Montrons $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$.
Montrons la première implication : supposons $A \cup B = A \cap C$.
Alors, comme $B \subset A \cup B$, on obtient $B \subset A \cap C$.
En particulier $B \subset A$.
De plus comme $A \subset A \cup B$, on obtient $A \subset A \cap C$.
Or $A \cap C \subset C$, donc $A \subset C$.
Ainsi $B \subset A \subset C$.

Montrons l'implication réciproque : supposons $B \subset A \subset C$.
Alors $A \cup B = A$ et $A \cap C = A$. Donc $A \cup B = A \cap C$.
Par double implication, le résultat est démontré.

Montrons $A \cap B = A \cap C \Leftrightarrow A \cap \bar{B} = A \cap \bar{C}$ par double implication.
Supposons $A \cap B = A \cap C$.
Soit $x \in A \cap \bar{B}$.
En particulier $x \in A$. Et $x \notin B$.
Donc $x \notin A \cap B$.
Or $A \cap B = A \cap C$, donc $x \notin A \cap C$.
Or $x \in A$, donc cela implique $x \notin C$, *i.e.*$x \in \bar{C}$.
Finalement $x \in A$ et $x \in \bar{C}$, donc $x \in A \cap \bar{C}$.
On a ainsi montré $A \cap \bar{B} \subset A \cap \bar{C}$.
Le même raisonnement permet de montrer $A \cap \bar{C} \subset A \cap \bar{B}$.
Donc par double inclusion, $A \cap \bar{B} = A \cap \bar{C}$ et la première implication est démontré.

Montrons l'implication réciproque. Pour cela, appliquons le résultat ci-dessus aux ensembles A, $\bar{B}$ et $\bar{C}$. On obtient $A \cap \bar{B} = A \cap \bar{C} \implies A \cap \bar{\bar{B}} = A \cap \bar{\bar{C}}$, donc $A \cap \bar{B} = A \cap \bar{C} \implies A \cap B = A \cap C$.
Par double implication le résultat est démontré.

Exercice **Images d'unions et d'intersections.**

1. Soient A et B des parties de E et f une application de E vers F.
   Montrons que $f(A \cup B) \subset f(A) \cup f(B)$: soit $x \in A \cup B$. Alors $x \in A$ ou $x \in B$.
   Si $x \in A$, alors $f(x) \in f(A)$ par définition de $f(A)$.
   De même, si $x \in B$, alors $f(x) \in f(B)$.
   Donc dans tous les cas, $f(x) \in f(A) \cup f(B)$ et donc $f(A \cup B) \subset f(A) \cup f(B)$.

   Montrons $f(A) \cup f(B) \subset f(A \cup B)$: soit $y \in f(A) \cup f(B)$. Alors $y \in f(A)$ ou $y \in f(B)$.
   Si $y \in f(A)$, alors cela signifie qu'il existe $x \in A$ tel que $y = f(x)$.
   Et comme $A \subset A \cup B$, $x \in A \cup B$ et $y \in f(A \cup B)$.
   De même, si $y \in f(B)$, on déduit que $y \in f(A \cup B)$.
   Dans tous les cas on conclut $y \in f(A \cup B)$, donc $f(A) \cup f(B) \subset f(A \cup B)$.

   Par double inclusion, on a démontré $f(A) \cup f(B) = f(A \cup B)$.

2. Montrons que : $\forall A \subset E, \forall B \subset E,\ \ f(A \cap B) = f(A) \cap f(B)$ équivaut à dire que f est injective.

   Commençons par la première implication : supposons la propriété de l'intersection satisfaite et montrons alors que f est injective.

Soient x et x' dans E tels que $f(x) = f(x')$. Appliquons la propriété aux ensembles $A = \{x\}$ et $B = \{x'\}$: $f(A \cap B) = f(A) \cap f(B)$, donc $f(\{x\} \cap \{x'\}) = \{f(x)\} \cap \{f(x')\}$.
Comme $f(x) = f(x')$, $\{f(x)\} \cap \{f(x')\} = \{f(x)\}$.
En particulier c'est un ensemble non vide. Donc $f(\{x\} \cap \{x'\})$ doit aussi être non vide.
Cela implique que $\{x\} \cap \{x'\} \neq \emptyset$ et donc $x = x'$.
Ainsi f est injective.

Passons à la réciproque : supposons f injective. Commençons par une propriété qui ne dépend pas de f. Soient A et B des parties de E.
Comme $A \cap B \subset A$, on obtient naturellement $f(A \cap B) \subset f(A)$. De même $f(A \cap B) \subset f(B)$, donc finalement $f(A \cap B) \subset f(A) \cap f(B)$ quelque soit la fonction f.
Montrons maintenant l'autre inclusion en utilisant cette fois l'injectivité de f. Soit $y \in f(A) \cap f(B)$.
Donc $y \in f(A) : \exists x \in A,\ \ f(x) = y$.
De plus $y \in f(B) : \exists x' \in B,\ \ f(x') = y$.
Ainsi $f(x) = f(x')$. Or f est injective donc $x = x'$.
On en déduit que $x \in A \cap B$ et que $y = f(x)$.
Donc $y \in f(A \cap B)$ et on conclut que $f(A) \cap f(B) \subset f(A \cap B)$.
Conclusion : si f est injective, alors $\forall A \subset E, \forall B \subset E,\ \ f(A \cap B) = f(A) \cap f(B)$.

3. Montrons que : $\forall A \subset E,\ \ f(\bar{A}) = \overline{f(A)}$ équivaut à dire que f est surjective.

Commençons par la première implication : supposons la propriété du complémentaire satisfaite et démontrons alors que f est surjective.
Appliquons la propriété à l'ensemble $A = \emptyset$: $f(\bar{A}) = \overline{f(A)}$, donc $f(E) = \overline{f(\emptyset)} = \overline{\emptyset} = F$.
Ainsi $f(E) = F$ et l'application f est surjective.

Passons à la réciproque : supposons y surjective.
Soit A une partie de E.
D'après la première question $f(A) \cup f(\bar{A}) = f(A \cup \bar{A}) = f(E)$.
Comme f est supposée surjective, $f(E) = F$.
Donc $f(A) \cup f(\bar{A}) = F$.
Autrement dit, $f(\bar{A})$ est le complémentaire de $f(A)$ dans F : $f(\bar{A}) = \overline{f(A)}$.

Exercice **Preuve de l'indénombrabilité de $\mathbf{P}(\mathbf{N})$**

1. Donnons quatre exemples d'applications de $\mathbf{N}$ vers $\mathbf{P}(\mathbf{N})$:

$$\forall n \in \mathbf{N}, f_1(n) = \emptyset, \quad f_2(n) = \{n\}, \quad f_3(n) = \{0, 1, 2, \ldots, n-1, n\}, \quad f_4(n) = \mathbf{N} \setminus \{n\}.$$

On remarque que ces applications sont clairement non bijectives.

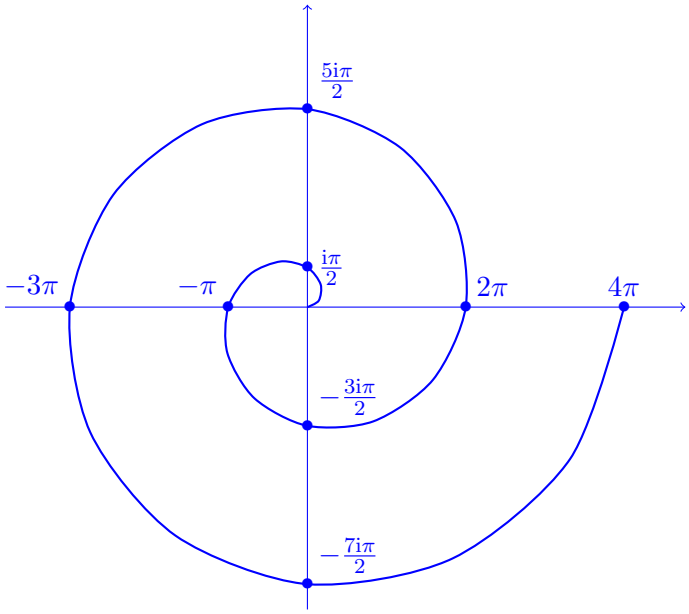
2. Supposons par l'absurde que A possède un antécédent par f : $\exists n \in \mathbf{N},\ \ f(n) = A$. On rappelle que A est une partie de $\mathbf{N}$.
Si $n \in A$, alors par définition de A, on a $n \notin f(n)$. Or $f(n) = A$, donc si $n \in A$, on obtient $n \notin A$, ce qui est absurde.
Si $n \notin A$, alors par définition de A, on a $n \in f(n)$. Donc $n \in A$, ce qui encore absurde.
Dans tous les cas, on obtient une contradiction. Donc l'ensemble A n'a pas d'antécédent par f. Or f étant parfaitement quelconque, on en déduit qu'il n'existe pas d'application

surjective de $\mathbf{N}$ vers $\mathbf{P}(\mathbf{N})$. Ces deux ensembles ne sont donc pas en bijection ce qui signifie que $\mathbf{P}(\mathbf{N})$ n'est pas dénombrable.

4 Complexes

Exercice **Exercices de base**

L'ensemble $\{\theta e^{i\theta}; \theta \in \mathbf{R}_+\}$ est une spirale : l'argument augmente avec le module. On le représente ci-contre pour θ entre 0 et 4π.



Exercice **Formes polaires**

— $(1+i)(\sqrt{3}-i)$: surtout, ne pas développer. Graphiquement, on voit immédiatement que $1+i = \sqrt{2}e^{i\frac{\pi}{4}}$. D'autre part, $\sqrt{3}-i$ est de module 2 et en factorisant par son module, on reconnaît une expression trigonométrique :

$$\sqrt{3}-i = 2(\tfrac{\sqrt{3}}{2} - \tfrac{1}{2}i) = 2(\cos(-\tfrac{\pi}{6} + i\sin(-\tfrac{\pi}{6})) = 2e^{-i\frac{\pi}{6}}.$$

Ainsi

$$(1+i)(\sqrt{3}-i) = \sqrt{2}e^{i\frac{\pi}{4}}2e^{-i\frac{\pi}{6}} = 2\sqrt{2}e^{-\frac{\pi}{12}}.$$

— $\frac{5}{(1-i)(2-i)(3-i)}$: là il faut développer. Ce nombre est égal à $\frac{5}{-10i} = \frac{i}{2} = \frac{1}{2}e^{i\frac{\pi}{2}}$.

— $3+7i$: il est de module $\sqrt{58}$ et il n'y a aucun espoir de reconnaître son argument. Tout ce qu'on peut dire est que sa partie réelle étant strictement positive, son argument s'exprime par $\arctan(\frac{7}{3})$. Donc $3+7i = \sqrt{58}e^{i\arctan(\frac{7}{3})}$.

— $\frac{(\sqrt{3}+i)^8}{(-1+i)^4}$: ne surtout pas développer. Écrire les formes polaires de $\sqrt{3}+i$ et $-1+i$ puis calculer ensuite simplement les puissances et le quotient.

Exercice **Une factorisation intéressante**

Factorisation de $e^{i\alpha} + e^{i\beta}$: les nombres $e^{i\alpha}$ et $e^{i\beta}$ sont sur le cercle trigonométrique. Leur somme s'obtient graphiquement en additionnant les vecteurs correspondants. Avec O, on obtient les 4 sommets d'un losange de côté 1. On en déduit graphiquement que l'argument de $e^{i\alpha}+e^{i\beta}$ est la moyenne des angles α et β. On factorise alors par $e^{i\frac{\alpha+\beta}{2}}$:

$$e^{i\alpha} + e^{i\beta} = e^{i\frac{\alpha+\beta}{2}}(e^{i\frac{\alpha-\beta}{2}} + e^{i\frac{-\alpha+\beta}{2}}) = e^{i\frac{\alpha+\beta}{2}}2\cos(\tfrac{\alpha-\beta}{2}).$$

Si le cosinus est un nombre positif, on a obtenu la forme polaire recherchée. S'il est négatif, on écrit $\cos(\frac{\alpha-\beta}{2}) = \left|\cos(\frac{\alpha-\beta}{2})\right| \mathrm{e}^{\mathrm{i}\pi}$ pour obtenir la forme polaire.

En appliquant cette même méthode, on obtient la forme polaire d'expressions plus compliquées :

$$\frac{\mathrm{e}^{\mathrm{i}\alpha} - \mathrm{e}^{\mathrm{i}\beta}}{1 - \mathrm{e}^{\mathrm{i}\beta}} = \frac{\mathrm{e}^{\mathrm{i}\frac{\alpha+\beta}{2}} 2\mathrm{i}\sin(\frac{\alpha-\beta}{2})}{\mathrm{e}^{\mathrm{i}\frac{\beta}{2}} 2\mathrm{i}\sin(\frac{-\beta}{2})} = \mathrm{e}^{\mathrm{i}\frac{\alpha}{2}} \frac{\sin(\frac{\alpha-\beta}{2})}{\sin(\frac{-\beta}{2})}.$$

Si cette fraction est un nombre positif, alors nous avons obtenu la forme polaire du nombre complexe considéré. On en déduit alors que l'argument de $\frac{\mathrm{e}^{\mathrm{i}\alpha}-\mathrm{e}^{\mathrm{i}\beta}}{1-\mathrm{e}^{\mathrm{i}\beta}}$ est $\frac{\alpha}{2}$.
Rappelons que $\arg(\frac{z_A-z_B}{z_C-z_B})$ est l'angle orienté $\widehat{CBA}$. Avec les notations de l'exercice, on déduit que $\widehat{IBA} = \frac{\alpha}{2} = \frac{1}{2}\widehat{IOA}$.

Exercice **Équation et géométrie**

1. L'équation $\frac{z-2}{z-1} = i$ est équivalente à

   $$z - 2 = i(z-1) \quad \text{et} \quad z \neq 1.$$

   C'est une équation d'ordre 1 facile à résoudre. On obtient

   $$z = \frac{2-i}{1-i} = \frac{3}{2} + \frac{i}{2} \neq 1.$$

2. Reprenons la résolution. Si z est solution de l'équation, alors en particulier $\left|\frac{z-2}{z-1}\right| = |i| = 1$. Donc $|z-2| = |z-1|$. Cela signifie que le point M d'affixe z est à égale distance des points d'affixe 1 et 2. Il est donc situé sur la médiatrice de $[AB]$.

   De même, on doit avoir $\arg(\frac{z-2}{z-1}) = \arg(i) = \frac{\pi}{2}$. Donc $\arg(z-2) - \arg(z-1) = \frac{\pi}{2}$. Cela signifie géométriquement que l'angle orienté $\widehat{AMB}$ vaut $\frac{\pi}{2}$.
3. Avec les deux propriétés ci-dessus, on trouve facilement le point M géométriquement : il est situé sur la droite d'équation $y = \frac{3}{2}$ et le triangle AMB est rectangle en M. Donc M est sur le cercle de diamètre $[AB]$. On retrouve bien la solution de la question 1.
4. Si z est solution de $\left(\frac{z-2}{z-1}\right)^n = i$, alors l'égalité reste vraie en module et on obtient $\left|\frac{z-2}{z-1}\right|^n = 1$, donc $\left|\frac{z-2}{z-1}\right| = 1$. C'est la même condition qu'à la question 2 et on retrouve le fait que M est sur la médiatrice de $[AB]$.
5. Le même raisonnement avec les arguments aboutit à $2\arg(z-2) - 2\arg(z-1) = \frac{\pi}{2} \mod 2\pi$, donc $\arg(z-2) - \arg(z-1) = \frac{\pi}{4} \mod \pi$. Autrement dit, l'angle orienté $\widehat{AMB} = \frac{\pi}{4}$ ou $\widehat{AMB} = \frac{\pi}{4} + \pi = \frac{5\pi}{4}$.
   On trouve graphiquement deux solutions, l'une au-dessus de l'axe réel tel que AMB ait un angle intérieur de $\frac{\pi}{4}$ et une en-dessous de l'axe réel tel que AMB ait un angle intérieur de $\frac{3\pi}{4}$.

