HAX501X – Groupes et anneaux 1

CM10 26/10/2023

Clément Dupont

Retour sur les exercices du cours

Exercice 51
Soit $G = \mathfrak{S}_3$ et soit $H = \langle \tau \rangle = \{\mathrm{id}, \tau\}$ où τ est la transposition $(1\ 2)$. Lister les classes à gauche des éléments de G suivant H, puis les classes à droite.

Il y a 3 classes à gauche :

- $\mathrm{id}\, H = \tau H = H = \{\mathrm{id}, (1\ 2)\}$;
- $(1\ 3)H = (1\ 2\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$;
- $(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\}$.

Il y a 3 classes à droite :

- $H\, \mathrm{id} = H\tau = H = \{\mathrm{id}, (1\ 2)\}$;
- $H(1\ 3) = H(1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\}$;
- $H(2\ 3) = H(1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$.

On remarque que ce ne sont pas les même classes : $(1\ 3)H \neq H(1\ 3)$.

Exercice 52

Réciproquement, est-ce que tout élément de $\mathfrak{S}_n$ d'ordre k est un k-cycle ?

- C'est faux en général. Par exemple, l'élément

$$(1\ 2)(3\ 4)\ \in \mathfrak{S}_4$$

est d'ordre 2 mais n'est pas une transposition.

Exercice 53

Déterminer la décomposition en produit de cycles à supports disjoints de la permutation

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

- On obtient facilement :

$$\sigma = (1\ 8\ 3\ 9)(4\ 6)(5\ 7).$$

Exercice 54
Calculer l'inverse de la permutation $(1\ 3\ 7)(2\ 9\ 4\ 5)(6\ 8) \in \mathfrak{S}_9$.

- C'est facile :

$$\sigma^{-1} = (6\ 8)^{-1}(2\ 9\ 4\ 5)^{-1}(1\ 3\ 7)^{-1} = (6\ 8)(2\ 5\ 4\ 9)(1\ 7\ 3).$$

Comme des cycles à supports disjoints commutent, on peut aussi le réécrire :

$$\sigma^{-1} = (1\ 7\ 3)(2\ 5\ 4\ 9)(6\ 8).$$

Exercice 55

Avec les notations de la proposition précédente, exprimer l'ordre de σ en fonction des longueurs des cycles γ_i.

- On a écrit

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r$$

  où les γ_i sont des cycles dont les supports sont deux à deux disjoints. On note ℓ_i la longueur de γ_i, c'est aussi son ordre dans $\mathfrak{S}_n$.
- Un point important est que les γ_i commutent deux à deux. On a donc, pour tout $k \in \mathbb{N}^*$:

$$\sigma^k = \gamma_1^k \gamma_2^k \cdots \gamma_r^k.$$

- Par l'unicité de la décomposition en produit de cycles à supports disjoints :

$$\begin{aligned} \sigma^k = \mathrm{id} &\iff \forall i \in \{1, \ldots, r\}, \gamma_i^k = \mathrm{id} \\ &\iff \forall i \in \{1, \ldots, r\}, \ell_i | k \\ &\iff (\ell_1 \vee \ell_2 \vee \cdots \vee \ell_r) | k. \end{aligned}$$

- On en déduit que

  l'ordre de σ est le PPCM des ordres des γ_i : $\ell_1 \vee \ell_2 \vee \cdots \vee \ell_r$.

Exercice 55
Quel est l'ordre maximal d'un élément du groupe symétrique $\mathfrak{S}_5$? de $\mathfrak{S}_6$? de $\mathfrak{S}_7$? de $\mathfrak{S}_8$?

On classifie les éléments de $\mathfrak{S}_5$ selon le nombre de cycles dans la décomposition en produit de cycles à support disjoints.

- L'identité, d'ordre 1.
- Un cycle de longueur $\ell \in \{2, 3, 4, 5\}$, d'ordre ℓ.
- Un produit de deux cycles γ et γ' à supports disjoints, de longueurs respectives ℓ, ℓ'. On a nécessairement $(\ell, \ell') \in \{(2, 2), (2, 3), (3, 2)\}$ car $\ell + \ell' \leqslant 5$. Dans le cas $\ell = \ell' = 2$, l'ordre est 2. Dans le cas $\ell = 2, \ell' = 3$, l'ordre est $2 \vee 3 = 6$.

