Étude élémentaire du groupe diédral $\mathcal{D}_n$

Pierre LOISEL

6 novembre 2021

Ce petit document sert à donner les bases de ce qu'est le groupe diédral. On étudiera sa structure, son cardinal, ses éléments et certains de ses sous-groupes. C'est un groupe extrêmement important, notamment car il provient d'une situation très naturelle (l'étude des symétries des n-gones réguliers) et qu'il possède de jolies propriétés et qu'il est très présent en mathématique et intervient naturellement dans des questions de classification. Le document est volontairement très détaillé, avec quelques passages qui ne le sont pas que j'ai jugé faciles et que vous devriez être capable de faire sans aide. Mais si ça bloque, n'hésitez pas à me contacter !

Dans la suite, on considère $n \geq 3$ (les cas $n = 1$ et $n = 2$ sont faciles, ennuyants et m'empêchent de donner des théorèmes bien généraux dans la suite) et on note $\mathcal{P}_n$ le polygone régulier à n côtés de $\mathbb{R}^2$, donc l'ensemble des $(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right))$ avec $k \in \{0, \dots, n-1\}$. En identifiant $\mathbb{R}^2$ et $\mathbb{C}$, c'est aussi l'ensemble des points $e^{\frac{2ik\pi}{n}}$ pour $k \in \{0, \dots, n-1\}$.

Définition 1 *On note $\mathcal{D}_n$ l'ensemble des isométries affines*[1] *du plan conservant $\mathcal{P}_n$, c'est-à-dire l'ensemble des isométries affines f telles que $f(\mathcal{P}_n) = \mathcal{P}_n$, ou encore*[2] *à ce que $f(\mathcal{P}_n) \subset \mathcal{P}_n$, ou encore à ce que $\mathcal{P}_n \subset f(\mathcal{P}_n)$.*

L'ensemble $\mathcal{D}_n$ est non-vide : il contient en effet la transformation identité. Étant donné qu'une isométrie affine conserve les barycentres, comme 0 est le barycentre de $\mathcal{P}_n$, on obtient que pour tout $f \in \mathcal{D}_n$ on a $f(0) = 0$ et donc $\mathcal{D}_n$ est un sous-ensemble de $\mathrm{O}(\mathbb{R}^2)$. On considérera maintenant que $\mathbb{R}^2$ est munit de sa base canonique $(e_1, e_2) = ((1,0),(0,1))$. On peut supposer, quitte à appliquer une rotation à $\mathcal{P}_n$, que le point $(1,0)$ est dans $\mathcal{P}_n$[3]. On va maintenant montrer que l'ensemble $\mathcal{D}_n$ est bien muni d'une structure de groupe.

Propriété 2 *L'ensemble $\mathcal{D}_n$ est un sous-groupe de* $\mathrm{O}(\mathbb{R}^2)$.

Démonstration : Il est clair que $Id \in \mathcal{D}_n$. Soit $f \in \mathcal{D}_n$, montrons que $f^{-1} \in \mathcal{D}_n$. Comme $\mathrm{O}(\mathbb{R}^2)$ est un groupe, on a bien que f^{-1} est une isométrie. Il suffit donc de montrer que f^{-1} laisse invariant $\mathcal{P}_n$. Soit donc $y \in \mathcal{P}_n$. Comme $f \in \mathcal{D}_n$, il existe $x \in \mathcal{P}_n$ tel que $f(x) = y$. Donc $f^{-1}(y) = x \in \mathcal{P}_n$ et ainsi $f^{-1} \in \mathcal{D}_n$. Le fait que si $f, g \in \mathcal{D}_n$ entraîne que $fg \in \mathcal{D}_n$ est laissé en exercice (c'est facile, il suffit de vérifier les mêmes choses que pour l'inverse !). □

On aimerait maintenant avoir une idée du cardinal du groupe $\mathcal{D}_n$. Pour cela, on va en exhiber certains éléments importants. Rappelons tout d'abord que si $f \in \mathrm{O}(\mathbb{R}^2)$, alors soit $\det(f) = 1$ et dans ce cas f est une rotation, soit $\det(f) = -1$ et dans ce cas f est une symétrie. Commençons par regarder les isométries directes qui sont contenues dans $\mathcal{D}_n$, c'est à dire les rotations.