   Analytiquement, on peut résoudre l'équation en cherchant z sous la forme $z = \frac{3}{2} + iy$. On obtient $(\frac{3}{2} + iy - 2)^2 = i(\frac{3}{2} + iy - 1)^2$ puis $(-1+i)y^2 + (-i+1)y + \frac{1}{4} - \frac{i}{4} = 0$ donc $y^2 - y - \frac{1}{4} = 0$. Les racines de ce polynôme sont $y = \frac{1+\sqrt{2}}{2}$ et $y = \frac{1-\sqrt{2}}{2}$.

Exercice **Racines de polynômes complexes**

— $P = X^2 + (2-2i)X - 2i$: son discriminant vaut $\Delta = (2-2i)^2 - 4(-2i) = 0$, donc P possède une racine double $-\frac{2-2i}{2} = -1+i$. Donc P se factorise en $P = (X+1-i)^2$.

— $Q = X^2 + (i-3)X - 3i$: son discriminant vaut $\Delta = (i-3)^2 + 12i = 8+6i$. Il faut extraire une racine carrée de Δ : on cherche $\delta = x+iy$ tel que $\delta^2 = \Delta$. On obtient le système $x^2 - y^2 = 8, 2xy = 6, x^2 + y^2 = |\Delta| = 10$. On en déduit $x = \pm 3$ et $y = \pm 1$. or $xy > 0$, donc $\delta = 3+i$ ou $\delta = -3-i$.
Alors les racines de Q sont :

$$\frac{-(i-3)+3+i}{2} = 3, \qquad \frac{-(i-3)-3-i}{2} = -i.$$

Et $Q = (X-3)(X+i)$.

— $R = iX^2 - X + 1$: son discriminant vaut $\Delta = 1-4i$. Une racine carrée est (après calcul) $\delta = \sqrt{\frac{\sqrt{17}+1}{2}} - i\sqrt{\frac{\sqrt{17}-1}{2}}$ et les racines de R sont

$$\frac{1+\delta}{2i}, \qquad \frac{1-\delta}{2i}.$$

— $S = X^6 + 27$: soit $z \in \mathbf{C}$. Alors z est racine du polynôme si et seulement si $z^6 = -27$, si et seulement z est une racine sixième de $-27 = 27e^{i\pi}$. les racines de S sont donc les nombres

$$\sqrt[6]{27}e^{i(\frac{\pi}{6}+\frac{2k\pi}{6})} = \sqrt{3}e^{i\frac{\pi}{6}(1+2k)},$$

avec $k = 0, 1, \ldots, 5$. Ces nombres sont tous situés sur le cercle de centre O de rayon $\sqrt{3}$ et forment un hexagone régulier.

— $T = X^5 - X^4 + 4X - 4$: on remarque que 1 est une racine de T. On peut donc factoriser T : $T = (X-1)(X^4+4)$. On en déduit que les racines de T sont 1 et les racines quatrièmes de -4 qu'on peut aisément trouver.

— Les solutions du système $u+v = 3$ et $uv = -4$ sont les racines du polynôme $X^2 - 2X - 4$. Le second système se ramène à un système du même genre.

Exercice **Calculs de** $\cos(\frac{\pi}{6})$ **et** $\sin(\frac{\pi}{6})$

1. Les racines du polynôme $P = X^2 - 2\mathrm{i}X - 4$ sont $\sqrt{3}+\mathrm{i}$ et $-\sqrt{3}+\mathrm{i}$.
2. Soit z une racine de P. Alors $z^2 - 2\mathrm{i}z - 4$. En multipliant par z, on obtient $z^3 - 2\mathrm{i}z^2 - 4z$. Or d'après la première égalité, $z^2 = 2\mathrm{i}z + 4$. En remplaçant ainsi z^2 dans la seconde, on obtient $z^3 - 2\mathrm{i}(2\mathrm{i}z+4) - 4z = 0$, donc $z^3 + 4z - 8\mathrm{i} - 4z = 0$ et finalement $z^3 = 8\mathrm{i}$.
Il était également possible de vérifier que $(\sqrt{3}+\mathrm{i})^3 = 8\mathrm{i}$ et $(-\sqrt{3}+\mathrm{i})^3 = 8\mathrm{i}$.
3. On déduit que si z est racine de P, alors z est une racine cubique de $8\mathrm{i}$. La forme polaire de $8\mathrm{i}$ est $8\mathrm{e}^{\mathrm{i}\frac{\pi}{2}}$. Ses racines cubiques sont les nombres de la forme $\sqrt[3]{8}\mathrm{e}^{\mathrm{i}(\frac{\pi}{6}+\frac{2k\pi}{3})}$, $k = 0, 1, 2$. Il s'agit des nombres complexes $2\mathrm{e}^{\mathrm{i}\frac{\pi}{6}}$, $2\mathrm{e}^{\mathrm{i}\frac{5\pi}{6}}$ et $-2\mathrm{i}$.
Ces nombres ne sont pas tous racines de P, nous n'avons pas raisonné par équivalence. On constate immédiatement grâce à la question 1 que $-2\mathrm{i}$ n'en est pas une. Donc les racines de P sont $2\mathrm{e}^{\mathrm{i}\frac{\pi}{6}}$ et $2\mathrm{e}^{\mathrm{i}\frac{5\pi}{6}}$.
4. Il ne reste qu'à comparer avec les résultats de la question 1. Pour des questions angulaires, on voit que $2\mathrm{e}^{\mathrm{i}\frac{\pi}{6}}$ est de partie réelle positive tandis que $2\mathrm{e}^{\mathrm{i}\frac{5\pi}{6}}$ est de partie réelle négative. On peut donc affirmer que c'est le premier des deux qui est égal à $\sqrt{3}+\mathrm{i}$. Donc $2\cos(\frac{\pi}{6}) + 2\mathrm{i}\sin(\frac{\pi}{6}) = \sqrt{3}+\mathrm{i}$. En identifiant parties réelles et imaginaires, on retrouve les valeurs bien connues de ce cosinus et ce sinus.

5. On cherche de la même manière à déterminer les autres valeurs trigonométriques bien connues. On sait que $(\mathrm{e}^{\mathrm{i}\frac{\pi}{4}})^2 = \mathrm{e}^{\mathrm{i}\frac{\pi}{2}} = \mathrm{i}$. Ainsi $\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}$ est une racine carrée de i (ou autrement dit une racine du polynôme $X^2 - \mathrm{i}$). On peut déterminer les racines carrées de i avec la méthode algébrique. Cela revient à résoudre le système $x^2 - y^2 = 0$ et $2xy = 1$. On en déduit facilement que $x = y = \pm\frac{\sqrt{2}}{2}$. Comme les racines carrées de i sont sous forme polaire $\pm\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}$, il en reste qu'à identifier et conclure.

   Pour $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$, c'est plus délicat. On sait que $(\mathrm{e}^{\mathrm{i}\frac{\pi}{3}})^2 = \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}}$. Si on représente les points d'affixes $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$ et $\mathrm{e}^{\mathrm{i}\frac{2\pi}{3}}$, on peut montrer qu'ils forment avec l'origine un triangle équilatéral. Avec d'autres considérations angulaires, on peut aussi montrer que $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$ et $\mathrm{e}^{\mathrm{i}\frac{2\pi}{3}}$ ont la même partie imaginaire. On peut alors déduire de tout cela que $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}} - \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}} = 1$. Donc $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$ est racine du polynôme $X - X^2 - 1$.
   Autre méthode : on sait que $(\mathrm{e}^{\mathrm{i}\frac{\pi}{3}})^3 = \mathrm{e}^{\mathrm{i}\pi} = -1$. Donc $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$ est une racine cubique de -1 ou encore une racine du polynôme $X^3 + 1$. Or ce polynôme se factorise en $X^3 + 1 = (X + 1)(X^2 - X + 1)$ et on en déduit que $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$ est racine de $X^2 - X + 1$.
   Il ne reste alors qu'à calculer les racines de ce polynôme sous forme algébrique et à les comparer à $\mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$.

   Passons à $\mathrm{e}^{\mathrm{i}\frac{\pi}{6}}$. Les racines cubiques de $\mathrm{i} = \mathrm{e}\mathrm{i}\frac{\pi}{2}$ sont $\mathrm{e}\mathrm{i}\frac{\pi}{6}$, $\mathrm{e}\mathrm{i}(\frac{\pi}{6} + \frac{2\pi}{3}) = \mathrm{e}\mathrm{i}\frac{5\pi}{6}$ et $\mathrm{e}\mathrm{i}(\frac{\pi}{6} + \frac{4\pi}{3}) = \mathrm{e}\mathrm{i}\frac{9\pi}{6} = -\mathrm{i}$. Nous cherchons donc une des racines du polynôme $X^3 - \mathrm{i}$. Il se factorise en $X^3 - \mathrm{i} = X^3 - (-\mathrm{i})^3 = (X - \mathrm{i})(X^2 - \mathrm{i}X + (-\mathrm{i})^2)$. Ainsi $\mathrm{e}^{\mathrm{i}\frac{\pi}{6}}$ est une racine de $X^2 - \mathrm{i}X - 1$ (puisqu'il n'est pas égal à i). Son discriminant est $\Delta = (-\mathrm{i})^2 + 4 = 3$ et ses racines sont $\frac{\mathrm{i}+\sqrt{3}}{2}$ et $\frac{\mathrm{i}-\sqrt{3}}{2}$. Comme $\mathrm{e}^{\mathrm{i}\frac{\pi}{6}}$ est de partie réelle positive, nous concluons que $\mathrm{e}^{\mathrm{i}\frac{\pi}{6}} = \frac{\mathrm{i}+\sqrt{3}}{2}$ et par identification des parties réelle et imaginaire : $\cos(\frac{\pi}{6} = \frac{\sqrt{3}}{2}$ et $\sin(\frac{\pi}{6} = \frac{1}{2}$.

Exercice **Calcul de somme et de primitive**

Calculons $S = \sum_{i=0}^{n} \cos(kx)$. Remarquons que S est la partie réelle de $\sum_{i=0}^{n} e^{ikx} = \sum_{i=0}^{n} (e^{ix})^k$. On reconnaît la somme des termes d'une suite géométrique.

Si x est de la forme $2j\pi$ avec $j \in \mathbf{Z}$, $e^{ix} = 1$ et $S = \mathrm{Re}(\sum_{i=0}^{n} 1) = n + 1$.

Sinon, $e^{ix} \neq 1$ et

$$\sum_{i=0}^{n} (e^{ix})^k = \frac{1 - (e^{ix})^{n+1}}{1 - e^{ix}} = \frac{1 - e^{i(n+1)x}}{1 - e^{ix}}$$

$$= \frac{e^{ix(n+1)/2}(e^{-ix(n+1)/2} - e^{ix(n+1)/2})}{e^{ix/2}(e^{-ix/2} - e^{ix/2})} = e^{inx/2} \frac{\sin(x(n+1)/2)}{\sin(x/2)}.$$

Donc $S = \cos(nx/2)\frac{\sin(x(n+1)/2)}{\sin(x/2)}$.

Pour le calcul de $\sum_{i=0}^{n} \sin^2(kx)$, on ne peut pas dire qu'il s'agit de la partie imaginaire de $\sum_{i=0}^{n} e^{2ikx}$. Il faut utiliser la formule d'Euler : $\sum_{i=0}^{n} \sin^2(kx) = \sum_{i=0}^{n} (\frac{e^{ikx} - e^{-ikx}}{2i})^2$. Puis il faut développer et reconnaître des sommes géométriques.

Calculons $\int_{-\pi}^{\pi} \sin^4(x)dx$. Pour cela, linéarisons $\sin^4(x)$:

$$\sin^4(x) = (\frac{e^{ix} - e^{ix}}{2i})^4 = \frac{1}{2^4}(e^{4ix} - 4e^{3ix}e^{-ix} + 6e^{2ix}e^{-2ix} - 4e^{ix}e^{-3ix} + e^{-4ix})$$

$$= \frac{1}{2^4}(e^{4ix} + e^{-4ix} - 4e^{2ix} - 4e^{-2ix} + 6) = \frac{1}{2^4}(2\cos(4x) - 8\cos(2x) + 6).$$

Une primitive de cette fonction est $\frac{1}{2^4}(\sin(4x)/2 - 4\sin(2x) + 6x)$. L'intégrale étudiée vaut donc $12\pi/16 = 3\pi/4$.

Exercice **Transformations géométriques**

Soit f définie sur $\mathbf{C}$ par $f(z) = iz + 2$. Pour z dans $\mathbf{C}$, on peut écrire $f(z) = e^{i\pi/2}z + 2$. On reconnaît un terme de translation et un terme de rotation. On en déduit que f est la composée de la rotation de centre O et d'angle $\pi/2$ et de la translation de vecteur 2 :

$$f = T_2 \circ R_{\pi/2}.$$

On peut de plus montrer que f est une rotation. Pour cela, commençons par chercher le centre de cette rotation. C'est le point de $\mathbf{C}$ qui est laissé invariant par f. Soit ω tel que $f(\omega) = \omega$. On trouve $\omega = \frac{2}{1-i} = 1 + i$.

Alors pour tout z dans $\mathbf{C}$, on peut écrire

$$f(z) = iz + 2 = i(z - \omega) + \omega = T_\omega \circ R_{\pi/2} \circ T_{-\omega}(z).$$

Il s'agit de la rotation de centre ω et d'angle $\pi/2$.

Soit g définie sur $\mathbf{C}$ par $g(z) = i\bar{z}$. On reconnaît un terme de rotation et un terme de symétrie par rapport à l'axe des abscisses :

$$g = R_{\pi/2} \circ S.$$

On peut aussi reconnaître directement la symétrie par rapport à la droite passant par 0, d'angle $\pi/4$.

Essayons de le redémontrer. On cherche l'ensemble des points de $\mathbf{C}$ laissés invariant par g. Soit $z \in \mathbf{C}$ tel que $g(z) = z$. Notons-le $z = x + iy$ avec $x, y \in \mathbf{R}$. Alors $x + iy = i(x - iy) = y + ix$. On en déduit en identifiant ces deux écritures algébriques que $x = y$ et $y = x$. Donc la droite du plan définie par $x = y$ est laissée invariante par g.

Montrons que g est la symétrie orthogonale par rapport à cette droite. Soit $z = x + iy \in \mathbf{C}$. Alors $g(z) = i(x - iy) = y + ix$. Ainsi g envoie le point de coordonnées (x, y) sur le point de coordonnées (y, x). Il s'agit bien de la symétrie orthogonale par rapport à la droite d'équation $x = y$.

Soit h définie sur $\mathbf{C}$ par $h(z) = \bar{z} + 3 - \mathrm{i}$. On peut décomposer h en reconnaissant une symétrie d'axe réel et une translation :

$$h = T_{3+\mathrm{i}} \circ S_{\mathbf{R}}.$$

En particulier, h est une composée d'isométries, donc également une isométrie. Cherchons les points fixes de h. Soit $z \in \mathbf{C}$. On l'écrit $z = x + \mathrm{i}y$. Alors

$$h(z) = z \text{ ssi } x - \mathrm{i}y + 3 - \mathrm{i} = x + \mathrm{i}y \text{ ssi } x + 3 = x \text{ et } -y - 1 = y.$$

Ces deux équations étant impossibles à satisfaire, on en déduit que h ne possède pas de point fixe. Comme h n'est visiblement pas une translation, il doit s'agir d'une symétrie glissée.