Conclusion : l'ordre maximal d'un élément de $\mathfrak{S}_5$ est 6. C'est le cas par exemple de la permutation

$$\sigma = (1\ 2)(3\ 4\ 5).$$

L'ordre maximal d'un élément de $\mathfrak{S}_6$ est 6 aussi, par exemple pour

$$(1\ 2)(3\ 4\ 5) \quad \text{ou} \quad (1\ 2\ 3\ 4\ 5\ 6).$$

L'ordre maximal d'un élément de $\mathfrak{S}_7$ est 12, par exemple pour

$$(1\ 2\ 3)(4\ 5\ 6\ 7).$$

L'ordre maximal d'un élément de $\mathfrak{S}_8$ est 15, par exemple pour

$$(1\ 2\ 3)(4\ 5\ 6\ 7\ 8).$$

Exercice 56
Écrire la permutation de l'exercice 53 comme un produit de transpositions.

$$\sigma = (1\ 8\ 3\ 9)(4\ 6)(5\ 7) = (1\ 8)(8\ 3)(3\ 9)(4\ 6)(5\ 7).$$

Le groupe alterné

Exercice 57
Lister les éléments de $\mathfrak{A}_3$ et de $\mathfrak{A}_4$.

- On a :
$$\mathfrak{A}_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}.$$
On note que $\mathfrak{A}_3$ est un groupe cyclique d'ordre 3 car engendré par $(1\ 2\ 3)$.

- On a :
$$\mathfrak{A}_4 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$
$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$
C'est un groupe d'ordre 12 qui n'est pas abélien (vérifiez-le).

Contexte et notation

Soit $n \in \mathbb{N}$. On se place dans $\mathbb{R}^n$ munie de sa base canonique et de son **produit scalaire** canonique, défini pour $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ par la formule :

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

La base canonique est donc orthonormée. On a aussi la **norme euclidienne** :

$$||x|| = \sqrt{\langle x, x \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

On retrouve le produit scalaire à partir de la norme grâce à la **formule de polarisation** :

$$\langle x, y \rangle = \frac{1}{2} \left(||x + y||^2 - ||x||^2 - ||y||^2 \right).$$

Une proposition

Proposition

Soit $f \in \mathrm{Aut}(\mathbb{R}^n)$ un automorphisme linéaire de $\mathbb{R}^n$. Les assertions suivantes sont équivalentes.

(i) f *préserve la norme :*

$$\forall x \in \mathbb{R}^n,\ ||f(x)|| = ||x||.$$

(ii) f *préserve le produit scalaire :*

$$\forall x, y \in \mathbb{R}^n,\ \langle f(x), f(y)\rangle = \langle x, y\rangle.$$

(iii) f *envoie la base canonique de* $\mathbb{R}^n$ *sur une base orthonormée.*

(iv) *Si* A *désigne la matrice de* f *dans la base canonique,*

$$^{t}A\,A = I_n = A\,^{t}A.$$

Automorphismes orthogonaux

Définition

Un automorphisme linéaire $f \in \mathrm{Aut}(\mathbb{R}^n)$ *est appelé* **automorphisme orthogonal** *s'il vérifie les assertions équivalentes* (i), (ii), (iii), (iv) *de la proposition précédente. On note*

$$\mathrm{O}_n(\mathbb{R}) \subset \mathrm{Aut}(\mathbb{R}^n)$$

l'ensemble des automorphismes orthogonaux de $\mathbb{R}^n$.

- Les automorphismes orthogonaux sont parfois appelés **isométries linéaires**.

Proposition

$\mathrm{O}_n(\mathbb{R})$ *est un sous-groupe de* $\mathrm{Aut}(\mathbb{R}^n)$.

Définition

On appelle $\mathrm{O}_n(\mathbb{R})$ *le* **groupe orthogonal** *de degré* n *sur* $\mathbb{R}$.

Démonstration : $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{Aut}(\mathbb{R}^n)$.

1) Clairement, l'identité est un automorphisme orthogonal.
2) Soient f, g deux automorphismes orthogonaux. Pour tout $x \in \mathbb{R}^n$ on a :

   $$||f(g(x))|| = ||g(x)|| = ||x||$$

   où la première égalité utilise le fait que f est un automorphisme orthogonal, et la deuxième égalité utilise le fait que g est un automorphisme orthogonal. Donc $f \circ g$ est un automorphisme orthogonal.
3) Soit f un automorphisme orthogonal. Pour tout $x \in \mathbb{R}^n$ on a :

   $$||f(f^{-1}(x))|| = ||f^{-1}(x)||$$

   et donc

   $$||x|| = ||f^{-1}(x)||.$$

   On en conclut que f^{-1} est un automorphisme orthogonal.