Propriété 3 *Le groupe $\mathcal{D}_n$ possède exactement n rotations, qui sont exactement les rotations d'angle $\frac{2k\pi}{n}$ avec $k \in \{0, \dots, n-1\}$.*

Démonstration : Notons r_k les rotations d'angle $\frac{2k\pi}{n}$. Tout d'abord, montrons que ces rotations sont bien des éléments de $\mathcal{D}_n$. Soit $k, k' \in \{0, \dots, n-1\}$. On a

$$\begin{aligned}
\begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{2k'\pi}{n}\right) \\ \sin\left(\frac{2k'\pi}{n}\right) \end{pmatrix} &= \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right)\cos\left(\frac{2k'\pi}{n}\right) - \sin\left(\frac{2k\pi}{n}\right)\sin\left(\frac{2k'\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right)\cos\left(\frac{2k'\pi}{n}\right) + \cos\left(\frac{2k\pi}{n}\right)\sin\left(\frac{2k'\pi}{n}\right) \end{pmatrix} \\
\text{(On utilise les formules trigo usuelles.)} \quad &= \begin{pmatrix} \cos\left(\frac{2(k+k')\pi}{n}\right) \\ \sin\left(\frac{2(k+k')\pi}{n}\right) \end{pmatrix} \in \mathcal{P}_n
\end{aligned}$$

Ainsi, on a bien que pour tout $k \in \{0, \dots, n-1\}$, on a $r_k \in \mathcal{D}_n$. Soit maintenant $r \in \mathcal{D}_n$ une rotation d'angle θ. On va d'abord montrer qu'une rotation est entièrement déterminée (modulo 2π) par l'image du vecteur e_1. En effet, on a

$$r(e_1) = \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix}$$

et on peut ainsi directement déterminer la valeur de θ. Ainsi, comme on a supposé que $e_1 \in \mathcal{P}_n$ et comme $r \in \mathcal{D}_n$, on a qu'il existe un entier k tel que :

1. Si vous ne savez pas ce que ça veut dire, c'est pas grave, on va très rapidement montrer que l'on peut se limiter aux isométries vectorielles.
2. Cela vient de l'injectivité de f.
3. Précisons que l'abus point/vecteur sera souvent fait dans ce document.

$$\begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$$

On obtient ainsi directement que $\theta = \frac{2k\pi}{n}$ et donc que r est bien de la forme r_k. $\square$

On peut en réalité affiner cette propriété très simplement en un résultat très important : les isométries positives de $\mathcal{D}_n$ forment un sous-groupe abélien de $\mathcal{D}_n$!

Propriété 4 *Le sous-ensemble de $\mathcal{D}_n$ constitué des rotations est un sous-groupe de $\mathcal{D}_n$. Ce sous-groupe est isomorphes à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration : Les détails de la preuve seront laissés en exercice, c'est pas compliqué une fois que l'on a compris qu'un calcul bourrin fonctionne ! Notons H ce sous-groupe et r_k la rotation d'angle $\frac{2k\pi}{n}$. De la même façon que dans la preuve de 3, on montre que le produit de deux rotations de $\mathcal{D}_n$ reste une rotation de $\mathcal{D}_n$. En particulier, en notant r la rotation d'angle $\frac{2\pi}{n}$, on voit que $r_k = r^k$. Ainsi, le morphisme $\phi : \mathbb{Z} \to H$ définit par $\phi(k) = r^k$ est surjectif de noyau $n\mathbb{Z}$, donc H est bien isomorphe à $\mathbb{Z}/n\mathbb{Z}$. $\square$

On voudrait maintenant savoir si le groupe $\mathcal{D}_n$ possède des isométries de déterminant -1, c'est-à-dire (comme nous sommes dans le plan) des symétries. C'est le cas et on va le voir tout de suite.