Afin de mieux comprendre cette transformation, nous allons essayer d'exprimer h comme une composée d'une symétrie et d'une translation parallèle à l'axe de la symétrie. Le mieux est de

commencer par représenter les images de plusieurs points du plan pour visualiser l'action de h. On peut ainsi voir que l'axe de la symétrie de h est horizontal. Récrivons h :

$$h(z) = \bar{z} + 3 - \mathrm{i} = \overline{z + \mathrm{i}} + 3.$$

Montrons que $s : z \mapsto \overline{z + \mathrm{i}}$ est la symétrie d'axe la droite d'équation $y = -\frac{1}{2}$. Soit $z' = -\frac{\mathrm{i}}{2}$ un point de cette droite. Alors, pour tout $z = x + \mathrm{i}y$,

$$|s(z) - z'| = |x - \mathrm{i}y - \mathrm{i} + \tfrac{\mathrm{i}}{2}| = |x + \mathrm{i}(-y - \tfrac{1}{2})| = |x + \mathrm{i}(y + \tfrac{1}{2})| = |z - z'|.$$

Ainsi, tout point z' de la droite D est à la même distance des points d'affixe z et $s(z)$. La transformation s est donc bien la symétrie d'axe D. Et finalement, nous pouvons écrire h comme la composée de cette symétrie et de la translation de vecteur 3 : $h = T_3 \circ S_D$ ou encore $h = S_D \circ T_3$ car ces deux transformations commutent.

Exercice **Extrema d'une fonction trigonométrique**

Trouver la valeur maximale de : $f(x) = \cos(x) + 2\cos(x + \frac{\pi}{3})$.

La fonction f est 2π-périodique. Sa dérivée est donnée par : $f'(x) = -\sin(x) - 2\sin(x + \frac{\pi}{3})$. Pour étudier son signe, nous devons résoudre : $f'(x) = 0$. Or nous ne savons pas résoudre explicitement l'équation $\sin(x) = -2\sin(x + \frac{\pi}{3})$. Avec un peu de trigonométrie, nous pouvons la transformer en : $\sin(x) = -2\sin(x)\cos(\frac{\pi}{3}) - 2\cos(x)\sin(\pi/3)$ puis $2\sin(x) = -\sqrt{3}\cos(x)$. On obtient $x = \arctan(-\sqrt{3}/2)$, mais c'est difficilement exploitable (à moins de faire beaucoup de trigonométrie).

Introduisons la fonction complexe : $g(x) = \mathrm{e}^{\mathrm{i}x} + 2\mathrm{e}^{\mathrm{i}(x+\pi/3)}$. Ainsi, pour tout x, $f(x)$ est égal à la partie réelle de $g(x)$. En particulier, pour tout x, $f(x) \leqslant |g(x)|$. Or le module de g est facile à calculer :

$$|g(x)| = \left|\mathrm{e}^{\mathrm{i}x}\left(1 + 2\mathrm{e}^{\mathrm{i}\pi/3}\right)\right| = \left|1 + 2\mathrm{e}^{\mathrm{i}\pi/3}\right| = |2 + \mathrm{i}\sqrt{3}| = \sqrt{7}.$$

Donc, pour tout x, $f(x) \leqslant \sqrt{7}$. Enfin, étudions la partie imaginaire de g : $h(x) = \sin(x) + 2\sin(x + \frac{\pi}{3})$. Son étude permet de montrer qu'elle s'annule (TVI avec $h(0) > 0$ et $h(\pi) < 0$). Ainsi, il existe x tel que $g(x) = f(x)$. En cette valeur, $|f(x)| = |g(x)| = \sqrt{7}$. En précisant un peu notre étude, on comprend que f est une fonction sinusoïdale, et elle a ainsi pour maximum $\sqrt{7}$ et pour minimum $-\sqrt{7}$.

Remarques : le passage en complexe a permis d'accéder très simplement aux extrema de f, mais sans en déterminer les positions. C'est une des raisons qui rend l'utilisation des complexes si fréquente en physique. Il est classique de rencontrer des sommes de fonctions sinusoïdales de même fréquence, mais déphasées (phénomènes d'interférences, d'échos, etc). La méthode étudiée permet d'accéder facilement à l'amplitude de l'onde résultante.

Si on souhaite être plus précis, il faut faire de la trigonométrie. Là encore, le plus simple est de passer par les complexes et notamment les formules d'Euler. On montre ainsi que :

$$f(x) = -\sqrt{7}\sin(x - \arctan(\sqrt{3}/2)).$$

Sous cette forme, les valeurs extrémales de f et leurs positions sont évidentes.

Exercice **Triangles équilatéraux**

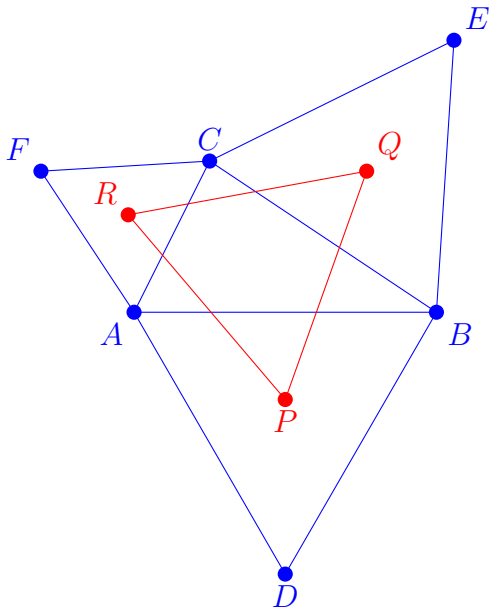
1. On considère dans le plan trois points A, B et C, d'affixes respectives a, b et c. Trouver une condition nécessaire et suffisante sur a, b et c, faisant intervenir le nombre $k = \mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$, pour que le triangle ABC soit équilatéral.
   Le nombre k écrit sous forme polaire évoque un angle. Partir du fait que les trois côtés du triangle sont de même longueur n'est sans doute pas la bonne idée :

$$|a-b| = |b-c| = |c-a|.$$

   La bonne caractérisation d'un triangle équilatéral est ici la suivante : c'est un triangle isocèle dont l'un des angles est égal à $\frac{\pi}{3}$.
   Supposons que les sommets du triangle ABC soient disposés dans un sens direct, c'est-à-dire que l'angle $\widehat{BAC}$ est compris entre 0 et π. Alors ABC est équilatéral si et seulement si C est l'image de B par la rotation de centre A et d'angle $\frac{\pi}{3}$. En écriture complexe, cela s'écrit ainsi : $c = \mathrm{e}^{\mathrm{i}\frac{\pi}{3}}(b-a)+a$. Avec la notation $k = \mathrm{e}^{\mathrm{i}\frac{\pi}{3}}$, nous concluons que ABC est équilatéral si et seulement si

$$(1-k)a + kb - c = 0$$

2. Soient $\mathcal{T}$ un triangle quelconque du plan. On construit les trois triangles équilatéraux extérieurs à $\mathcal{T}$, de bases les côtés de $\mathcal{T}$. Montrer que les centres de gravité de ces trois triangles forment un triangle équilatéral.
   Commençons par faire une figure



   Le triangle $\mathcal{T}$ a pour sommets A, B et C. Insistons sur le fait qu'il est quelconque. Par hypothèse, les triangles ADB, BEC et ACF sont équilatéraux. Il s'agit de montrer que le triangle PQR est également équilatéral.

   Notons en minuscule les affixes de tous ces points. D'après la condition obtenue précédemment, en tenant compte des orientations des triangles, nous avons :

$$(1-k)d + kb - a = 0, \quad (1-k)b + ke - c = 0, \quad (1-k)a + kc - f = 0.$$

Par ailleurs, l'affixe du barycentre d'un triangle est facile à exprimer, c'est la moyenne des affixes des sommets :

$$p = \frac{1}{3}(a+d+b), \qquad q = \frac{1}{3}(b+e+c), \qquad r = \frac{1}{3}(a+c+f).$$

Il ne reste qu'à vérifier la condition d'équilatéralité :

$$\begin{aligned} kq + (1-k)p - r &= \frac{1-k}{3}(a+d+b) + \frac{k}{3}(b+e+c) - \frac{1}{3}(a+c+f) \\ &= \frac{1}{3}\big((1-k)a + (1-k)d + (1-k)b + kb + ke + kc - a - c - f\big) \\ &= \frac{1}{3}\big((1-k)d + kb - a \quad + \quad (1-k)b + ke - c \quad + \quad (1-k)a + kc - f\big) \\ &= 0 \end{aligned}$$

Donc PQR est bien un triangle équilatéral.

Exercice **Inversion**

L'inversion de centre O, de rapport 1, est la transformation du plan qui à tout point $M \neq O$ associe le point N aligné avec O et M tel que $\overline{OM} \cdot \overline{ON} = 1$.

1. Déterminer l'expression complexe de cette transformation φ.
   O, M et N sont alignés, et comme $\overline{OM} \cdot \overline{ON} > 0$, M et N sont situés du même côté par rapport à O. Autrement dit, M et N ont le même argument. Si on note $z = re^{i\theta}$ l'affixe de M, alors celle de N est de la forme $z' = r'e^{i\theta}$.
   Enfin, $\overline{OM} \cdot \overline{ON} = |z| \cdot |z'| = rr' = 1$, donc $r' = \frac{1}{r}$.
   Conclusion : l'image N de M a pour affixe : $z' = \frac{1}{r}e^{i\theta}$. On peut la reformuler :

   $$\frac{1}{r}e^{i\theta} = \frac{1}{re^{-i\theta}} = \frac{1}{\overline{z}}.$$

   L'application φ s'écrit en complexe : $\varphi(z) = \frac{1}{\overline{z}}$.
2. Déterminer ses points fixes.
   On résout $\varphi(z) = z$:

   $$\frac{1}{\overline{z}} = z \Leftrightarrow z\overline{z} = 1 \Leftrightarrow |z| = 1.$$

   l'ensemble des points fixes de φ est dans le plan le cercle unité.
3. Déterminer l'image par φ d'un cercle passant par O.
   Soit $a > 0$. Commençons par le cercle de centre $(a, 0)$ de rayon a. On peut le paramétrer par $\{a + ae^{i\theta} \ ; \ \theta \in \mathbf{R}\}$. Il faut exclure le point O pour lequel φ n'est pas défini, ce qui revient à exclure $\theta = \pi \mod 2\pi$.

L'image d'un point du cercle est alors :

$$\begin{aligned}\varphi(a+a\mathrm{e}^{\mathrm{i}\theta}) &= \frac{1}{\overline{a+a\mathrm{e}^{\mathrm{i}\theta}}}\\ &= \frac{1}{a(1+\mathrm{e}^{-\mathrm{i}\theta})}\\ &= \frac{1}{a\mathrm{e}^{-\mathrm{i}\theta/2}(\mathrm{e}^{\mathrm{i}\theta/2}+\mathrm{e}^{-\mathrm{i}\theta/2})}\\ &= \frac{1}{a\mathrm{e}^{-\mathrm{i}\theta/2}2\cos(\theta/2)}\\ &= \frac{\mathrm{e}^{\mathrm{i}\theta/2}}{2a\cos(\theta/2)}\\ &= \frac{\cos(\theta/2)+\mathrm{i}\sin(\theta/2)}{2a\cos(\theta/2)}\\ &= \frac{1}{2a}+\mathrm{i}\frac{\sin(\theta/2)}{2a\cos(\theta/2)}\end{aligned}$$

On constate que la partie réelle est toujours égale à $\frac{1}{2a}$ indépendamment de θ. Ainsi l'image de tout point du cercle est située sur la droite verticale d'abscisse $\frac{1}{2a}$.
L'analyse de la partie réelle $\frac{\sin(\theta/2)}{2a\cos(\theta/2)} = \frac{1}{2a}\tan(\theta/2)$ permet de montrer que tous les points de cette droite sont atteints.
Conclusion : l'image du cercle est cette droite.

Considérons maintenant un cercle quelconque passant par O. On peut l'obtenir en faisant tourner notre cercle précédent autour de O. Or, faire tourner un point autour de O revient à faire tourner son image par φ de la même manière :

$$\varphi(\mathrm{e}^{\mathrm{i}\alpha}z) = \mathrm{e}^{\mathrm{i}\alpha}\varphi(z)(\quad \text{à vérifier})$$

Nous pouvons en déduire que l'image de tout cercle passant par O est une droite du plan (obtenue en faisant tourner la droite verticale précédente autour de O.

4. Déterminer l'image par φ d'une droite du plan.
   On peut remarquer que l'inversion est une involution : $\varphi \circ \varphi = \mathrm{id}$:

$$\varphi(\varphi(z)) = \varphi(1/\overline{z}) = \frac{1}{\overline{1/\overline{z}}} = z.$$

   Ainsi comme l'image de tout cercle passant par O est une droite, l'image d'une droite du plan est un cercle passant par O.
   Attention, toutes les droites ne sont pas concernées : seules les droites ne passant pas par O ont été obtenues dans la question précédente. On peut vérifier que l'image d'une droite passant par O est elle-même.

5. En déduire une condition pour que 4 points 0, A, B et C soient cocycliques.
   Nous avons montré l'équivalence suivante : $\mathcal{C}$ cercle passant par O ssi $\varphi(\mathcal{C})$ droite du plan ne passant pas par O. Nous en déduisons : 0, A, B et C sont cocycliques ssi $\varphi(A)$, $\varphi(B)$ et $\varphi(C)$ sont alignés.

L'alignement peut se caractériser facilement en complexe. Par exemple E, F et G sont alignés dans cet ordre ssi $|f-e|+|g-f|=|g-e|$. Nous en déduisons une condition : O, A, B et C cocycliques (dans cet ordre) ssi

$$\left|\frac{1}{\overline{b}}-\frac{1}{\overline{a}}\right|+\left|\frac{1}{\overline{c}}-\frac{1}{\overline{b}}\right|=\left|\frac{1}{\overline{c}}-\frac{1}{\overline{a}}\right|.$$

si et seulement si (après réécriture) :

$$|c||a-b|+|a||c-b|=|b||a-c|.$$

Autre possibilité : E, F et G sont alignés ssi $f-e$ et $g-e$ ont le même argument à π près, donc ssi $\frac{f-e}{g-e}$ est un nombre réel. Ainsi, 0, A, B et C sont cocyliques ssi

$$\frac{1/\overline{b}-1/\overline{a}}{1/\overline{c}-1/\overline{a}}=\frac{\overline{c}}{\overline{b}}\frac{\overline{a}-\overline{b}}{\overline{a}-\overline{c}}\in\mathbf{R}$$

donc ssi : $\dfrac{c}{b}\cdot\dfrac{a-b}{a-c}\in\mathbf{R}$.

Exercice **Calcul de somme**

Calculons $\sum_{i=0}^{n}\binom{n}{k}\sin(kx)$.

On remarque que c'est la partie imaginaire de $\sum_{i=0}^{n}\binom{n}{k}e^{ikx}=\sum_{i=0}^{n}\binom{n}{k}(e^{ix})^k$. On reconnaît la formule du binôme de Newton. Cette dernière somme est donc égale à $(1+e^{ix})^n$ qui est égal à $[e^{ix/2}(e^{-ix/2}+e^{ix/2})]^n=e^{inx/2}(2\cos(x/2))^n$. Donc la somme considérée est égale à la partie imaginaire de ce nombre, soit $2^n\sin(nx/2)\cos(x/2)$.

Exercice **Intégrales**

Calculons $\int_0^{\frac{\pi}{6}}\cos^2(x)\sin(x)dx$.