Automorphismes orthogonaux et matrices orthogonales

- On rappelle l'isomorphisme de groupes

$$\mathrm{Aut}(\mathbb{R}^n) \simeq \mathrm{GL}_n(\mathbb{R})$$

  où l'on représente un automorphisme de $\mathbb{R}^n$ par sa matrice dans la base canonique.

- On se permet d'identifier ainsi les deux groupes $\mathrm{Aut}(\mathbb{R}^n)$ et $\mathrm{GL}_n(\mathbb{R})$, et on peut donc voir $\mathrm{O}_n(\mathbb{R})$ comme un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

- D'après la proposition ci-dessus, c'est le sous-groupe formé des matrices carrées A de taille n qui vérifient

$${}^tA\,A = I_n = A\,{}^tA.$$

- Avec ce point de vue, on parle de **matrices orthogonales**.

Proposition

Soit $f \in \mathrm{O}_n(\mathbb{R})$*. Alors* $\det(f) \in \{-1, 1\}$.

Démonstration. Soit A la matrice de f dans la base canonique. D'après une proposition vue plus tôt on a ${}^t\!A\,A = I_n$, et donc en prenant les déterminants : $\det({}^t\!A)\det(A) = 1$. Or $\det({}^t\!A) = \det(A)$ et donc $\det(A)^2 = 1$, d'où $\det(A) \in \{-1, 1\}$. $\square$

Le groupe spécial orthogonal

Définition

L'ensemble des automorphismes orthogonaux de $\mathbb{R}^n$ *dont le déterminant est égal à* 1 *est noté* $\mathrm{SO}_n(\mathbb{R})$ *est appelé le* **groupe spécial orthogonal** *de degré* n *sur* $\mathbb{R}$.

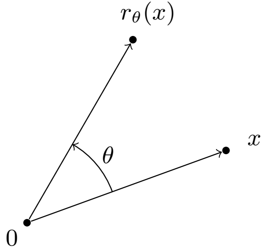
- C'est clairement un sous-groupe de $\mathrm{O}_n(\mathbb{R})$ car c'est le noyau du morphisme de groupes $\det : \mathrm{O}_n(\mathbb{R}) \to \{-1, 1\}$.

Remarque

Les éléments de $\mathrm{SO}_n(\mathbb{R})$ sont parfois appelés automorphismes orthogonaux **directs** car ils préservent l'orientation. Dit autrement, ils envoient la base canonique sur une base orthonormée directe. (En général, un automorphisme linéaire de $\mathbb{R}^n$ est dit direct si son déterminant est > 0, et indirect si son déterminant est < 0.)

Rotations

- Pour tout réel θ on a la **rotation** d'angle θ, notée $r_\theta \in \mathrm{SO}_2(\mathbb{R})$.



- Sa matrice dans la base canonique est
$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

- On a
$$r_\theta = r_{\theta'} \iff \theta - \theta' \in 2\pi\mathbb{Z}$$
et les identités évidentes :
$$r_0 = \mathrm{id} \quad , \quad r_\theta r_{\theta'} = r_{\theta+\theta'} \quad , \quad r_\theta^{-1} = r_{-\theta}.$$

Structure de $\mathrm{SO}_2(\mathbb{R})$

Proposition

Soit $f \in \mathrm{SO}_2(\mathbb{R})$. Alors f est une rotation, c'est-à-dire qu'il existe $\theta \in \mathbb{R}$, unique modulo $2\pi\mathbb{Z}$, tel que $f = r_\theta$.

Remarque

On déduit de cette proposition que $\mathrm{SO}_2(\mathbb{R})$ est un groupe abélien, qui est isomorphe au groupe $\mathbb{U}$ (cercle unité dans $\mathbb{C}^*$), l'isomorphisme identifiant la rotation r_θ à $e^{i\theta}$.