Propriété 5 *Soit s la symétrie d'axe e_1. Alors $s \in \mathcal{D}_n$.*

Démonstration : Soit $k \in \{0, \dots, n-1\}$. Alors on a

$$s \cdot \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ -\sin\left(\frac{2k\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{-2k\pi}{n}\right) \\ \sin\left(\frac{-2k\pi}{n}\right) \end{pmatrix} \in \mathcal{P}_n \quad \text{(par parité et imparité de cos et sin)}$$

Ce qui nous donne directement que $s \in \mathcal{D}_n$. $\square$

L'existence d'une symétrie dans $\mathcal{D}_n$ va nous permettre d'en trouver plein d'autres, comme l'atteste la proposition suivante.

Propriété 6 *Soit $k \in \{0, \dots, n-1\}$. On note $p_k = \left(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right)\right)$. Alors $r^k s \in \mathcal{D}_n$ est une symétrie axiale d'axe $\frac{p_k + p_0}{2}$. En particulier, on a que $|\mathcal{D}_n| \geq 2n$.*

Démonstration : Toute la preuve repose sur un fait important des symétries (c'est aussi vrai en dimension supérieur) : l'ensemble des points fixes d'une symétrie est exactement son hyperplan de symétrie. Dit en dimension 2, c'est le fait que l'axe de symétrie d'une symétrie est exactement l'ensemble de ses points fixes. Ainsi, il suffit de démontrer que $r^k s$ est une symétrie et que $r^k s(p_k) = p_k$. Le premier point est direct par multiplicativité du déterminant, on a en effet

$$\det(r^k s) = \det(r^k)\det(s) = 1^k \times -1 = -1$$

Montrons maintenant le second point. On a d'une part que

$$r^k s(p_0) = r^k(p_0) = p_k$$

et d'autre part que

$$r^k s(p_k) = p_0$$

et on obtient donc que $r^k s$ fixe l'axe défini par le vecteur $\frac{p_0 + p_k}{2}$, d'où le résultat. Le deuxième point de la proposition vient du fait que ces vecteurs définissent tous des droites distinctes lorsque k parcourt $\{0, \dots, n-1\}$. Ainsi, il y a n rotations et au moins n symétries dans $\mathcal{D}_n$, donc il y a au moins $2n$ éléments dans $\mathcal{D}_n$, d'où $|\mathcal{D}_n| \geq 2n$. $\square$

Afin de montrer que le groupe $\mathcal{D}_n$ possède exactement $2n$ éléments, nous allons en exhiber un système de générateur.

Théorème 7 *Soit r la rotation d'angle $\frac{2\pi}{n}$ et s la symétrie d'axe e_1. Alors tout élément de $\mathcal{D}_n$ s'écrit de manière unique comme étant $r^k s^l$ avec $k \in \{0, \dots, n-1\}$ et $l \in \{0, 1\}$. En particulier, on a que $|\mathcal{D}_n| = 2n$ et que $< r, s >= \mathcal{D}_n$.*

Démonstration : On reprend les notations de la preuve de 6. L'idée est que, comme $n \geq 3$, les vecteurs p_0 et p_1 forment une base de $\mathbb{R}^2$ et donc tout élément de $\mathcal{D}_n$ est entièrement déterminé par son image de la base (p_0, p_1). Soit alors $f \in \mathcal{D}_n$. On sait que f préserve aussi les angles, donc il existe $k \in \mathbb{Z}$ tel que $\{f(p_0), f(p_1)\} = \{p_k, p_{k+1}\}$ [4]. Ainsi, si on décide que l'on envoie p_0 sur p_k, il y a n choix possibles d'images. De plus, on peut soit envoyer la base (p_0, p_1) sur la base (p_k, p_{k+1}) ou sur la base (p_{k+1}, p_k) suivant si f conserve ou non l'orientation. Il y a donc au plus $2n$ choix possibles, d'où $|\mathcal{D}_n| \leq 2n$. Ainsi, par 6, on conclut que $|\mathcal{D}_n| = 2n$. Le fait que tout les éléments sont de la forme $r^k s^l$ est laissé en exercice (on distingue selon si $l = 0$ ou si $l = 1$, en s'aidant de la preuve de 6). $\square$