Pour cela, linéarisons l'expression $\cos^2(x)\sin(x)$:

$$\begin{aligned}\cos^2(x)\sin(x)&=\left(\frac{e^{ix}+e^{-ix}}{2}\right)^2\left(\frac{e^{ix}-e^{-ix}}{2i}\right)\\&=\frac{1}{8i}(e^{2ix}+e^{-2ix}+2)(e^{ix}-e^{-ix})\\&=\frac{1}{8i}(e^{3ix}+e^{-ix}+2e^{ix}-e^{ix}-e^{-3ix}-2e^{-ix})\\&=\frac{1}{4}(\sin(3x)+\sin(x))\end{aligned}$$

Ainsi

$$\int_0^{\frac{\pi}{6}}\cos^2(x)\sin(x)dx=\int_0^{\frac{\pi}{6}}\frac{1}{4}(\sin(3x)+\sin(x))dx=[-\frac{\cos(3x)}{12}-\frac{\cos(x)}{4}]_0^{\frac{\pi}{6}}=\frac{1}{3}-\frac{\sqrt{3}}{8}.$$

Pour les autres intégrales, on trouve

$$\int_0^{\pi}\cos^3(x)dx=0,\quad\int_{-\pi}^{\pi}\cos^4(x)dx=\frac{3\pi}{4},\quad\int_0^{\frac{\pi}{4}}\cos(x)\sin^5(x)dx=\frac{1}{48}.$$

Remarques : certains résultats peuvent se retrouver plus facilement. Pour tout x, $\cos^3(\pi - x) = -\cos^3(x)$. Ainsi le graphe de la fonction $\cos^3$ possède une symétrie centrale par rapport à $x = \frac{\pi}{2}$. Il est donc logique que l'intégrale soit nulle entre 0 et π.

D'autre part, l'expression $\cos^2 \sin$ est à peu près de la forme uu' et est donc facile à intégrer : c'est la dérivée de la fonction $-\cos^3$. De même, la fonction $\cos \sin^5$ est la dérivée de la fonction $\sin^6$.

Exercice **Inégalité triangulaire**

Soient z et z' dans $\mathbf{C}$. Démontrer l'inégalité triangulaire : $|z + z'| \leqslant |z| + |z'|$.

On pourra utiliser les formes polaires de z et z' et la formule $\cos(a - b) = \cos(a)\cos(b) + \sin(a)\sin(b)$.

Sous quelle condition a-t-on égalité ?

Si z ou z' est nul, le résultat est trivial. Supposons $z \neq 0$ et $z' \neq 0$. On les écrit sous forme polaire : $z = re^{i\theta}$ et $s' = r'e^{i\theta'}$ avec r, r' des réels strictement positifs et θ, θ' des réels. Alors, par définition, $|z| = r$ et $|z'| = r'$, et :

$$|z + z'| = |re^{i\theta} + r'e^{i\theta'}| = |r\cos(\theta) + r'\cos(\theta') + i(r\sin(\theta) + r'\sin(\theta'))|$$

$$= \sqrt{(r\cos(\theta) + r'\cos(\theta'))^2 + (r\sin(\theta) + r'\sin(\theta'))^2} = \sqrt{r^2 + 2rr'\cos(\theta)\cos(\theta') + r'^2 + 2rr'\sin(\theta)\sin(\theta')}.$$

(Après développement, on a reconnu des formules trigo et on a simplifié.)

Or $\cos(\theta)\cos(\theta') + \sin(\theta)\sin(\theta') = \cos(\theta - \theta') \leqslant 1$. Donc

$$|z + z'| \leqslant \sqrt{r^2 + 2rr' + r'^2} = \sqrt{(r + r')^2} = r + r'$$

car $r + r' > 0$. Ainsi, nous obtenons bien : $|z + z'| \leqslant |z| + |z'|$.

Si on reprend notre raisonnement, on comprend que si $\cos(\theta)\cos(\theta') + \sin(\theta)\sin(\theta') < 1$, notre majoration finale sera stricte. Ainsi l'inégalité sera une égalité si et seulement si $\cos(\theta)\cos(\theta') + \sin(\theta)\sin(\theta') = 1$, autrement dit si $\cos(\theta - \theta') = 1$.

C'est le cas si et seulement si $\theta - \theta' = 0$ modulo 2π, donc si $\theta = \theta'$ modulo 2π. Conclusion : $|z + z'| = |z| + |z'|$ ssi z et z' ont le même argument.

Exercice **Carré et triangle équilatéral**

Soient A et B des points d'affixes z_A et z_B. Comment calculer des affixes z_C et z_D de manière à ce que $ABCD$ soit un carré ?

De même, déterminer l'affixe d'un point E tel que ABE soit un triangle équilatéral.

Faire une figure ! Par définition d'un carré, le point C est obtenu en faisant tourner le point A d'un angle $\frac{\pi}{2}$ (ou $-\frac{\pi}{2}$) autour du point B. On peut donc utiliser la rotation de centre B d'angle $\frac{\pi}{2}$. On en déduit que $z_C = i(z_A - z_B) + z_B$.

De même D s'obtient en faisant tourner B d'un angle $-\frac{\pi}{2}$ (ou $\frac{\pi}{2}$ si on avait choisi $-\frac{\pi}{2}$ précédemment) autour de A. Ainsi $z_D = -i(z_B - z_A) + z_A$.

Vérifions avec un exemple : prenons $z_A = 1$ et $z_B = 3 + i$. On obtient avec les formules ci-dessus : $z_C = 4 - i$ et $z_D = 2 - 2i$. Les quatre points forment bien un carré.

Pour obtenir un triangle équilatéral de côté AB, il faut faire tourner B autour de A d'un angle $\frac{\pi}{3}$ (ou $-\frac{\pi}{3}$). Ainsi $z_E = e^{i\frac{\pi}{3}}(z_B - z_A) + z_A$.

Exercice **Calcul de** $\cos(2\pi/5)$

1. Soit $z = \mathrm{e}^{2\mathrm{i}\pi/5}$. Alors, en reconnaissant une somme géométrique :
$$1 + z + z^2 + z^3 + z^4 = \frac{1 - z^5}{1 - z} = 0$$
car $z^5 = \mathrm{e}^{2\mathrm{i}\pi} = 1$.
2. On remarque que $z^4 = \mathrm{e}^{8\mathrm{i}\pi/5} = \mathrm{e}^{-2\mathrm{i}\pi/5} = \bar{z}$. Donc $z + z^4 = 2\Re(z) = 2\cos(2\pi/5)$.
De même, on montre que $z^3 = \overline{z^2}$ et ainsi que $z^2 + z^3 = 2\Re(z^2) = 2\cos(4\pi/5)$.
D'après 1., on en déduit que $1 + 2\cos(2\pi/5) + 2\cos(4\pi/5) = 0$.
Enfin, d'après la formule trigonométrique $\cos(2\theta) = \cos^2(\theta) - \sin^2(\theta) = 2\cos^2(\theta) - 1$, on déduit que $\cos(4\pi/5) = 2\cos^2(2\pi/5) - 1$.
En remplaçant dans l'équation plus haut on obtient
$$4\cos^2(2\pi/5) + 2\cos(2\pi/5) - 1 = 0.$$
Donc $\cos(2\pi/5)$ est racine du polynôme $4X^2 + 2X - 1$.
3. Les racines de ce polynôme sont $\frac{-1+\sqrt{5}}{4}$ et $\frac{-1-\sqrt{5}}{4}$.
Comme $2\pi/5 \in [0, \pi/2]$, on peut affirmer que $\cos(2\pi/5)$ est positif. Donc
$$\cos(2\pi/5) = \frac{-1 + \sqrt{5}}{4}.$$
4. À l'aide d'une règle et d'un compas, on est capable de faire un grand nombre de constructions géométriques : des médiatrices, des bissectrices, des parallèles, etc. Pour notre problème, il s'agit de construire le point d'affixe $\mathrm{e}^{2\mathrm{i}\pi/5}$. On pourra facilement reporter ce point sur le cercle unité afin de construire les autres sommets d'un pentagone régulier.
On commence par se fixer une unité : on choisit deux points initiaux arbitraires et on dit que leur distance est 1.
On construit à partir de ce segment un triangle rectangle de côtés 1 et 2. Son hypoténuse a alors une longueur $\sqrt{5}$.
On peut reporter une fois notre segment unitaire pour obtenir un segment de longueur $\sqrt{5} - 1$. Puis on divise ce segment en 4 et pour obtenir un segment de longueur $\frac{-1+\sqrt{5}}{4}$.
On représente ensuite un cercle unité avec deux axes orthogonaux. On reporte notre segment de longueur $\frac{-1+\sqrt{5}}{4}$ sur un des axes. On construit la perpendiculaire au segment passant par son extrémité. Ses intersections avec le cercle unité nous donnent deux sommets de notre pentagone régulier.
Le point d'affixe 1 en fournit un autre. Il suffit alors de reporter les longueurs entre ces sommets sur le cercle pour obtenir les deux derniers sommets.

Exercice **Somme d'un cosinus et d'un sinus**

Cet exercice repose sur les écritures algébriques et polaires d'un même nombre complexe.

Posons $z = a - \mathrm{i}b$ et $z' = \mathrm{e}^{\mathrm{i}x} = \cos(x) + \mathrm{i}\sin(x)$.
Alors $zz' = a\cos(x) + b\sin(x) + \mathrm{i}(a\sin(x) - b\cos(x))$.
Nous reconnaissons l'un des deux termes qui nous intéressent :
$$\Re(zz') = a\cos(x) + b\sin(x).$$
Recalculons ce produit zz' à l'aide d'écritures polaires. Le nombre z admet une écriture polaire de la forme $z = a - \mathrm{i}b = r\mathrm{e}^{\mathrm{i}\theta}$ avec $r \in \mathbf{R}_+$ et $\theta \in \mathbf{R}$.
Alors $zz' = r\mathrm{e}^{\mathrm{i}\theta}\mathrm{e}^{\mathrm{i}x} = r\mathrm{e}^{\mathrm{i}(x+\theta)}$. Sa partie réelle est ainsi égale à
$$\Re(zz') = r\cos(x + \theta).$$

En identifiant nos deux résultats, nous avons bien démontré qu'il existe des nombres réels r et θ tels que

$$a\cos(x) + b\sin(x) = r\cos(x+\theta).$$

Remarque : notre preuve ne fournit pas de manière explicite les valeurs de r et θ ; elle se contente de justifier leur existence en invoquant l'existence d'une forme polaire pour tout nombre complexe.
Nous pouvons néanmoins être plus précis : r est le module de z. Il s'exprime donc en fonction des nombres a et b ainsi : $r = \sqrt{a^2+b^2}$.
Le nombre θ est l'argument de z. Si $a > 0$, il est égal à $\arctan(-b/a)$. Pour les autres cas, on reprend les formules du cours pour l'argument.

Exercice **Somme de carrés**

Soit n et m des nombres entiers s'écrivant comme sommes de deux carrés. On souhaite montrer que le produit nm peut également s'écrire comme la somme de deux carrés.

On a donc des entiers a, b, c et d tels que $n = a^2+b^2$ et $m = c^2+d^2$. On pourrait développer le produit $(a^2+b^2)(c^2+d^2)$ et reconnaître de nouveau une somme de deux carrés mais cela n'a rien d'évident.

Remarquons que $n = |a+\mathrm{i}b|^2$ et $m = |c+\mathrm{i}d|^2$. Notons $z = a+\mathrm{i}b$ et $z' = c+\mathrm{i}d$. Alors $nm = |z|^2|z'|^2 = |zz'|^2$ où $zz' = ac-bd+\mathrm{i}(ad+bc)$ est un nombre complexe dont les parties réelle et imaginaire sont des entiers. Ainsi nm est bien la somme de deux carrés d'entiers et plus précisément

$$nm = (ac-bd)^2 + (ad+bc)^2.$$

Un exemple : $26 = 5^2+1^2$ et $13 = 2^2+3^2$. Alors $13*26 = 338 = (5*2-1*3)^2+(5*3+1*2)^2 = 7^2+17^2$.

5 Groupes

Exercice **Manipulations dans un groupe**

— Si $xyz = e$, alors en composant par x^{-1} à gauche des deux côtés : $x^{-1}xyz = x^{-1}e$, donc $yz = x^{-1}$. Composons par x à droite des deux côtés : $yzx = x^{-1}x = e$. Nous avons bien démontré :

$$xyz = e \implies yzx = e.$$

Il n'est en revanche pas possible de déduire $xzy = e$. C'est évidemment le cas si le groupe est commutatif mais c'est faux dans le cas général. Il est facile de trouver un contre-exemple dans un groupe non commutatif, par exemple dans le groupe des permutations $\mathfrak{S}_3$ ou dans le groupe des fonctions réelles bijectives muni de la composition. Prenons par exemple les fonctions f_1, f_2 et f_3 définies par $f_1(x) = x + 1$, $f_2(x) = 2x$ et $f_3(x) = \frac{x-1}{2}$. Alors $f_1 \circ f_2 \circ f_3 = \mathrm{id}$ mais $f_1 \circ f_3 \circ f_2 : x \mapsto 2x - 12 + 1 = x + \frac{1}{2}$ n'est pas l'application identité.

— Soit G un groupe fini et soient a et b dans G. Soit $n \in \mathbf{N}^*$ tel que $(ab)^n = e$, c'est-à-dire $abab\cdots abab = e$, où ab apparaît n fois. Multiplions par a^{-1} à gauche : $baba\cdots abab = a^{-1}$. Puis multiplions par a à droite : $baba\cdots ababa = e$. Donc $(ba)^n = e$.
Avec ce raisonnement, on peut montrer que si ab est d'ordre n (c'est-à-dire que n est la plus petite puissance telle que $(ab)^n = e$, alors ba est également d'ordre n.

— Soit G un groupe dont tous les éléments sauf le neutre e sont d'ordre 2. Montrons que G est commutatif. Soient x et y dans G. On a par hypothèse $x^2 = e$ et $y^2 = e$. Mais xy est également dans G, donc $(xy)^2 = e$. Donc $xyxy = e$. Alors en multipliant à gauche par x, $x^2yxy = x$, donc $yxy = x$. Puis en multipliant à droite par y, $yxy^2 = xy$, donc $yx = xy$. On a donc montré que pour tous x et y dans G, $xy = yx$. Le groupe est donc commutatif.

Exercice **Groupes ?**

— L'ensemble $\{(x, y) \in \mathbf{R}^2 \mid x^2 = y^2\}$ muni de l'addition sur $\mathbf{R}^2$ n'est pas un groupe car l'addition n'est pas une opération interne à cet ensemble : par exemple $(1, 1)$ et $(2, -2)$ sont des éléments de cet ensemble mais leur somme $(3, -1)$ n'en est pas un car $3^2 \neq (-1)^2$.
Remarquons tout de même que les autres axiomes sont satisfaits : l'addition est associative, notre ensemble possède un élément neutre $(0, 0)$, et tout élément (x, y) de cet ensemble possède un opposé dans l'ensemble $(-x, -y)$ car si $x^2 = y^2$ on a aussi $(-x)^2 = (-y)^2$.

— L'ensemble $G = \{xe^{i\ln(x)}; x \in \mathbf{R}_+^*\}$ muni du produit sur $\mathbf{C}^*$ est un groupe. C'est donc un sous-groupe de $(\mathbf{C}^*, \times)$. Démontrons-le.
Montrons que la loi $\times$ est une loi interne à G. Prenons deux éléments de G que nous notons $xe^{i\ln(x)}$ et $ye^{i\ln(y)}$ avec x et y dans $\mathbf{R}_+^*$. Leur produit est :

$$xe^{i\ln(x)}ye^{i\ln(y)} = xye^{i(\ln(x)+\ln(y))} = xye^{i\ln(xy)}.$$

Or $xy \in \mathbf{R}_+^*$ et ce nombre complexe est donc de la forme $ze^{i\ln(z)}$ avec $z \in \mathbf{R}_+^*$. Il s'agit donc d'un élément de G et la loi $\times$ est donc interne à G : G est stable par produit.
Montrons que G possède un élément neutre. On connaît l'élément neutre de $(\mathbf{C}^*, \times)$, c'est 1. Il suffit de remarquer que $1 \in G$ car $1 = 1e^{i\ln(1)}$.
Montrons que tout élément de G admet un inverse dans G. Nous savons qui est l'inverse d'un nombre complexe pour la loi $\times$. Il s'agit de vérifier que l'inverse d'un élément de G est encore un élément de G. L'inverse d'un élément $xe^{i\ln(x)}$ de G est le nombre $\frac{1}{x}e^{-i\ln(x)}$. Il

est égal à $\frac{1}{x}e^{i\ln(\frac{1}{x})}$ qui est bien un élément de la forme $ze^{i\ln(z)}$ avec $z = \frac{1}{x}$, c'est donc bien un élément de G.