Démonstration

- Soit
$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$
la matrice de f dans la base canonique.
- Les égalités ${}^{t}A\,A = I_2$ et $\det(A) = 1$ se traduisent par les égalités
$$a^2 + b^2 = c^2 + d^2 = 1 \quad , \quad ac + bd = 0 \quad , \quad ad - bc = 1.$$
- Comme $a^2 + b^2 = c^2 + d^2 = 1$, il existe $\theta, \theta' \in \mathbb{R}$ tels que
$$(a, b) = (\cos(\theta), \sin(\theta)) \quad \text{et} \quad (c, d) = (\cos(\theta'), \sin(\theta')).$$
Les identités $ac + bd = 0$ et $ad - bc = 1$ s'écrivent, en utilisant des formules de trigonométrie bien connues :
$$\cos(\theta' - \theta) = 0 \quad \text{et} \quad \sin(\theta' - \theta) = 1.$$
Donc il existe $k \in \mathbb{Z}$ tel que $\theta' - \theta = \frac{\pi}{2} + 2\pi k$, et donc $\theta' = \theta + \frac{\pi}{2} + 2\pi k$. On a donc $(c, d) = (\cos(\theta + \frac{\pi}{2}), \sin(\theta + \frac{\pi}{2})) = (-\sin(\theta), \cos(\theta))$, et donc $f = r_\theta$.

Sous-groupes finis de $\mathrm{SO}_2(\mathbb{R})$

Pour tout entier $n \in \mathbb{N}^*$ on note C_n le sous-groupe de $\mathrm{SO}_2(\mathbb{R})$ engendré par la rotation d'angle $2\pi/n$:

$$C_n = \langle\, r_{2\pi/n} \,\rangle \subset \mathrm{SO}_2(\mathbb{R}).$$

Comme $r_{2\pi/n}$ est d'ordre n, C_n est un groupe cyclique d'ordre n.

Proposition

Les C_n, pour $n \in \mathbb{N}^*$, sont les seuls sous-groupes finis de $\mathrm{SO}_2(\mathbb{R})$.

Démonstration

- Commençons par remarquer qu'un élément r_θ est d'ordre fini dans $\mathrm{SO}_2(\mathbb{R})$ si et seulement s'il existe $N \in \mathbb{N}^*$ tel que $r_\theta^N = \mathrm{id}$, c'est-à-dire $r_{N\theta} = \mathrm{id}$, ou encore $N\theta \in 2\pi\mathbb{Z}$. Donc les éléments d'ordre fini dans $\mathrm{SO}_2(\mathbb{R})$ sont les rotations r_θ avec $\theta \in 2\pi\mathbb{Q}$.

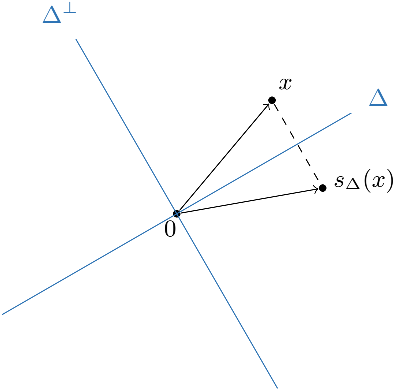
- Soit maintenant G un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. Tous les éléments de G sont nécessairement d'ordre fini, et il existe donc un entier $N \in \mathbb{N}^*$ tel que les éléments de G soient tous de la forme $r_{2\pi k/N}$ avec $k \in \mathbb{Z}$. Donc G est un sous-groupe du groupe cyclique C_N. Par la classification des sous-groupes d'un groupe cyclique, G est donc un groupe cyclique C_n pour n un diviseur de N.

Réflexions

- Notons $O_2^-(\mathbb{R}) \subset O_2(\mathbb{R})$ l'ensemble des automorphismes orthogonaux de $\mathbb{R}^2$ dont le déterminant est -1. (Ce n'est pas un sous-groupe de $O_2(\mathbb{R})$.) On a donc une partition

$$O_2(\mathbb{R}) = SO_2(\mathbb{R}) \sqcup O_2^-(\mathbb{R}).$$

- Pour toute droite (linéaire) Δ de $\mathbb{R}^2$ on a la **réflexion** par rapport à Δ, notée $s_\Delta \in O_2^-(\mathbb{R})$.