On va pouvoir maintenant énoncer quelques propriétés du groupe diédral.

4. Attention, on ne sait pas si f préserve l'orientation ou non, d'où l'écriture ensembliste

Propriété 8 *Soit r la rotation d'angle $\frac{2\pi}{n}$ et s la symétrie d'axe e_1. Alors*

1. *r est un élément d'ordre n et s est un élément d'ordre 2.*
2. *On a $< r > \simeq \mathbb{Z}/n\mathbb{Z}$ et $< s > \simeq \mathbb{Z}/2\mathbb{Z}$.*
3. *On a $srs^{-1} = r^{-1}$.*
4. *Pour $n \geq 3$, le groupe $\mathcal{D}_n$ n'est pas commutatif.*

Démonstration : Le premier point est un calcul facile laissé en exercice. La première partie du second point est une réécriture de 4, le second point vient du fait qu'il n'existe qu'un seul groupe d'ordre 2 à isomorphisme près. Pour le troisième point, il suffit de vérifier que la base (p_0, p_1) est bien envoyée sur (p_{n-1}, p_0) [5] par l'application srs^{-1}. En effet, on rappelle qu'une isométrie est entièrement déterminée par son image sur une base. Or, on a

$$srs^{-1}(p_0) = srs(p_0) = sr(p_0) = s(p_1) = p_{-1} = p_{n-1}, \quad srs^{-1}(p_1) = srs(p_1) = sr(p_{-1}) = s(p_0) = p_0$$

D'où le résultat comme r^{-1} envoie l'image de la base (p_0, p_1) sur la base (p_{n-1}, p_0). Le quatrième point en découle donc directement : dès que $n \geq 3$, on a que $r \neq r^{-1}$. □
On va maintenant énoncer un résultat important, à savoir qu'un groupe vérifiant les relations que nous avons vu précédemment (qui vont être rappelé dans le théorème) est isomorphe au groupe $\mathcal{D}_n$.

Théorème 9 *Soit $n \geq 1$. Soit G un groupe non commutatif fini engendré par deux éléments τ et σ vérifiant*

1. *τ est d'ordre 2 et σ est d'ordre n.*
2. *On a $\tau\sigma\tau^{-1} = \sigma^{-1}$.*

Alors G est isomorphe à $\mathcal{D}_n$ et tout élément s'écrit de manière unique $\sigma^k\tau^l$ avec $k \in \{0, \ldots, n-1\}$ et $l \in \{0, 1\}$.

Démonstration : Par théorème de la flemme, c'est vrai. □

Remarque : Le choix des lettres n'est pas anodin ! On peut en effet montrer que :

1. Si $n = 2k$, le sous-groupe de $\mathfrak{S}_n$ engendré par les permutations $\sigma = (1 \ldots n)$ et $\tau = (1\ \ n-1)(2\ \ n-2)\ldots(k\ \ k+1)$ est isomorphe à $\mathcal{D}_n$.
2. Si $n = 2k+1$, le sous-groupe de $\mathfrak{S}_n$ engendré par les permutations $\sigma = (1 \ldots n)$ et $\tau = (1\ n-1)(2\ n-2)\ldots(k-1\ k)$ est isomorphe à $\mathcal{D}_n$.

On va finir par une propriété nous permettant d'écrire $\mathcal{D}_n$ comme un produit semi-direct plus simple à manier [6].