— L'ensemble des applications affines complexes $z \mapsto az + b$ $(a \neq 0)$ muni de la composition est un groupe. C'est un sous-groupe du groupe des bijections de $\mathbf{C}^*$ vers $\mathbf{C}^*$. Démontrons-le.
L'ensemble est stable par composition, *i.e.* la composée de deux applications affines est encore une application affine. Soient a, b, c, d des complexes avec $a, c \neq 0$. La composée des applications $z \mapsto az + b$ et $z \mapsto cz + d$ est l'application $z \mapsto c(az + b) + d = caz + cb + d$. Il s'agit bien d'une application affine de coefficients $ca \neq 0$ et $cb + d$.
Le neutre pour la composition des bijections est l'application identité $z \mapsto z$. C'est une application affine.
L'inverse d'une bijection est sa bijection réciproque. L'inverse de l'application affine $z \mapsto az + b$ est l'application $z \mapsto \frac{1}{a}(z - b) = \frac{1}{a}z - \frac{b}{a}$. Il s'agit encore d'une application affine.

— L'ensemble des fonctions réelles croissantes muni de l'addition des fonctions n'est pas un groupe car l'opposé d'une fonction croissante n'est en général pas une fonction croissante. Remarquons que les autres axiomes sont satisfaits : la loi + est associative et interne à notre ensemble car la somme de deux fonctions croissantes est encore une fonction croissante. L'élément neutre est la fonction nulle qui est bien une fonction croissante. Mais à part les fonctions constantes, aucune fonction croissante n'admet d'opposé dans l'ensemble des fonctions croissantes.

Exercice **Inverses dans $\mathbf{Z}/n\mathbf{Z}$**

Cherchons les inverses de $\bar{4}$ et $\bar{5}$ dans $\mathbf{Z}/7\mathbf{Z}$. On cherche dons des entiers a et b tels que $\bar{4}\bar{a} = \bar{1}$ et $\bar{5}\bar{b} = \bar{1}$. On peut simplement faire une recherche intuitive ou un tableau de congruence.
On trouve $\bar{4} \cdot \bar{2} = \bar{1}$ et $\bar{5} \cdot \bar{3} = \bar{1}$ dans $\mathbf{Z}/7\mathbf{Z}$. Donc $\bar{4}^{-1} = \bar{2}$ et $\bar{5}^{-1} = \bar{3}$.

Dans $\mathbf{Z}/11\mathbf{Z}$ on trouve $\bar{4} \cdot \bar{3} = \bar{1}$ et $\bar{5} \cdot \bar{9} = \bar{1}$, donc $\bar{4}^{-1} = \bar{3}$ et $\bar{5}^{-1} = \bar{9}$.

Dans $\mathbf{Z}/14\mathbf{Z}$ on trouve $\bar{5}\cdot\bar{3} = \bar{1}$, donc $\bar{5}^{-1} = \bar{3}$. Mais on ne trouve pas d'inverse pour $\bar{4}$. Justifions-le : s'il existait un entier a tel que $\bar{4}\bar{a} = \bar{1}$, alors on aurait un entier k tel que $4a = 1 + 12k$. On en déduirait que 1 est un nombre pair ce qui est absurde. Donc $\bar{4}$ n'est pas inversible dans $\mathbf{Z}/14\mathbf{Z}$.

Dans $\mathbf{Z}/43\mathbf{Z}$ il est plus difficile de trouver intuitivement des inverses et fastidieux de faire des tables de congruences. La méthode générale est alors l'algorithme d'Euclide et l'égalité de Bézout.
On applique l'algorithme à 4 et 43 et on obtient $4 \cdot 11 - 43 \cdot 1 = 1$. On en déduit que $\bar{4} \cdot \bar{11} = \bar{1}$, donc $\bar{4}^{-1} = \bar{11}$.
Avec 5, on obtient $-17 \cdot 5 + 2 \cdot 43 = 1$. On en déduit $\bar{5}^{-1} = -\bar{17} = \bar{26}$.

Pour déterminer l'ordre d'un élément dans, on calcule ses puissances jusqu'à ce qu'on obtienne l'élément neutre $\bar{1}$.
Dans $\mathbf{Z}/7\mathbf{Z}$: $\bar{4}^2 = \bar{2}$, $\bar{4}^3 = \bar{8} = \bar{1}$. Donc $\bar{4}$ est d'ordre 3. Le sous-groupe qu'il engendre est $<\bar{4}> = \{\bar{4}, \bar{2}, \bar{1}\}$. Le groupe dans lequel on travaille est $(\mathbf{Z}/7\mathbf{Z})^*$. Il est de cardinal 6 et 3 divise 6, donc le théorème de Lagrange est bien satisfait.
$\bar{5}^2 = \bar{4}$, $\bar{5}^3 = \bar{20} = \bar{6}$, $\bar{5}^4 = \bar{2}$, $\bar{5}^5 = \bar{3}$, $\bar{5}^6 = \bar{1}$. Donc $\bar{5}$ est d'ordre 6 et $<\bar{5}> = (\mathbf{Z}/7\mathbf{Z})^*$.

Dans $\mathbf{Z}/11\mathbf{Z}$, on trouve que $\bar{4}$ est d'ordre 5 et 5 divise bien 10, le cardinal de $(\mathbf{Z}/11\mathbf{Z})^*$. Et $\bar{5}$

est d'ordre 5 également. $<\bar{4}> = <\bar{5}> = \{\bar{4}, \bar{5}, \bar{9}, \bar{3}, \bar{1}\}$.

Dans $\mathbf{Z}/14\mathbf{Z}$, $\bar{4}$ n'a pas d'ordre et n'engendre pas de groupe, ce qui est logique puisqu'il n'est même pas inversible.

On trouve que $\bar{5}$ est d'ordre 6 et $<\bar{5}> = \{\bar{5}, \bar{11}, \bar{13}, \bar{9}, \bar{3}, \bar{1}\}$. Comme 14 n'est pas un nombre premier et $(\mathbf{Z}/14\mathbf{Z})^*$ n'est pas un groupe. Le théorème de Lagrange n'a pas lieu de s'appliquer dans ce contexte. Mais il y a bien un groupe qui se cache : l'ensemble engendré par $\bar{5}$ est l'ensemble des éléments inversibles de $\mathbf{Z}/14\mathbf{Z}$, il forme un groupe de 6 éléments pour la multiplication.

Dans $\mathbf{Z}/43\mathbf{Z}$, on trouve que $\bar{4}$ est d'ordre 7 et $<\bar{4}> = \{\bar{4}, \bar{16}, \bar{21}, \bar{41}, \bar{35}, \bar{11}, \bar{1}\}$. 7 divise bien 42. $\bar{5}$ est d'ordre 42 et $<\bar{4}> = (\mathbf{Z}/43\mathbf{Z})^*$.

Exercice $\mathbf{Q}[\sqrt{2}]$

1. Montrons que $(\mathbf{Q}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbf{R}, +)$.
   Soient $x = p + q\sqrt{2}$ et $x' = p' + q'\sqrt{2}$ deux éléments de $\mathbf{Q}[\sqrt{2}]$. Alors
   $$x + x' = (p + p') + (q + q')\sqrt{2}.$$
   Comme $p + p'$ et $q + q'$ sont des rationnels, $x + x'$ est bien un élément de $\mathbf{Q}[\sqrt{2}]$.
   $0 = 0 + 0\sqrt{2}$, donc $0 \in \mathbf{Q}[\sqrt{2}]$.
   Comme $-x = -p - q\sqrt{2}$ avec $-p$ et $-q$ dans $\mathbf{Q}$, $-x \in \mathbf{Q}[\sqrt{2}]$.
2. Montrons que $(\mathbf{Q}[\sqrt{2}]^*, +)$ est un sous-groupe de $(\mathbf{R}^*, \times)$.
   Soient $x = p + q\sqrt{2}$ et $x' = p' + q'\sqrt{2}$ deux éléments de $\mathbf{Q}[\sqrt{2}]^*$. Alors
   $$xx' = (pp' + 2qq') + (pq' + p'q)\sqrt{2}.$$
   Comme $pp' + 2qq'$ et $pq' + p'q$ sont des rationnels, xx' est bien un élément de $\mathbf{Q}[\sqrt{2}]^*$.
   $1 = 1 + 0\sqrt{2}$, donc $1 \in \mathbf{Q}[\sqrt{2}]^*$.
   Enfin
   $$\frac{1}{x} = \frac{1}{p + q\sqrt{2}} = \frac{p - q\sqrt{2}}{p^2 - 2q^2} = \frac{p}{p^2 - 2q^2} + \frac{q}{p^2 - 2q^2}\sqrt{2},$$
   donc $\frac{1}{x} \in \mathbf{Q}[\sqrt{2}]^*$.
3. L'application f est bien définie car l'écriture d'un élément de $\mathbf{Q}[\sqrt{2}]$ sous la forme $p + q\sqrt{2}$ est unique. En effet si $p + q\sqrt{2} = p' + q'\sqrt{2}$, on peut montrer que $p = p'$ et $q = q'$ (sinon on en déduirait que $\sqrt{2}$ est rationnel). Il n'y a donc pas d'ambiguïté dans la définition de f. Un élément de $Q[\sqrt{2}]$ n'ayant pas deux écritures distinctes, il ne peut pas avoir deux images distinctes par f.
4. La surjectivité de f est claire : un élément de $\mathbf{Q}[\sqrt{3}]$ s'écrit sous la forme $p+q\sqrt{3}$ et possède naturellement un antécédent par f : $p + q\sqrt{2}$.
   Pour l'injectivité : si $p+q\sqrt{2}$ et $p'+q'\sqrt{2}$ ont la même image par f, alors $p+q\sqrt{3} = p'+q'\sqrt{3}$. On peut alors en déduire que $p = p'$ et $q = q'$ (sinon on pourrait montrer que $\sqrt{3}$ est rationnel). Donc f est injective.
   Ainsi f est bijective.
5. Montrons que f est un morphisme pour l'addition :
   $$f((p+q\sqrt{2})+(p'+q'\sqrt{2})) = f((p+p')+(q+q')\sqrt{2}) = (p+p')+(q+q')\sqrt{3} = f(p+q\sqrt{2})+f(p'+q'\sqrt{2}).$$
   Il s'agit donc d'un morphisme bijectif : f est un isomorphisme.

6. $f(\sqrt{2}^2) = f(2) = 2$. Si f était un morphisme pour la multiplication, on aurait $f(\sqrt{2}^2) = f(\sqrt{2}) \times f(\sqrt{2}) = \sqrt{3} \times \sqrt{3} = 3$. Or $f(\sqrt{2}^2) = 2 \neq 3$, donc f ne peut pas être un morphisme pour la multiplication.

Exercice **Isomorphisme entre U_n et $\mathbf{Z}/n\mathbf{Z}$**

1. L'ensemble U_n est l'ensemble des racines n-èmes de l'unité dans $\mathbf{C}$. Cet ensemble est bien connu : $U_n = \{e^{\frac{2ik\pi}{n}} \ ; \ k = 0, \ldots, n-1\}$, il contient n éléments. Montrons que c'est un sous-groupe de $(\mathbf{C}^*, \times)$.
   Soient z et z' dans U_n. Alors $z^n = 1$ et $z'^n = 1$. Donc $(zz')^n = z^n z'^n = 1 \times 1 = 1$. Ainsi zz' est également un élément de U_n.
   L'élément neutre est 1. Comme $1^n = 1$, c'est aussi un élément de U_n.
   Soit $z \in U_n$. Alors $z^n = 1$. Et son inverse $\frac{1}{z}$ satisfait : $(\frac{1}{z})^n = \frac{1}{z^n} = \frac{1}{1} = 1$. Donc $\frac{1}{z} \in U_n$.
   Ainsi U_n est bien un sous-groupe de $(\mathbf{C}^*, \times)$.
2. Définissons l'application
$$\begin{array}{rccc} f: & \mathbf{Z}/n\mathbf{Z} & \to & U_n \\ & \bar{k} & \mapsto & e^{\frac{2ik\pi}{n}} \end{array}$$
   Nous allons montrer que f est isomorphisme de groupes pour l'addition modulo n et la multiplication dans U_n. Mais vérifions d'abord que f est bien défini. Il y a en effet une ambiguïté dans sa définition : $\bar{k}$ représente tous les entiers égaux à k modulo n. Il faut être sûr que l'image d'une classe de congruence ne dépend pas du représentant k choisi. Soient k et k' deux entiers tels que $\bar{k} = \bar{k'}$. Alors il existe un entier j tel que $k = k' + jn$. Ainsi $f(\bar{k}) = e^{\frac{2ik\pi}{n}} = e^{\frac{2i(k'+jn)\pi}{n}} = e^{\frac{2ik'\pi}{n} + 2\pi j} = e^{\frac{2ik'\pi}{n}} = f(\bar{k'})$. L'image par f est bien la même dans les deux cas.

   Vérifions maintenant que f est un morphisme de groupe : Soient $\bar{a}$ et $\bar{b}$ dans $\mathbf{Z}/n\mathbf{Z}$. Alors
$$f(\bar{a} + \bar{b}) = f(\overline{a+b}) = e^{\frac{2i(a+b)\pi}{n}} = e^{\frac{2ia\pi}{n}} e^{\frac{2ib\pi}{n}} = f(\bar{a}) f(\bar{b}).$$

   Montrons enfin qu'il s'agit d'une bijection. Cherchons le noyau de f : soit $\bar{k} \in \mathbf{Z}/n\mathbf{Z}$. Alors $f(\bar{k}) = 1$ ssi $e^{\frac{2ik\pi}{n}} = 1$ ssi $\frac{2ik\pi}{n} = 0 \mod 2\pi$ ssi $k = 0 \mod n$ ssi $\bar{k} = \bar{0}$. Donc $\mathrm{Ker}(f) = \{\bar{0}\}$. Le noyau est réduit à l'élément neutre, donc le morphisme f est injectif.
   Comme f est injectif est va d'un ensemble à n éléments vers un autre ensemble à n éléments, il et nécessairement surjectif. Ainsi f est une bijection. Donc f est un isomorphisme de groupe.
3. Cela signifie que toute propriété algébrique de l'un des deux groupes correspond à une propriété dans l'autre groupe. Ainsi pour déterminer les générateurs de $(U_n, \times)$, on peut commencer par chercher les générateurs de $(\mathbf{Z}/n\mathbf{Z}, +)$. On peut démontrer facilement que $\bar{a}$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$ ssi a et n sont premiers entre eux :
   Soit $a \in \mathbf{Z}$. Alors $<\bar{a}> = \mathbf{Z}/n\mathbf{Z}$ ssi $\bar{1} \in <\bar{a}>$
   ssi $\exists u \in \mathbf{Z}, \ u\bar{a} = \bar{1}$
   ssi $\exists (u, v) \in \mathbf{Z}^2, \ au = 1 + vn$
   ssi $\exists (u, v) \in \mathbf{Z}^2, \ au - vn = 1$
   ssi a et n sont premiers entre eux (en invoquant le théorème de Bézout et sa réciproque.

On en déduit que le même résultat est vrai dans U_n via l'isomorphisme : $e^{\frac{2ik\pi}{n}}$ engendre U_n ssi k et n sont premiers entre eux.