Matrices de réflexion

- La définition formelle de s_Δ est la suivante. Notons $\Delta^\perp$ la droite orthogonale à Δ, de sorte qu'on a la décomposition en somme directe orthogonale :
$$\mathbb{R}^2 = \Delta \oplus \Delta^\perp.$$
On définit s_Δ comme l'unique automorphisme linéaire de $\mathbb{R}^2$ qui agit comme id sur Δ et $-\mathrm{id}$ sur $\Delta^\perp$. Dit autrement, si e est un vecteur non nul de Δ et f un vecteur non nul de $\Delta^\perp$, la matrice de s_Δ dans la base (e, f) est :
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$
Cela permet notamment de se convaincre que $\det(s_\Delta) = -1$.
- En général, si l'on note θ l'angle orienté entre l'axe des abscisses et Δ, la matrice de s_Δ dans la base canonique est
$$\begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}.$$
- On note que s_Δ est d'ordre 2 : $s_\Delta \neq \mathrm{id}$ et $s_\Delta^2 = \mathrm{id}$.

Classification des éléments de $\mathrm{O}_2^-(\mathbb{R})$

Proposition

Soit $f \in \mathrm{O}_2^-(\mathbb{R})$. *Alors il existe une unique droite* Δ *telle que* $f = s_\Delta$.

Classification des éléments de $\mathrm{O}_2(\mathbb{R})$

Théorème

Soit $f \in \mathrm{O}_2(\mathbb{R})$. Alors f est soit une rotation r_θ, pour un $\theta \in \mathbb{R}$ unique modulo $2\pi\mathbb{Z}$, soit une réflexion s_Δ, pour une unique droite Δ.

Comment multiplier rotations et réflexions

Proposition

1) *Soient Δ, Δ' deux droites de $\mathbb{R}^2$ et soit θ l'angle orienté entre Δ et Δ'. Alors on a :*

$$s_\Delta s_{\Delta'} = r_{-2\theta}.$$

2) *Soit Δ une droite et $\theta \in \mathbb{R}$. Alors on a :*

$$r_\theta s_\Delta = s_{r_{\theta/2}(\Delta)} \quad \textit{et} \quad s_\Delta r_\theta = s_{r_{-\theta/2}(\Delta)}.$$

Notamment, on a :

$$r_\theta s_\Delta = s_\Delta r_{-\theta}.$$

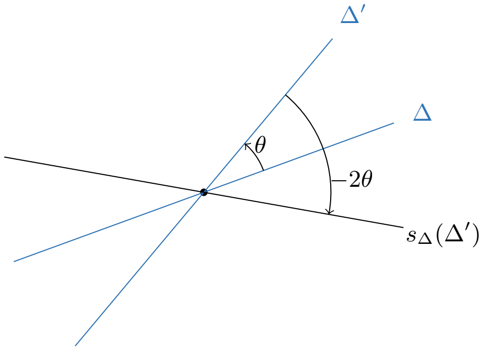
- Il découle de cette proposition que $\mathrm{O}_2(\mathbb{R})$ n'est pas un groupe abélien.

Démonstration

1) On a $\det(s_\Delta s_{\Delta'}) = \det(s_\Delta)\det(s_{\Delta'}) = (-1)\times(-1) = 1$ et donc $s_\Delta s_{\Delta'} \in \mathrm{SO}_2(\mathbb{R})$. Par une proposition vue plus haut on a donc $s_\Delta s_{\Delta'} = r_\varphi$ pour $\varphi \in \mathbb{R}$. Pour calculer φ il suffit de calculer l'angle orienté de D à $(s_\Delta s_{\Delta'})(D)$ pour n'importe quelle droite D de $\mathbb{R}^2$. On choisit de prendre $D = \Delta'$ car $s_{\Delta'}(\Delta') = \Delta'$. On a :

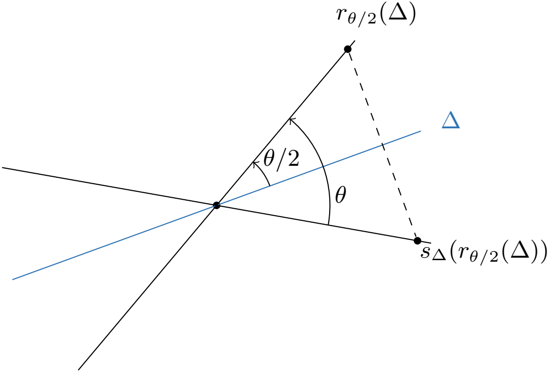
$$(s_\Delta s_{\Delta'})(\Delta') = s_\Delta(s_{\Delta'}(\Delta')) = s_\Delta(\Delta').$$

Or l'angle orienté de Δ' à $s_\Delta(\Delta')$ est -2θ (voir la figure suivante), et donc $\varphi = -2\theta$.