Propriété 10 *On a $\mathcal{D}_n = < r > \rtimes < s >$.*

Démonstration : On sait que le groupe $< r >$ est d'indice 2 dans $\mathcal{D}_n$, donc il est automatiquement distingué (si vous ne savez plus pourquoi c'est vrai, redémontrez-le ! Sinon, il est facile en utilisant le fait que $srs^{-1} = r^{-1}$ que $< r >$ est distingué dans $\mathcal{D}_n$). L'existence et l'unicité de l'écriture des éléments de $\mathcal{D}_n$ de 7 nous permet d'avoir que $|\mathcal{D}_n| = 2n = |< r >| \times |< s >|$. Enfin, si $f \in < r > \cap < s >$, comme il existe k, l tels que $f = r^k s^l$, comme $s \notin < r >$, on a nécessairement que $k = l = 0$ et donc $< r > \cap < s > = \{Id\}$, d'où le résultat. □

Digressons un peu et allons regarder les produits semi-directs de la forme $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ avec $\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ un morphisme de groupe. Si ρ est trivial, alors le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ est isomorphe au produit direct $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si par contre ρ n'est pas trivial, on montre facilement que $\rho(\overline{1})(\overline{m}) = -\overline{m}$ pour tout $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Ceci nous fournit un second produit semi-direct. La propriété suivante nous en dit un peu plus.

Propriété 11 *En reprenant les notations ci-dessus, si $\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est non-trivial, alors*

$$\mathcal{D}_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$$

En particulier, les deux seuls produits semi-directs de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ sont exactement $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathcal{D}_n$.

Démonstration : Laissé en exercice : il faut montrer que $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ vérifie le critère du théorème 9 afin de l'appliquer.

On va finir ce document en étudiant le centre de $\mathcal{D}_n$.

Propriété 12 *Si $n = 2m+1$, alors $Z(\mathcal{D}_n) = \{Id\}$. Si $n = 2m$, alors $Z(\mathcal{D}_n) = \{Id, r^m\}$.*

5. Au cas-où, on a que $p_n = p_0$ par définition des p_k.
6. Ou pas, mais ça vous fera des révisions au moins !

Démonstration : Supposons que $f \in Z(\mathcal{D}_n)$. Alors il existe k, l tels que $f = r^k s^l$. Soit $k' \in \{0, \ldots, n-1\}$. On a que

$$r(r^{k'}s)r^{-1} = r^{k'+1}sr^{-1} = r^{k'+1}(sr^{-1}s^{-1})s = r^{k'+1}(srs^{-1})^{-1}s = r^{k'+2}s$$

et on obtient donc que

$$r(r^{k'}s)r^{-1}(r^{k'}s)^{-1} = r^2 \neq Id \quad \text{Car } n \geq 3$$

On obtient donc nécessairement que $l = 0$. Ainsi, si $r^k \in Z(\mathcal{D}_n)$, alors r^k et s commutent et on obtient alors de la relation $sr^ks^{-1} = r^{-k}$ que $r^{2k} = Id$ et donc $2k|n$. Si n est impair, alors on a nécessairement que $k = 0$ et dans ce cas on a bien que $Z(\mathcal{D}_n) = \{id\}$. Si $n = 2m$, alors on trouve bien le fait que $Z(\mathcal{D}_n) = \{Id, r^m\}$. □

Remarque : Je n'ai pas traité le cas D_1 et D_2, mais si tu es arrivé jusqu'ici, je peux vendre la mèche : $D_1 \simeq \mathbb{Z}/2\mathbb{Z}$ et $D_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Pourquoi de tels isomorphismes ? Exercice !

A Rappels sur les isométries de $\mathbb{R}^2$

On va ici rappeler et étudier la structure des isométries du plan. On va d'abord rappeler ce qu'est une isométrie. Dans toute la suite, $(\cdot;\cdot)$ est le produit scalaire usuel $\mathbb{R}^2$. On note aussi $||\cdot||$ la norme associée (c'est la norme euclidienne). Rappelons que si $\mathcal{B}$ est une base orthonormée, si $x, y \in \mathbb{R}^2$ et que X et sont leurs matrices représentatives dans la base $\mathcal{B}$, alors on a $(x;y) = X^TY$ [7]. On va commencer par définir ce qu'est une isométrie du plan.