Exercice **Système RSA**

1. Soit $k \in \mathbf{Z}$ tel que $k \notin p\mathbf{Z}$. Donc $\bar{k} \in (\mathbf{Z}/p\mathbf{Z})^*$. D'après le petit théorème de Fermat (qui découle du théorème de Lagrange), $k^{p-1} = 1 \mod p$. Donc $k^{\varphi} = (k^{p-1})^{q-1} = 1^{q-1} = 1 \mod p$. De même si $k \notin q\mathbf{Z}$, $k^{\varphi} = 1 \mod q$.
2. Cela signifie que p et q divisent $k^{\varphi} - 1$. Comme p et q sont des nombres premiers distincts, ils apparaissent tous deux dans la décomposition en facteurs premiers de $k^{\varphi} - 1$. Donc $pq = n$ divise $k^{\varphi} - 1$ et donc $k^{\varphi} = 1 \mod n$.
3. On a dans $\mathbf{Z}/n\mathbf{Z}$, $m_2 = m_1^d = (m^e)^d = m^{ed}$. Or d est l'inverse de e modulo φ. Il existe donc un entier a tel que $ed = 1 + a\varphi$. Ainsi $m_2 = m^{1+a\varphi} = m \times (m^{\varphi})^a$. Or d'après la question précédente, $m^{\varphi} = 1$. Donc $m_2 = m \times 1^a = m$ modulo n.
   Notons que nous avons besoin d'une condition sur m pour appliquer le résultat de la question 2 : m ne doit pas être multiple de p ou q ; il doit donc être premier avec n. Il y a peu de chances que cela pose un problème car il y a bien plus de nombres premiers avec n que le contraire ($n - p - q$ contre $p + q$). D'autre part, m est en général une clé de cryptage et non le message lui-même. Si m est mal choisi, il suffit d'en changer.

   Enfin, si on ne connaît que m_1, n et e, il est difficile de retrouver m. Si on veut refaire le même calcul, il faut absolument trouver d. Cela est très difficile sans connaître φ. On pourrait essayer tous les nombres m et voir lequel satisfait $m^d = m_1 \mod n$ mais c'est extrêmement long. (Il s'agit en fait d'un problème d'extraction de racine d-ème dans Z/nZ. Faisons une analogie avec $\mathbf{R}$: il est très facile de calculer la puissance d'un nombre, il est bien plus difficile d'extraire une racine k-ème.)
   L'idéal est donc de connaître φ. Or, si on ne connaît pas p et q, il n'y a pas de moyen a priori de trouver φ à partir de n : $\varphi = n - p - q + 1$. Connaître φ équivaut à connaître p et q et donc à savoir factoriser n, ce qui est très difficile si n est très grand (de l'ordre de 10^{200}).
4. Avec $p = 5$, $q = 7$ et $e = 5$. Commençons par chercher d. $\varphi = (p-1)(q-1) = 24$. Remarquons que $5e = 25 = 1 \mod 24$. Ainsi $d = 5$ est l'inverse de e modulo φ.
   Soit $m = 3$. Calculons m_1 : $m^e = 3^5$. On calcule modulo $n = 35$. On trouve $3^5 = 33$. Calculons m_2 : $m^2 = m_1^d = 33^5 = (-2)^5 = -32 = 3$. On retrouve bien m !

Exercice **Groupe de cardinal premier**

Soit G un groupe dont les seuls sous-groupes sont $\{e\}$ et G. En particulier, cela implique que pour tout élément x de G différent de e, le sous-groupe engendré par x est égal à G.

Supposons G de cardinal infini. Soit $x \in G$ avec $x \neq e$. S'il existe un entier $n \geq 2$ tel que $x^n = x$, alors $x^{n-1} = e$ et on peut montrer (comme dans le cours) que le sous-groupe engendré par x est l'ensemble $\{x, x^2, x^3, \ldots, x^{n-2}, x^{n-1}\}$. Mais cela est impossible puisque ce sous-groupe serait alors différent de e et G. Donc pour tout $n \geq 2$, $x^n \neq x$.

Regardons alors le sous-groupe engendré par x^2. Ce sous-groupe ne peut pas contenir x d'après la propriété précédente. C'est donc un sous-groupe différent de G et de $\{e\}$. Cela est impossible et on peut donc en déduire que G est nécessairement fini.

Montrons maintenant que G est de cardinal n premier. Soit encore x dans G différent de e. Alors x engendre G par hypothèse et donc $G = \{x, x^2, \dots, x^{n-1}, x^n = e\}$.

Supposons par l'absurde que n s'écrive $n = pq$ avec $p > 1$ et $q > 1$. Soit $y = x^p$. Alors $y^q = x^n = e$. On en déduit que le sous-groupe engendré par y est inclus dans l'ensemble $\{y, y^2, \dots, y^q\}$ (il est en fait égal à cet ensemble). Comme $y \neq e$, on a obtenu un sous-groupe différent de $\{e\}$ et G ce qui est absurde.

On en déduit que $n = 1$ ou n est premier.

Exercice **Carrés dans $\mathbf{Z}/p\mathbf{Z}$**

1. Pour déterminer l'ensemble C des carrés de $(\mathbf{Z}/p\mathbf{Z})^2$, on calcule x^2 pour tout x dans $(\mathbf{Z}/p\mathbf{Z})^*$. Pour $p = 3$, on obtient $C = \{1\}$; pour $p = 5$, $C = \{1, 4\}$; pour $p = 7$, $C = \{1, 2, 4\}$; pour $p = 11$, $C = \{1, 3, 4, 5, 9\}$.
2. Montrons que C est un sous-groupe de $(\mathbf{Z}/p\mathbf{Z})^*$ pour la multiplication.
   $1^2 = 1$, donc l'élément neutre 1 est un carré et est dans C.
   Soient x et y dans C. Il existe alors x' et y' dans $(\mathbf{Z}/p\mathbf{Z})^*$ tels que $x'^2 = x$ et $y'^2 = y$. Alors $(x'y')^2 = x'^2y'^2 = xy$ (on a utilisé le fait que le groupe est commutatif). Donc xy est un carré. (De plus, on rappelle que dans $\mathbf{Z}/p\mathbf{Z}$ avec p premier, si x et y sont non nuls, alors xy est non nul.) Donc $xy \in (\mathbf{Z}/p\mathbf{Z})^*$ et $xy \in C$.
   Soit $x \in C$. Il existe y dans $(\mathbf{Z}/p\mathbf{Z})^*$ tel que $y^2 = x$. Alors $(y^{-1})^2 = (y^2)^{-1} = x^{-1}$. Donc x^{-1} est un carré. Donc $x^{-1} \in C$.
   Ainsi, C est bien un sous-groupe de $(\mathbf{Z}/p\mathbf{Z})^*$.
3. Montrons que f est un morphisme de groupes.
   Soient x et y dans $(\mathbf{Z}/p\mathbf{Z})^*$. Alors $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$. Donc f est bien un morphisme de groupes.
4. Soient x et y dans $(\mathbf{Z}/p\mathbf{Z})^*$ tels que $f(x) = f(y)$. Alors $x^2 = y^2$, donc $x^2 - y^2 = 0$ dans $\mathbf{Z}/p\mathbf{Z}$. Donc $(x - y)(x + y) = 0$. Or comme p est premier, l'anneau $(\mathbf{Z}/p\mathbf{Z}, +, \cdot)$ est intègre. Cela implique que $x - y = 0$ ou $x + y = 0$. Donc $x = y$ ou $x = -y$.
   Réciproquement, si $x = y$ alors $x^2 = y^2$ et $f(x) = f(y)$. Et si $x = -y$, alors $x^2 = (-y)^2 = y^2$, donc $f(x) = f(y)$. L'équivalence demandée est donc démontrée par double inclusion.
5. D'après la question précédente, tout élément de C a exactement deux antécédents dans $(\mathbf{Z}/p\mathbf{Z})^*$: en effet, si $x \in C$, il existe y tel que $y^2 = x$, et le seul autre antécédent est alors $-y$. Comme dans $(\mathbf{Z}/p\mathbf{Z})^*$, aucun élément n'est égal à son opposé (c'est faux pour $p = 2$ mais ce cas est exclus par l'énoncé), on obtient bien deux antécédents exactement.
   Tout élément de $(\mathbf{Z}/p\mathbf{Z})^*$ est l'antécédent d'un unique élément de C et chaque élément de C a deux antécédents. On en déduit que le cardinal de $(\mathbf{Z}/p\mathbf{Z})^*$ est égal au double du cardinal de C. Donc $\mathrm{Card}(C) = \frac{p-1}{2}$.

Exercice **Générateurs de $\mathfrak{S}_n$**

Montrons que le groupe $\mathfrak{S}_n$ est engendré par les transpositions τ_{1j} pour $j \in \{2, \dots, n\}$. Pour cela, montrons que toutes les transpositions sont dans le groupe H engendré par les transpositions τ_{1j}.

Soit τ_{ij} une transposition. Alors $\tau_{ij} = \tau_{1i}\tau_{1j}\tau_{1i}$. Donc τ_{ij} est un produit d'éléments du sous-groupe H, donc $\tau_{ij} \in H$.

Ainsi, H est un sous-groupe contenant toutes les transpositions. Hors les transpositions engendrent le groupe $\mathfrak{S}_n$. Le seul sous-groupe qui les contient toutes est le groupe tout entier. Donc $H = \mathfrak{S}_n$ et les transpositions τ_{1j} engendrent bien le groupe symétrique.

Matrices

Exercice **Calculs de puissances**

Soit $D = \begin{bmatrix} i & -i \\ i & i \end{bmatrix}$. Alors $D^2 = \begin{bmatrix} 0 & -2 \\ 2 & 0 \end{bmatrix}$, $D^3 = \begin{bmatrix} -2i & -2i \\ 2i & -2i \end{bmatrix}$ et $D^4 = \begin{bmatrix} -4 & 0 \\ 0 & 4 \end{bmatrix}$. On remarque que $D^4 = -4I_2$. On peut en déduire toutes les puissances de D. Par exemple $D^5 = DD^4 = -4DI_2 = -4D$ ou $D^{23} = (D^4)^5 D^3 = (-4I_2)^5 D^3 = (-4)^3 D^3$. Plus généralement, si $n = 4k$ avec $k \in \mathbf{N}$, $D^n = (D^4)^k = (-4)^k I_2$. Si $n = 4k+1$, $D^n = (-4)^k D$. Si $n = 4k+2$, $D^n = (-4)^k D^2$. Et si $n = 4k+3$, $D^n = (-4)^k D^3$.

Soit $E = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$. Montrons par récurrence sur n que $E^n = \begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ \frac{n(n+1)}{2} & n & 1 \end{bmatrix}$. Le résultat est vrai pour $n = 1$. (Remarque : il est aussi vrai pour $n = 0$: $E^0 = I_3$.)

Supposons le résultat vrai au rang n. Calculons alors E^{n+1} : $E^{n+1} = E^n E \begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ \frac{n(n+1)}{2} & n & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ n+1 & 1 & 0 \\ \frac{n(n+1)}{2} + n + 1 & 1+n & 1 \end{bmatrix}$, avec $\frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$. Le résultat est donc encore valable au rang $n+1$. cqfd.

Soit $F = EAE^{-1}$. Alors pour tout n, $F^n = (EAE^{-1})^n = EAE^{-1}EAE^{-1}EA \cdots AE^{-1}EAE^{-1} = EA^nE^{-1}$. Ainsi, si on sait calculer A^n, on en déduit l'expression de F^n.

On remarque que $CD = DC$: les matrices C et D commutent. Alors pour tout n, $(CD)^n = CDCDC \cdots CDCD = C^n D^n$.

Exercice **Matrices inversibles de taille 2**

Soit $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Soient α et β dans $\mathbf{R}$. Alors $A^2 + \alpha A + \beta I_2 = \begin{bmatrix} a^2 + bc + \alpha a + \beta & ab + bd + \alpha b \\ ca + db + \alpha c & cb + d^2 + \alpha d + \beta \end{bmatrix}$. Trouver α et β tels que cette matrice soit la matrice nulle revient à résoudre un système à 4 équations et 2 inconnues. On trouve finalement $\alpha = -(a+d)$ et $\beta = ad - bc$. Donc

$$A^2 - (a+d)A + (ad-bc)I_2 = 0.$$

Si $ad - bc \neq 0$, on peut isoler I_2 de l'équation et montrer que A est inversible : $A^2 - (a+d)A = -(ad-bc)I_2$ et donc $A \times \frac{A-(a+d)I_2}{bc-ad} = I_2$. Donc A est inversible et $A^{-1} = \frac{A-(a+d)I_2}{bc-ad} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.
Un exemple : $A = \begin{bmatrix} 3 & 2 \\ -1 & 1 \end{bmatrix}$ est inversible car $3 \times 1 - (-1) \times 2 = 5 \neq 0$ et $A^{-1} = \frac{1}{5} \begin{bmatrix} 1 & -2 \\ 1 & 3 \end{bmatrix}$.

Supposons maintenant que $ad - bc = 0$, et montrons que A est non inversible. Avec cette condition, notre égalité initiale devient $A \times (A - (a+d)I_2) = 0$. On peut en déduire que l'un des deux facteurs est non inversible. Soyons un peu plus précis : si A est non inversible, nous avons fini notre preuve. Si A est inversible, alors en multipliant par son inverse à gauche des deux côtés de l'égalité, on obtient $A - (a+d)I_2 = 0$. Or $A - (a+d)I_2 = \begin{bmatrix} -d & b \\ c & -a \end{bmatrix}$. Comme cette matrice est nulle, on déduit $a = b = c = d = 0$. Donc $A = 0$ ce qui contredit le fait que A est inversible.

Finalement, la seule conclusion possible est que A soit non inversible. On a ainsi démontré le critère d'inversibilité suivant :

$$A \text{ est inversible ssi } ad-bc \neq 0 : GL_2(\mathbf{R}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad-bc \neq 0\}.$$

(Remarque : $ad-bc$ est appelé déterminant de A. C'est un outil important que l'on sait étendre aux matrices de tailles supérieures.)

Considérons maintenant les matrices à coefficients entiers. Tout ce qu'on a démontré reste valable, mais dans $\mathbf{R}$. Si $ad-bc \neq 0$, alors la matrice est inversible dans $\mathcal{M}_2(\mathbf{R})$. Pour qu'elle soit inversible dans $\mathcal{M}_2(\mathbf{Z})$, il faut et il suffit que sa matrice inverse soit à coefficients entiers. Comme on a exprimé son inverse dans les questions précédentes, on trouve facilement le critère : A est inversible dans $\mathcal{M}_2(\mathbf{Z})$ ssi $ad-bc = \pm 1$ (autrement dit si son déterminant est inversible dans $\mathbf{Z}$.

Démontrons-le. Si $ad-bc = \pm 1$, alors A est inversible dans $\mathcal{M}_2(\mathbf{R})$ et $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Comme $ad-bc = \pm 1$, cette matrice est à coefficients entiers et A est donc inversible dans $\mathcal{M}_2(\mathbf{Z})$. Réciproquement, si A est inversible dans $\mathcal{M}_2(\mathbf{Z})$ alors son inverse $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ est à coefficients entiers. En particulier $\frac{d}{ad-bc}\frac{a}{ad-bc} - \frac{-b}{ad-bc}\frac{-c}{ad-bc}$ est une somme de produits d'entiers. Or ce nombre vaut $\frac{1}{ad-bc}$, donc $ad-bc = \pm 1$. Conclusion : $GL_2(\mathbf{R}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad-bc \pm 1\}$.

Exercice **Matrices nilpotentes**

1. Soit A une matrice nilpotente et $d \in \mathbf{N}$ le plus petit entier tel que $A^d = 0$. Nécessairement $d > 0$ car $A^0 = I_n$. Alors on peut écrire $AA^{d-1} = 0$. Par hypothèse sur d, $A^{d-1} \neq 0$. On en déduit que $A = 0$ ou A et A^{d-1} sont non inversibles. Dans les deux cas, A est non inversible.
2. Soient c et d tels que $A^c = B^d = 0$. Supposons $c \geqslant d$. Si A et B commutent, on peut écrire :

   $$(AB)^c = ABABA\cdots BAB = A^cB^c = 0 \cdot 0 = 0.$$

   Donc, si $AB = BA$, la matrice AB est également nilpotente.
   Si A et B ne commutent pas, ce raisonnement n'est pas valable et on ne peut a priori pas déduire que AB est nilpotente. On peut même trouver des contre-exemples : $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ et $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ sont des matrices nilpotentes puisque $A^2 = B^2 = 0$. Mais $AB = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ n'est pas nilpotente puisque $\forall n,\ (AB)^n = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq 0$.
3. Avec les mêmes hypothèses. Il faut utiliser le binôme de Newton (c'est possible car $AB = BA$) :

   $$(A+B)^{c+d} = \sum_{k=0}^{c+d} \binom{c+d}{k} A^k B^{c+d-k}.$$

   Lorsque $k \geqslant c$, $A^c = 0$ et lorsque $k < c$, $c+d-k > d$, donc $B^{c+d-k} = 0$. Ainsi, pour tout indice k, on a $A^kB^{c+d-k} = 0$ et donc $(A+B)^{c+d} = 0$. La matrice $A+B$ est donc nilpotente.
4. On utilise une autre formule : $(I_n - A)\sum_{k=0}^{c-1} A^k = I_n - A^c$. Or $A^c = 0$, donc

   $$(I_n - A)\sum_{k=0}^{c-1} A^k = I_n.$$

On en déduit que $I_n - A$ est inversible et son inverse est $\sum_{k=0}^{c-1} A^k$.