Démonstration

2) On a $\det(r_\theta s_\Delta) = \det(r_\theta)\det(s_\Delta) = 1 \times (-1) = -1$ et donc $r_\theta s_\Delta \in \mathrm{O}_2^-(\mathbb{R})$. Par une proposition vue plus haut, on a donc $r_\theta s_\Delta = s_{\Delta'}$ pour une droite Δ'. Cette droite Δ' est l'ensemble des points fixes de $s_{\Delta'}$, et il suffit donc de trouver une droite qui est fixée par $r_\theta s_\Delta$. On voit facilement que la droite $r_{\theta/2}(\Delta)$ est fixée par $r_\theta s_\Delta$ (voir la figure suivante), et donc $\Delta' = r_{\theta/2}(\Delta)$. La deuxième identité se montre de la même manière.



Et deux remarques pour finir

Remarque

On peut garder en tête les identités de conjugaison suivantes, conséquences de la proposition précédente : pour une rotation r et une réflexion s_Δ on a

$$s_\Delta \, r \, s_\Delta^{-1} = r^{-1}.$$

et

$$r \, s_\Delta \, r^{-1} = s_{r(\Delta)}.$$

Remarque

Si l'on choisit une droite Δ_0 de $\mathbb{R}^2$ et qu'on note $s = s_{\Delta_0}$, alors on peut représenter toutes les réflexions sous la forme $r_\theta s$ avec θ unique modulo $2\pi\mathbb{Z}$.

Polygones réguliers

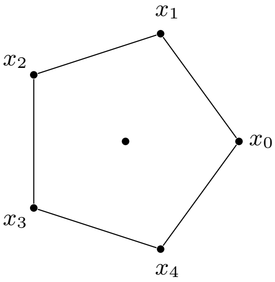
Soit un entier $n \in \mathbb{N}^*$. On note $P_n \subset \mathbb{R}^2$ l'ensemble formé des n points

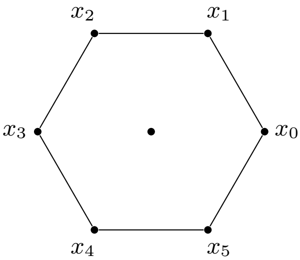
$$x_k = (\cos(2\pi k/n), \sin(2\pi k/n))$$

pour $k \in \{0, \ldots, n-1\}$. Ce sont les sommets d'un polygone régulier à n côtés.

Exemple

Voici P_5 et P_6.





Définition du groupe diédral

Définition

Le **groupe diédral** D_n *est l'ensemble des* $f \in \mathrm{O}_2(\mathbb{R})$ *qui stabilisent* P_n*, c'est-à-dire tels que* $f(P_n) \subset P_n$*.*

Proposition

D_n *est un sous-groupe de* $\mathrm{O}_2(\mathbb{R})$*.*

Démonstration.

1) Clairement, $\mathrm{id} \in D_n$.
2) Soient $f, g \in D_n$. Alors $f(P_n) \subset P_n$ et $g(P_n) \subset P_n$ et donc $(fg)(P_n) = f(g(P_n)) \subset f(P_n) \subset P_n$, donc $fg \in D_n$.
3) Soit $f \in D_n$. Alors $f(P_n) \subset P_n$. Comme f est bijective, on a pour des raisons de cardinal $f(P_n) = P_n$ et donc $f^{-1}(f(P_n)) = f^{-1}(P_n)$, d'où $P_n = f^{-1}(P_n)$, et donc $f^{-1} \in D_n$.

□

Rotations et réflexions

- Notons r la rotation d'angle $2\pi/n$. C'est clairement un élément de D_n, qui engendre le sous-groupe cyclique à n éléments $C_n = \langle r \rangle \subset D_n$.
- Pour $k \in \{0, \ldots, n-1\}$, notons aussi Δ_k la droite qui fait un angle de $\pi k/n$ avec l'axe des abscisses, et s_k la réflexion par rapport à Δ_k. Ce sont aussi des éléments de D_n.

Exemple

Voici, dans les cas $n = 5$ et $n = 6$, les n droites Δ_k.