Définition 13 *Soit $u \in \mathrm{GL}(\mathbb{R}^2)$. On dit que u est une isométrie si u vérifie l'une des propositions équivalentes suivante :*

1. *Pour tout $x, y \in \mathbb{R}^2$, on a $(u(x); u(y)) = (x; y)$.*
2. *Pour tout $x \in \mathbb{R}^2$, on a $||u(x)|| = ||x||$.*
3. *L'image d'une base orthonormée par u est toujours une base orthonormée.*
4. *Dans une base $\mathcal{B}$ orthonormée, si on note A la matrice de u dans $\mathcal{B}$, alors A est inversible et l'on a $AA^T = A^TA = I_2$ où A^T est la transposée de la matrice A.*

On note $\mathrm{O}(\mathbb{R}^2)$ l'ensemble des isométries de $\mathbb{R}^2$. On note $\mathrm{O}_2(\mathbb{R})$ l'ensemble des matrices orthogonales de taille 2 [8], c'est à dire les matrices vérifiant la propriété 4.

Remarques : En fait, ces propriétés caractérisent aussi les isométries de $\mathbb{R}^n$. Mais vu qu'on ne travaille que dans $\mathbb{R}^2$ au dessus, on ne va pas s'embêter avec ça.

Démonstration : On va montrer l'équivalence entre toute les définitions.

<u>$1 \Rightarrow 2$:</u> On utilise le fait suivant qui est fondamental quand on fait de l'algèbre euclidienne (vrai aussi dans $\mathbb{R}^n$) :

$$\forall x \in \mathbb{R}^2, \quad ||x||^2 = (x; x)$$

Ainsi, si $x \in \mathbb{R}^2$, on a

$$||u(x)||^2 = (u(x); u(x)) = (x; x) = ||x||^2$$

<u>$2 \Rightarrow 1$:</u> En exercice, on utilise quelque chose de fondamental à savoir une formule de polarisation qui est

$$\forall x, y \in \mathbb{R}^2, \quad (x; y) = \frac{1}{2}(||x+y||^2 - ||x||^2 - ||y||^2$$

<u>$2 \Rightarrow 3$:</u> Soit $\mathcal{B} = (e_1, e_2)$ une base orthonormée. On veut montrer que $\mathcal{B}' = (u(e_1), u(e_2))$ est une base orthonormée. Tout d'abord, comme $\mathcal{B}$ est une base et que $u \in \mathrm{GL}(\mathbb{R}^2)$, on a bien que $\mathcal{B}'$ est une base. De plus, on sait que pour $i = 1$ ou $i = 2$ que $||e_i||^2 = (u(e_i), u(e_i)) = (e_i, e_i) = ||e_i||^2 = 1$. De plus, on sait que $(u(e_1); u(e_2)) = (e_1, e_2) = 0$. Donc $\mathcal{B}'$ est une base orthonormée.

<u>$3 \Rightarrow 4$:</u> Soit $\mathcal{B}$ une base orthonormée et A la matrice de u dans la base $\mathcal{B}$. Comme $u \in \mathrm{GL}(\mathbb{R}^2)$, on a bien A qui est inversible. Soient $x, y \in \mathbb{R}^2$, de matrices représentatives X, Y dans $\mathcal{B}$. On a que $(u(x); u(y)) = (AX)^TAY = X^TA^TAY = (x; y) = X^TY$. On en déduit donc que $AA^T = I_2$.