Soient $A = \begin{bmatrix} -1 & 0 & 1 \\ -1 & -3 & 4 \\ -1 & -3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 & -2 \\ 1 & 4 & -5 \\ 1 & 4 & -5 \end{bmatrix}$ et $C = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

5. On a $A^3 = B^3 = C^2 = 0$. Donc A, B et C sont nilpotentes. D'autre part, $AB = BA$ et on peut vérifier que AB et $A + B$ sont aussi nilpotentes. Enfin C ne commute ni avec A, ni avec B et il n'y a rien de plus à vérifier.

Exercice **Système différentiel**

Le système différentiel proposé s'écrit $X'(t) = MX(t)$ avec $M = \begin{bmatrix} 3 & -4 \\ 1 & -2 \end{bmatrix}$. Afin de résoudre le système, nous allons nous ramener à un système diagonale en diagonalisant la matrice M. Cela est possible grâce à la matrice P proposée (qui est inversible) : $M = P^{-1}DP$ ce qui équivaut à $PMP^{-1} = D$ ou encore $PM = DP$.

Comme $X'(t) = MX(t)$, on en déduit $PX'(t) = PMX(t) = DPX(t)$. Et on peut voir que $PX'(t) = (PX)'(t)$ (en utilisant simplement la linéarité de la dérivée). Donc si on note $PX(t) = \begin{pmatrix} f(t)-g(t) \\ f(t)-4g(t) \end{pmatrix} = \begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix}$, on obtient $\begin{pmatrix} \alpha'(t) \\ \beta'(t) \end{pmatrix} = D \begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix} = \begin{pmatrix} 2\alpha(t) \\ -\beta(t) \end{pmatrix}$. Le système différentiel obtenu est trivial car les deux équations sont maintenant indépendantes l'une de l'autre. Les solutions sont de la forme $\alpha(t) = \lambda e^{2t}$, $\beta(t) = \mu e^{-t}$ où λ et μ sont des constantes réelles.

Il ne reste qu'à revenir à f et g. Comme $PX(t) = \begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix}$, $X(t) = P^{-1} \begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix}$. Finalement avec $P^{-1} = \frac{1}{3} \begin{bmatrix} 4 & -1 \\ 1 & -1 \end{bmatrix}$

$$f(t) = \frac{4\lambda}{3} e^{2t} - \frac{\mu}{3} e^{-t}, \qquad g(t) = \frac{\lambda}{3} e^{2t} - \frac{\mu}{3} e^{-t}.$$

Exercice **Projection**

L'application φ s'écrit matriciellement $\varphi(X) = MX$ avec $M = \begin{bmatrix} 6 & -3 \\ 10 & -5 \end{bmatrix}$ et $X = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbf{R}^2$.

Comme $M^2 = M$ on en déduit $\varphi \circ \varphi = \varphi$. Autrement dit, $\forall (x, y) \in \mathbf{R}^2, \varphi(\varphi(x, y)) = \varphi(x, y)$: les images de φ sont des points fixes de φ.

Soit $(x, y) \in \mathbf{R}^2$. $(x, y) \in \mathrm{Ker}(\varphi)$ ssi $\varphi(x, y) = (0, 0)$. cela revient à résoudre un système et on obtient $(x, y) \in \mathrm{Ker}(\varphi)$ ssi $y = 2x$. Le noyau de φ est donc la droite d'équation $y = 2x$.

Si on note C_1 et C_2 les colonnes de M, on remarque que $C_2 = 2C_1$.

Par définition l'image de φ est l'ensemble $D_2 = \{\varphi(x, y); (x, y) \in \mathbf{R}^2\} = \{(6x - 3y, 10x - 5y); (x, y) \in \mathbf{R}^2\}$. On peut montrer facilement qu'il s'agit de l'ensemble $D_2 = \{(a, b) \mid 5a = 3b\}$ ou encore $D_2 = \{(6t, 10t); t \in \mathbf{R}\}$. On reconnaît la droite d'équation $3y = 5x$ engendrée par le vecteur $(6, 10)$.

On remarque que c'est la droite engendrée par le vecteur colonne C_1 (ou C_2 qui lui est colinéaire). On remarque aussi que les lignes de M vérifient $5L_1 = 3L_2$.

Montrons que φ définit la projection sur la droite D_2 parallèlement à la droite D_1. Remarquons d'abord que D_1 et D_2 forment un repère du plan. Ainsi (en dessinant un parallélogramme et

en utilisant la relation de Chasles) tout vecteur X du plan peut s'écrire (de manière unique) $X = X_1 + X_2$ avec $X_1 \in D_1$ et $X_2 \in D_2$. Alors, comme φ est une application linéaire

$$\varphi(X) = \varphi(X_1 + X_2) = \varphi(X_1) + \varphi(X_2).$$

Comme $X_1 \in \mathrm{Ker}(\varphi)$, $\varphi(X_1) = 0$. Et comme X_2 est dans l'image de φ, on a vu que c'était un point fixe de φ : $\varphi(X_2) = X_2$. Finalement

$$\varphi(X) = X_2.$$

Ainsi l'image d'un vecteur X est sa composante sur D_2 dans le repère formé par D_1 et D_2. Il s'agit bien, géométriquement, de la projection sur D_2 parallèlement à D_1.

Exercice **Matrices symétriques et antisymétriques**

1. Soit $A \in \mathcal{M}_n(\mathbf{R})$. Posons $B = A + {}^tA$. Alors

   $${}^tB = {}^t(A + {}^tA) = {}^tA + A = B.$$

   Ainsi B est une matrice symétrique.

2. Nous cherchons une matrice symétrique S et une matrice antisymétrique T telles que $A = S + T$. Soit on les trouve intuitivement en nous appuyant sur la question précédente, soit on effectue un travail d'analyse :
   Si de telles matrices S et T existent, alors on aurait ${}^tA = {}^tS + {}^tT = S - T$ car S est symétrique et T antisymétrique. Comme de plus $A = S+T$, on obtient un système de deux équations que l'on peut résoudre et on trouve : $S = \frac{1}{2}(A + {}^tA)$ et $T = \frac{1}{2}(A - {}^tA)$.

   Rédigeons la synthèse : soit $A \in \mathcal{M}_n(\mathbf{R})$. Posons $S = \frac{1}{2}(A + {}^tA)$ et $T = \frac{1}{2}(A - {}^tA)$. Alors, d'après la question 1, S est une matrice symétrique, et avec le même raisonnement, on vérifie que ${}^tT = -T$, donc T est une matrice antisymétrique. Enfin on vérifie bien que $S + T = A$.

3. Reprenons les matrices de la question précédente. Le travail d'analyse que nous avons fait pourrait suffire à justifier l'unicité de S et T.
   Nous pouvons aussi raisonner ainsi : supposons qu'il existe des matrices S' et T', symétrique et antisymétrique, telles que $A = S'+T'$. Alors $S+T = S'+T'$, donc $S-S' = T'-T$. Passons à la transposée en utilisant le fait que ces matrices sont symétriques ou antisymétriques : $S - S' = -T' + T$. Donc $S - S' = S' - S = -(S - S')$. Or la seule matrice égale à son opposée est la matrice nulle, donc $S - S' = 0$, donc $S = S'$. Il s'ensuit que $T = T'$. Il y a donc bien unicité du couple (S, T) associé à la matrice A.

4. Tout ce qui a été dit dans les questions précédentes reste vrai si on travaille dans un autre anneau commutatif unitaire que $\mathbf{R}$ à une condition : il faut que le facteur $\frac{1}{2}$ soit défini dans cet anneau. Plus précisément, notons $2 \times \mathbf{1}$, où $\mathbf{1}$ désigne l'élément unité de l'anneau. Pour que nos raisonnements restent valables, il faut que cet élément $2 \times \mathbf{1}$ soit inversible dans l'anneau.

   Travaillons par exemple sur $\mathbf{Z}/5\mathbf{Z}$. L'élément $\bar{2}$ y est inversible et son inverse est $\bar{3}$. Alors toute matrice A peut s'écrire $A = 3(A+{}^tA)+3(A-{}^tA)$. Par exemple, modulo 5, on obtient $\begin{bmatrix} \bar{2} & \bar{1} \\ \bar{3} & \bar{4} \end{bmatrix} = \begin{bmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{4} \end{bmatrix} + \begin{bmatrix} \bar{0} & -\bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}$.

En revanche, sur $\mathbf{Z}/2\mathbf{Z}$, $\bar{2} = \bar{0}$ n'est pas inversible et notre méthode ne s'applique pas. Il est alors possible de démontrer que certaines matrices ne peuvent pas se décomposer en une somme de matrice symétrique et antisymétrique. C'est le cas, par exemple de la matrice $\begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix}$.

Exercice **Polynôme de matrice**

Soit $A = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 2 & -1 \\ 1 & -1 & 2 \end{bmatrix}$.

1. Calculons : $A^2 - 3A + 2I_3 = 0$.
2. On en déduit $A(A - 3I_3) = -2I_3$. Donc A est une matrice inversible et sa matrice inverse est $-\frac{1}{2}(A - 3I_3) = \frac{1}{2}\begin{bmatrix} 3 & -1 & 1 \\ 1 & 1 & 1 \\ -1 & 1 & 1 \end{bmatrix}$.
3. Toujours d'après la question 1, $A^2 = 3A - 2I_3$. Donc $A^3 = AA^2 = 3A^2 - 2A$. En réutilisant la première égalité : $A^3 = 3(3A - 2I_3) - 2A = 7A - 6I_3$.
   De la même manière on obtient $A^4 = 15A - 14I_3$. On peut conjecturer que pour tout $n \geqslant 1$, $A^n = (2^n - 1)A + (2 - 2^n)I_3$. Cela se démontre par récurrence. L'initialisation a été faite et l'hérédité repose sur le calcul suivant :

$$A^{n+1} = AA^n = (2^n - 1)A^2 + (2 - 2^n)A = (2^n - 1)(3A - 2I_3) + (2 - 2^n)A$$

$$= (3 \cdot 2^n - 3 + 2 - 2^n)A + (-2^{n+1} + 2)I_2 = (2^{n+1} - 1)A + (-2^{n+1} + 2)I_2.$$

Exercice **Matrices et nombres complexes**

On note $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \ ; \ a \in \mathbf{R}, b \in \mathbf{R} \right\}$.

1. Montrons que $(G, +)$ est un groupe en montrant que c'est un sous-groupe de $(\mathcal{M}_n(\mathbf{R}), +)$:
   Soient $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$ et $A' = \begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix} \in G$ où a, b, a' et b' sont des réels. Alors $A + B = \begin{bmatrix} a + a' & b + b' \\ -b - b' & a + a' \end{bmatrix}$. Il s'agit encore d'une matrice de G, associée aux nombres réels $a + a'$ et $b + b'$.
   La matrice nulle appartient à G puisqu'elle est de la forme $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ avec $a = b = 0$.
   L'opposé de $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$ est $\begin{bmatrix} -a & -b \\ b & -a \end{bmatrix}$. C'est encore un élément de G associé aux nombres réels $-a$ et $-b$.
   Ainsi G est un sous-groupe de $(\mathcal{M}_n(\mathbf{R}), +)$, c'est donc un groupe.
2. Montrons de même que G^* est un sous-groupe de $(\mathrm{GL}_n(\mathbf{R}), \times)$.
   Remarquons tout d'abord que si une matrice $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ est non nulle, cela signifie que $(a, b) \neq (0, 0)$. Il est alors possible de montrer (avec le pivot de Gauss ou le critère du déterminant pour les matrices de taille 2) qu'elle est inversible et que son inverse est $\frac{1}{a^2+b^2}\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

Ainsi G^* est bien inclus dans $\mathrm{GL}_n(\mathbf{R})$.
Soient A et A' deux matrices de G^*. Avec les mêmes notations que dans la question 1, on obtient

$$AA' = \begin{bmatrix} aa'-bb' & ab'+a'b & -ab'-a'b & aa'-b' \end{bmatrix}.$$

Comme A et A' sont non nulles, leur produit est non nul et il s'agit encore d'un élément de G^*, associé aux nombres $aa'-bb'$ et $ab'+a'b$.
la matrice identité appartient à G^*, elle est associée aux nombres $a=1$ et $b=0$.
On a vu qu'une matrice de G^* est inversible et son inverse est encore un élément de G^*, associé aux nombres $\frac{a}{a^2+b^2}$ et $\frac{-b}{a^2+b^2}$.

3. Posons

$$\begin{array}{rccc} f: & \mathbf{C} & \to & G \\ & z=a+\mathrm{i}b & \mapsto & \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \end{array}$$

Montrons que f est un isomorphisme de corps, c'est-à-dire un morphisme à la fois pour l'addition des complexes et des matrices et pour leur multiplication, et qu'il est bijectif.
D'après les calculs effectués ci-dessus, on a facilement

$$f((a+\mathrm{i}b)+(a'+\mathrm{i}b')) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} a' & -b' \\ b' & a' \end{bmatrix} = f(a+\mathrm{i}b)+f(a'+\mathrm{i}b'),$$

$$f((a+\mathrm{i}b)\times(a'+\mathrm{i}b')) = f((aa'-bb')+\mathrm{i}(ab'+a'b)) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \times \begin{bmatrix} a' & -b' \\ b' & a' \end{bmatrix} = f(a+\mathrm{i}b)\times f(a'+\mathrm{i}b').$$

Enfin, f est clairement une bijection par définition de G.

4. Grâce à cet isomorphisme, des opérations classique en complexe se traduisent par des opérations matricielles. Par exemple, la rotation de centre O, d'angle θ est donnée par $z \mapsto \mathrm{e}^{\mathrm{i}\theta}z$, autrement dit par la multiplication par $\mathrm{e}^{\mathrm{i}\theta} = \cos(\theta)+\mathrm{i}\sin(\theta)$. Matriciellement, on obtient la même chose en considérant la matrice associée à ce nombre complexe : $f(\cos(\theta)+\mathrm{i}\sin(\theta)) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$. La rotation s'écrit ainsi $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$.

De même, l'homothétie de centre O et de rapport λ est donnée par $z \mapsto \lambda z$. Matriciellement on obtient $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$.

La symétrie par rapport à la droite passant par O, d'angle θ est donnée par $z \mapsto \mathrm{e}^{2\mathrm{i}\theta}\bar{z}$ se traduirait par $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix} \begin{bmatrix} x \\ -y \end{bmatrix}$, que l'on peut aussi écrire $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$.

Exercice **Morphisme avec matrices**

Montrons que

$$\forall z \in \mathbf{C}, \forall z' \in \mathbf{C},\ \varphi(z+z') = \varphi(z)+\varphi(z') \ \text{ et } \ \varphi(zz') = \varphi(z)\varphi(z').$$

Soient $z = x+iy$ et $z' = x'+iy'$ dans $\mathbf{C}$. Alors $\varphi(z+z') = \varphi((x+x')+i(y+y')) = \begin{bmatrix} x+x' & y+y' \\ -(y+y') & x+x' \end{bmatrix} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} + \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = \varphi(z)+\varphi(z')$.