<u>$4 \Rightarrow 1$:</u> Exercice ! On utilise exactement les mêmes ingrédients que pour la preuve de $3 \Rightarrow 4$. □

On obtient ainsi rapidement des propriétés importantes des isométries vectorielles. On commence par démontrer de petites propriétés et on montre au passage que $\mathrm{O}(\mathbb{R}^2)$ est un groupe pour la composition.

7. Faites le calcul ! Si $x = (x_1, x_2)$ et $y = (y_1, y_2)$, on a bien que $(x, y) = x_1y_1 + x_2y_2$.
8. Attention, $\mathrm{O}(\mathbb{R}^2)$ est un groupe d'isométries, c'est à dire d'applications linéaires, tandis que $\mathrm{O}_2(\mathbb{R})$ est un groupe de matrice. La différence ? Quand on écrit une matrice, on fait le choix d'une base, ce qui n'est pas forcément le cas quand on écrit une application linéaire.

Propriété 14 *Soit $u \in \mathrm{O}(\mathbb{R}^2)$.*

1. *On a $\det(u) = \pm 1$.*
2. *L'ensemble $\mathrm{O}(\mathbb{R}^2)$ munit de la loi de composition est un sous-groupe de $\mathrm{GL}(\mathbb{R}^2)$.*

Démonstration :

1. Par la propriété 3 de 13, on a que dans une base orthonormée, la matrice représentative A de u vérifie $A^T A = I_2$, et donc $\det(A^T A) = 1 = \det(A^T)\det(A) = \det(A)^2 = \det(u)^2$, et donc $\det(u) = \pm 1$.
2. Exercice ! Le plus compliqué est de montrer que l'inverse d'une isométrie est bien une isométrie. Pour cela, il y a pleins de manières différentes de le faire. □

Le groupe $\mathrm{O}(\mathbb{R}^2)$ contient donc deux types d'éléments : ceux qui ont un déterminant positif et ceux qui ont un déterminant négatif. Il y a bien des éléments non-triviaux vérifiant cela dans $\mathrm{O}(\mathbb{R}^2)$: il suffit de considérer les isométries ayant comme matrices représentatives $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. (exercice : montrer que ce sont bien des matrices orthogonales). On va maintenant exhiber un sous-groupe important [9] à savoir le groupe spécial orthogonale.

Propriété 15 (Groupe spécial orthogonale) *L'ensemble des éléments $u \in \mathrm{O}(\mathbb{R}^2)$ tels que $\det(u) = 1$ forment un sous-groupe de $\mathrm{O}(\mathbb{R}^2)$ que l'on appelle le groupe spécial orthogonale et que l'on note $\mathrm{SO}(\mathbb{R}^2)$. On a aussi son penchant matriciel que l'on note $\mathrm{SO}_2(\mathbb{R})$.*

Démonstration : On veut montrer que l'ensemble des isométries de déterminant 1 forment bien un sous-groupe de $\mathrm{O}(\mathbb{R}^2)$. Il y a la manière bébé de le faire : vérifier que $\mathrm{SO}(\mathbb{R}^2)$ vérifie tout les axiomes de sous-groupe. Ça marche, mais c'est pas très sexy. L'autre manière de le faire, c'est de dire que $\mathrm{SO}(\mathbb{R}^2)$ est le noyau du morphisme $\det$ et donc on a automatiquement que c'est un sous-groupe (distingué même !) de $\mathrm{O}(\mathbb{R}^2)$. □

On va maintenant faire un truc très sympa, c'est qu'on va entièrement caractérisé les éléments de $\mathrm{SO}(\mathbb{R}^2)$, enfin plutôt ceux de $\mathrm{SO}_2(\mathbb{R})$. En effet, on va montrer que tout élément de $\mathrm{SO}_2(\mathbb{R})$ est une rotation... Mais c'est quoi déjà une rotation ?

Définition 16 *Soit $\theta \in \mathbb{R}$. On appelle rotation d'angle θ une application linéaire r_θ telle que, dans une base orthonormée, la matrice représentative de r_θ soit $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. On remarque [10] que pour tout $\theta \in \mathbb{R}$, on a $r_\theta \in \mathrm{SO}(\mathbb{R}^2)$.*

Théorème 17 (Structure de $\mathrm{SO}(\mathbb{R}^2)$) *Soit $u \in \mathrm{SO}(\mathbb{R}^2)$. Alors il existe $\theta \in \mathbb{R}$ tel que $u = r_\theta$. Autrement dit, les éléments de $\mathrm{SO}(\mathbb{R}^2)$ sont exactement les rotations. En particulier, le groupe $\mathrm{SO}(\mathbb{R}^2)$ est commutatif.*

Démonstration : Soit $u \in \mathrm{SO}(\mathbb{R}^2)$. On va raisonner de façon matricielle, fixons donc une base orthonormée $\mathcal{B}$ de $\mathbb{R}^2$ et notons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice représentative de u dans cette base. Étant donné que la matrice A est orthogonale par 13, on obtient les relations suivantes des relations $A^T A = I_2$ et $\det(A) = 1$:

$$\begin{cases} a^2 + b^2 = 1 \\ ac + bd = 0 \\ ad - bc = 1 \\ c^2 + d^2 = 1 \end{cases}$$

Montrons que (c, d) est uniquement déterminé par les valeurs de (a, b). Supposons donc que nous connaissons (a, b). Alors le système

$$\begin{cases} ac + bd = 0 \\ ad - bc = 1 \end{cases}$$

possède comme déterminant $c^2 + d^2 = 1$ et possède donc une unique solution. On vérifie de plus que le couple $(c, d) = (-b, a)$ est bien une solution du système. Il suffit donc de trouver a et b qui conviennent.

On sait que $a^2 + b^2 = 1$, donc il existe $\theta \in \mathbb{R}$ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$. On obtient ainsi que

$$A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

et donc u est bien une rotation. Le caractère abélien du groupe est laissé en exercice (pensez à vos formules de trigo !). □

On va maintenant caractériser d'une autre manière l'ensemble des isométries vectorielles du plan de déterminant 1.

Théorème 18 *Soit $s \in \mathrm{O}(\mathbb{R}^2)$ tel que $\det(s) = -1$. Alors s est diagonalisable et, dans une base de vecteurs propres, on a que la matrice représentative de s est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Autrement dit, les isométries négatives du plan sont exactement les symétries axiales.*

9. Et que j'aime de tout mon petit cœur !
10. Par "on remarque", je veux bien sûr dire "vous vérifiez".

Démonstration : De la même manière que précédemment (exercice : le refaire !), on trouve que dans une base orthonormée, s a comme matrice représentative $\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$. Le polynôme caractéristique de cette matrice est $X^2 - 1$ qui est scindé à racines simples sur $\mathbb{R}$, donc s est diagonalisable et ses valeurs propres sont 1 et -1 (exercice : pourquoi ?). Ainsi, dans une certaine base, la matrice représentative de s est bien $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $\square$

Remarques :

1. Si on regarde le polynôme caractéristique d'une rotation r_θ, on va trouver que son polynôme caractéristique est irréductible de racines $e^{\pm i\theta}$. Ainsi, à part dans deux cas, les rotations sont de bons exemples de matrices non-diagonalisables. Ce phénomène est en fait très clair visuellement : il n'y a que les rotations d'angle 0 et π qui stabilisent des droites du plan.
2. Si $\det(s) = -1$, s est une symétrie axiale. Mais quel est son axe de symétrie ? Si l'on note ε_1 un vecteur propre associé à la valeur propre 1 et ε_2 un vecteur propre associé à la valeur propre -1, on voit que $s(\varepsilon_1) = \varepsilon_1$ et que $s(\varepsilon_2) = \varepsilon_2$. Donc s est la symétrie d'axe $\mathrm{Vect}(\varepsilon_1)$. Rappelons en effet que l'axe d'une symétrie est l'ensemble des vecteurs invariant par la symétrie.