Et $\varphi(zz') = \varphi((xx'-yy')+i(xy'+x'y)) = \begin{bmatrix} xx'-yy' & xy'+x'y \\ -(xy'+x'y) & xx'-yy' \end{bmatrix}$. Or $\varphi(z)\varphi(z') = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}\begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = \begin{bmatrix} xx'-yy' & xy'+x'y \\ -(xy'+x'y) & xx'-yy' \end{bmatrix}$. Donc $\varphi(zz') = \varphi(z)\varphi(z')$.
Donc φ est bien un morphisme d'anneau.

Cherchons le noyau de φ. Soit $z = x+iy \in \mathbf{C}$ tel que $\varphi(z) = 0$. Cela signifie que la matrice $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$ est la matrice nulle. Donc $x = 0$ et $y = 0$. Donc $z = 0$. Ainsi le noyau de φ est $\{0\}$. On en déduit que φ est un morphisme injectif.

Cherchons l'image de φ. On peut déjà remarquer que l'image de tout nombre complexe par φ est une matrice antisymétrique de $M_2(\mathbf{R})$. Réciproquement, toute matrice antisymétrique de $M_2(\mathbf{R})$ est de la forme $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$ où x et y sont des nombres réels. Cette matrice est l'image du nombre complexe $z = x+iy$. Ainsi, toute matrice antisymétrique est l'image d'un élément de $\mathbf{C}$ par φ. Finalement, l'image de φ est l'ensemble des matrices antisymétriques réelles de taille 2.

Exercice **Un groupe de matrices.**

Pour a et b dans $\mathbf{R}$, notons $M(a,b)$ la matrice de $\mathcal{M}_4(\mathbf{R})$ définie par $M(a,b) = \begin{bmatrix} 1 & a & 2a & b \\ 0 & 1 & 0 & 2a \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Notons H l'ensemble des matrices $M(a,b)$:

$$H = \{M(a,b) \mid (a,b) \in \mathbf{R}^2\}.$$

1. Montrer
$$\forall (a,b,a',b') \in \mathbf{R}^4, \quad M(a,b)M(a',b') = M(a+a', b+b').$$
Soient a, b, a' et b' des nombres réels. On calcule le produit matriciel
$$M(a,b)M(a',b') = \begin{bmatrix} 1 & a & 2a & b \\ 0 & 1 & 0 & 2a \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a' & 2a' & b' \\ 0 & 1 & 0 & 2a' \\ 0 & 0 & 1 & -a' \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & 2a+2a' & b+b' \\ 0 & 1 & 0 & 2a+2a' \\ 0 & 0 & 1 & -a-a' \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$
On obtient bien $M(a,b)M(a',b') = M(a+a', b+b')$.
2. En déduire que toute matrice $M(a,b)$ de H est inversible et donner l'expression de son inverse.
On remarque que $M(0,0) = I_4$ la matrice identité de taille 4. Dans le calcul précédent, en prenant $a' = -a$ et $b' = -b$, on obtient $M(a,b)M(-a,-b) = M(a-a', b-b')$. Donc $M(a,b)M(a',b') = I_4$. On en déduit que $M(a,b)$ est inversible et sa matrice inverse est $M(a,b)^{-1} = M(-a,-b)$.
3. Conclure que H est un sous-groupe du groupe $(\mathrm{GL}_n(\mathbf{R}), \times)$ des matrices inversibles et qu'il est commutatif.
Nous venons de montrer que toute matrice de H est inversible, donc H est bien un sous-ensemble de $(\mathrm{GL}_4(\mathbf{R})$.
Nous avons également montré à la question 1 que le produit de deux matrices de H était encore une matrice de H. Donc H est stable par multiplication.

De plus, on a vu que $I_4 = M(0,0)$, donc I_4 est une matrice de H.
Enfin, nous avons montré que l'inverse d'une matrice de H est encore une matrice de H : $M(a,b)^{-1} = M(-a,-b) \in H$. Donc H est stable par inverse.
Nous pouvons conclure que H est un sous-groupe du groupe $(\mathrm{GL}_n(\mathbf{R}), \times)$.
D'autre part, ce sous-groupe est commutatif, car d'après la question 1,

$$\forall (a,b,a',b') \in \mathbf{R}^4, \quad M(a,b)M(a',b') = M(a+a', b+b') = M(a',b')M(a,b).$$

4. Montrer également que l'application $(a,b) \mapsto M(a,b)$ est un isomorphisme entre les groupes $(\mathbf{R}^2, +)$ et $(H, \times)$.
   Notons φ cette application. Le résultat découle directement de nos calculs précédents. En effet comme pour tous (a,b) et (a',b') dans $\mathbf{R}^4$, on a $M(a+a', b+b') = M(a,b)M(a',b')$, on obtient bien que $\varphi(a+a', b+b') = \varphi(a,b) \times \varphi(a',b')$, ou autrement dit $\varphi((a,b)+(a',b')) = \varphi(a,b) \times \varphi(a',b')$. L'image d'une somme par φ est égale au produit matriciel des images et φ est bien un morphisme de groupe de $(\mathbf{R}^2, +)$ vers $(H, \times)$.
5. Soient a et b des réels et n un entier positif. Donner l'expression de $(M(a,b))^n$.
   D'après ce qui précède, $M(2a,2b) = M(a+a, b+b) = M(a,b)M(a,b) = (M(a,b))^2$. Par une récurrence immédiate, ce résultat s'étend en : $\forall n \in \mathbf{N}$, $M(na,nb) = (M(a,b))^n$. Nous pouvons ainsi conclure que

$$(M(a,b))^n = \begin{bmatrix} 1 & na & 2na & nb \\ 0 & 1 & 0 & 2na \\ 0 & 0 & 1 & -na \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

6. En déduire $(M(a,b) - I_4)^4$ en utilisant la formule du binôme.
   Comme $M(a,b)$ et I_4 sotn des matrices qui commutent, on peut appliquer la formule du binôme de Newton :

$$(M(a,b) - I_4)^4 = M(a,b)^4 - 4M(a,b)^3 + 6M(a,b)^2 - 4M(a,b) + I_4.$$

   D'après la question précédente, on déduit

$$(M(a,b) - I_4)^4 = M(4a,4b) - 4M(3a,3b) + 6M(2a,2b) - 4M(a,b) + I_4.$$

   En explicitant ces matrices et en les additionnant, on obtient

$$(M(a,b) - I_4)^4 = 0.$$

7. Retrouver le fait que $M(a,b)$ est inversible et l'expression de son inverse.
   Ainsi, $M(a,b)^4 - 4M(a,b)^3 + 6M(a,b)^2 - 4M(a,b) + I_4 = 0$. Donc $M(a,b)(M(a,b)^3 - 4M(a,b)^2 + 6M(a,b) - 4I_4) = -I_4$. Après avoir multiplié des deux côtés par -1, on conclut que $M(a,b)$ est inversible et sa matrice inverse est la matrice $M(a,b)^{-1} = -(M(a,b)^3 - 4M(a,b)^2 + 6M(a,b) - 4I_4)$, qui après calcul donne de nouveau $M(a,b)^{-1} = M(-a,-b)$.
8. Que peut-on également déduire sur $M - I_4$?
   On déduit de $(M(a,b) - I_4)^4 = 0.$ que $(M(a,b) - I_4)$ est une matrice non inversible. En effet, si elle était inversible, on pourrait multiplier des deux côtés de l'égalité par sa matrice inverse : $(M(a,b) - I_4)^{-1}(M(a,b) - I_4)^4 = (M(a,b) - I_4)^{-1}0$, donc $(M(a,b) - I_4)^3 = 0$. En

répétant l'opération, on aboutit à $(M(a,b)-I_4)=0$, ce qui est faux. Donc $(M(a,b)-I_4)$ ne peut pas être une matrice inversible.
(On peut également dire que si $(M(a,b)-I_4)$, alors $(M(a,b)-I_4)^4$ l'est également car un produit de matrices inversibles est encore inversible. Donc en particulier, $(M(a,b)-I_4)^4 \neq 0$ ce qui est contradictoire.)

Exercice Pour x dans $\mathbf{R}$, on note $M(x)=\begin{bmatrix}1 & 0 & 0\\ -x^2 & 1 & x\\ -2x & 0 & 1\end{bmatrix}$.

1. Montrer que pour tous x et y dans $\mathbf{R}$, $M(x)M(y)=M(x+y)$.
   Soient x et y dans $\mathbf{R}$. Alors
   $$M(x)M(y)=\begin{bmatrix}1 & 0 & 0\\ -x^2 & 1 & x\\ -2x & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ -y^2 & 1 & y\\ -2y & 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\ -x^2-y^2-2xy & 1 & y+x\\ -2x-2y & 0 & 1\end{bmatrix}$$
   $$=\begin{bmatrix}1 & 0 & 0\\ -(x+y)^2 & 1 & x+y\\ -2(x+y) & 0 & 1\end{bmatrix}=M(x+y).$$
2. En déduire que pour tout x, $M(x)$ est inversible et donner son inverse.
   En particulier, le résultat précédent nous donne : $M(x)M(-x)=M(x-x)=M(0)$ donc $M(x)M(-x)=I_3$. Nous en déduisons que $M(x)$ est inversible et que sa matrice inverse est : $M(x)^{-1}=M(-x)$.
3. Déduire de tout cela que l'application $x\mapsto M(x)$ définit un morphisme entre deux groupes à préciser.
   Comme $M(x+y)=M(x)\times M(y)$, l'application M transforme une somme de réels en un produit de matrices. Le groupe de départ est : $(\mathbf{R},+)$, le groupe multiplicatif dans le monde des matrices est le groupe des matrices inversibles : $(\mathrm{GL}_3(\mathbf{R}),\times)$.
   D'après la question précédente, toutes les images $M(x)$ par M sont des matrices inversibles. Le résultat de la première question nous permet de conclure que M définit un morphismes entre les deux groupes cités.
4. Déduire également l'expression de A^n pour $A=\begin{bmatrix}1 & 0 & 0\\ -4 & 1 & -2\\ 4 & 0 & 1\end{bmatrix}$ et $n\in\mathbf{N}$.
   Toujours d'après la question 1 : $M(2x)=M(x+x)=M(x)M(x)=M(x)^2$. Et de manière récursive, on démontre immédiatement que pour tout n : $M(nx)=M(x)^n$.
   La matrice A proposée est égale à $M(-2)$. Donc
   $$A^n=M(-2)^n=M(-2n)=\begin{bmatrix}1 & 0 & 0\\ -4n^2 & 1 & -2n\\ 4n & 0 & 1\end{bmatrix}.$$

Exercice **Étude d'une application matricielle.**

Soit $M=\begin{bmatrix}\frac{3}{5} & -\frac{4}{5}\\ -\frac{4}{5} & -\frac{3}{5}\end{bmatrix}$. On note matriciellement $X=\begin{bmatrix}x\\ y\end{bmatrix}$ tout vecteur (x,y) de $\mathbf{R}^2$.

On considère l'application linéaire φ définie de $\mathbf{R}^2$ dans $\mathbf{R}^2$ que l'on écrit matriciellement sous la forme

$$\begin{array}{rccc}\varphi: & \mathbf{R}^2 & \to & \mathbf{R}^2\\ & X & \mapsto & MX\end{array}$$

1. Calculer M^2. Qu'en déduit-on sur φ ?
   On trouve $M^2 = I_2$. Donc pour tout vecteur X, $\varphi \circ \varphi(X) = M(MX) = M^2X = X$. Donc $\varphi \circ \varphi = \mathrm{id}$ (l'application identité). C'est la correspondance naturelle entre le produit matriciel et la composition des applications linéaires.
2. Déterminer l'ensemble D_1 des vecteurs X de $\mathbf{R}^2$ tels que $\varphi(X) = X$.
   Déterminer les vecteurs X tels que $\varphi(X) = X$ revient à résoudre le système :
   $$\frac{3}{5}x - \frac{4}{5}y = x \quad \text{et} \quad -\frac{4}{5}x - \frac{3}{5}y = y.$$
   À l'aide du pivot de Gauss, nous trouvons que les deux égalités sont équivalentes et l'ensemble des solutions est l'ensemble des couples (x, y) tels que $y = -\frac{1}{2}x$. Nous reconnaissons l'équation d'une droite dans le plan.
3. Déterminer l'ensemble D_2 des vecteurs X de $\mathbf{R}^2$ tels que $\varphi(X) = -X$.
   De la même manière, il s'agit de résoudre le système :
   $$\frac{3}{5}x - \frac{4}{5}y = -x \quad \text{et} \quad -\frac{4}{5}x - \frac{3}{5}y = -y.$$
   Nous trouvons l'ensemble des couples (x, y) tels que : $y = 2x$. C'est encore l'équation d'une droite du plan.
4. Soit $X \in \mathbf{R}^2$. Montrer qu'il existe $X_1 \in D_1$ et $X_2 \in D_2$ tels que $X = X_1 + X_2$.
   Cette question relève un peu de l'algèbre linéaire étudiée au second semestre. Mais on peut la résoudre géométriquement. Les droites D_1 et D_2 forment un nouveau repère du plan. Tout vecteur X peut facilement se décomposer dans ce repère à l'aide de projections et de la relation de Chasles.
   Plus précisément, le vecteur X_1 est obtenu en projetant X sur D_1 parallèlement à D_2. Et X_2 s'obtient de la même manière en projetant X sur D_2 parallèlement à D_1. Avec l'origine du repère, nos point forment un parallélogramme et nous déduisons que vectoriellement : $X = X_1 + X_2$.
5. En déduire $\varphi(X)$. Décrire géométriquement l'application φ.
   L'application φ est une application linéaire : c'est notamment un morphisme pour l'addition. Ainsi :
   $$\varphi(X) = MX = M(X_1 + X_2) = MX_1 + MX_2 = X_1 - X_2,$$
   car X_1 et X_2 appartiennent à D_1 et D_2. Géométriquement, ce vecteur $X_1 - X_2$ est obtenu en prenant le symétrique de X par rapport à D_1, parallèlement à D_2. l'application φ est donc une symétrie.

Exercice **Application linéaire bijective.**

Soit $n \in \mathbf{N}^*$ et $M \in \mathcal{G}l_n(\mathbf{R})$ une matrice inversible à coefficients réels. On définit l'application φ de $\mathbf{R}^n$ vers $\mathbf{R}^n$ qui à un vecteur colonne $X \in \mathbf{R}^n$ associe $\varphi(X) = MX$.

1. Montrer que φ est un endomorphisme du groupe $(\mathbf{R}^n, +)$.
   (Correction non rédigée, nous ne donnons que les idées principales)
   $\varphi(X_1 + X_2) = M(X_1 + X_2) = MX_1 + MX_2 = \varphi(X_1) + \varphi(X_2)$.
2. Montrer que φ est injective.
   Comme M est inversible, $MX_1 = MX_2$ implique $M^{-1}MX_1 = M^{-1}MX_2$ donc $X_1 = X_2$.

3. Montrer que φ est surjective.
   Pour $Y \in \mathbf{R}^n$ dans l'ensemble d'arrivée, posons $X = M^{-1}Y$. Alors $\varphi(X) = \cdots = Y$. Donc tout élément Y admet un antécédent, φ est surjective.
4. Soit $M = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \\ 3 & 3 & 2 \end{bmatrix}$ et $Y = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$. Déterminer $X \in \mathbf{R}^3$ tel que $MX = Y$.
   Commençons par inverser M (si elle est bien inversible). Nous trouvons : $M^{-1} = \begin{bmatrix} 3 & -1 & 0 \\ -2 & 1 & 0 \\ -\frac{3}{2} & 0 & \frac{1}{2} \end{bmatrix}$.
   Alors la solution de l'équation $MX = Y$ est $X = M^{-1}Y = \begin{bmatrix} 3 \\ -2 \\ -\frac{3}{2} \end{bmatrix}$.