# Géométrie (1er Semestre)

Philippe Michel January 13, 2019

# Table des matieres


Chapitre 1. Motivation: les pavages du plan 5

Chapitre 2. Groupes 9
1. Applications entre ensembles 9
2. Groupes 12
3. Morphismes de groupes 18
4. Le Theoreme de Lagrange 25
5. Groupe engendre par un ensemble 27

Chapitre 3. Isometries du plan 35
1. Plan vectoriel, affine, longueur et distance euclidienne 35
2. La structure du groupe des isometries 42
3. Classification des isometries lineaires 56
4. Conclusion 68

Chapitre 4. Isometries et nombres complexes 71
1. Construction des nombres complexes 71
2. Interpretation des isometries en termes de nombres complexes 73

Chapitre 5. Groupes finis d'isometries 81
1. Existence de groupes finis d'isometries 81
2. Groupes dihedraux 82
3. Classification des sous-groupes finis d'isometries 84

Chapitre 6. Polygones reguliers 91
1. Polygones generalises et poygones reguliers 91
2. Existence des polygones (generalises) reguliers 94
3. Polygones constructibles a la regle et au compas 97

Chapitre 7. Action d'un groupe sur un ensemble 103
1. Action a gauche, a droite 103
2. Noyau, Image d'une action 107
3. Points fixes et Stabilisateurs 108
4. Orbites 109
5. Espace quotient et quotient de groupes 112
6. La formule des points fixes (de Burnside) 115
7. Groupe quotient 118
8. Complement: Produit semi-direct 122

CHAPITRE 1

# Motivation: les pavages du plan

Un pavage du plan est un recouvrement complet du plan par un ensemble de "tuiles" qui ne se touchent que le long de leurs bord. Ces tuiles ont des dimension finies, il y en a donc un infinité mais on demande qu'il n'y ai qu'un nombre fini de formes de tuiles: deux tuiles sont de la meme forme signifies elles sont obtenues l'une par rapport a l'autre par une isométries: translation, rotation, symétrie axiale ou des composees de ces dernieres.

Le nombre de possibilités est infini; on va se restreindre au cas ou on ne dispose que d'une seule forme de tuile : on dispose donc d'une tuile $\mathbf{T} \subset \mathbb{R}^2$ et d'un ensemble d'isometries du plan (indexe par un ensemble necessairement infini $I$)

$$G = \{g \in G\} \subset \mathrm{Isom}(\mathbb{R}^2)$$

qui fournissent un ensemble de tuiles isometriques a la premiere

$$\{g(\mathbf{T}),\ g \in G\}$$

telles que cet ensemble de tuiles recouvre le plan

$$\mathbb{R}^2 = \bigcup_{g \in G} g(\mathbf{T}),$$

et tel que deux tuiles distincte ne peuvent s'intersecter que le long de leur bord

$$\text{si } g(\mathbf{T}) \neq g'(\mathbf{T}) \text{ alors } g(\mathbf{T}) \cap g'(\mathbf{T}) = \partial g(\mathbf{T}) \cap \partial g'(\mathbf{T})$$

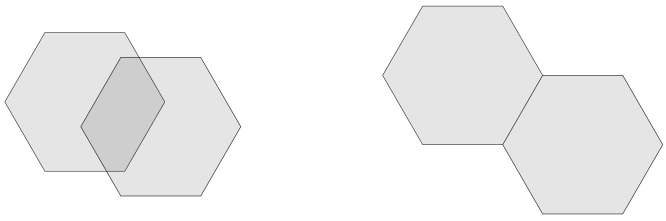

FIGURE 1. Tuiles qui s'intersectent suivant leurs bords ou non

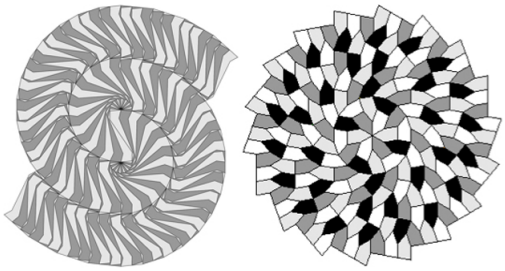

FIGURE 2. Pavages non-reguliers de Voderberg et de Hirschhorn-Hunt (source R. Coolman)

ou $\partial g(\mathbf{T})$ et $\partial g'(\mathbf{T})$ designent les "bords" de ces tuiles (on verra plus tard une definition precise de la notion de bord). On suppose par ailleurs qu'il existe deux vecteurs non colinéaires $\vec{u}$ et $\vec{v}$ tels que le pavage est invariant par les translations $t_{\vec{u}}$, $t_{\vec{v}}$ suivant l'un ou l'autre de ces vecteurs: un tel pavage est dit *régulier*.

*Invariant* signifie que l'ensemble des tuile ne change pas (et donc que la figure tracée sur le plan par la reunion des bords des differentes tuiles ne change pas) quand on applique l'une ou l'autre de ces translations:

$$\{g(\mathbf{T}),\ g \in G\} = \{\vec{u} + g(\mathbf{T}),\ g \in G\} = \{\vec{v} + g(\mathbf{T}),\ g \in G\}$$

Un résultat remarquable est qu'il n'existe qu'un nombre fini de manieres pour realiser de tels pavages (si on ne s'inquiete pas de la forme des tuiles.)

THÉORÈME 1.1 (E. Fedorov, 1891). *Il n'existe que 17 méthodes possibles pour réaliser un pavage régulier et 5 methodes possibles si $G$ ne contient pas de symetrie axiale.*

Pour chaque telle methode de pavage du plan il y a bien sur une infinité de tuiles possibles: en effet à partir d'une tuile on peut la déformer de maniere continue.

Par contre si on restreint la forme des tuiles au polygones reguliers (les polygones dont tous les cotes sont de meme longueur) on obtient

THÉORÈME 1.2 (Theoreme des polygones reguliers paveurs). *Les seul polygones reguliers permettant de paver le plan de maniere reguliere sont*

- *Les triangles equilateraux*
- *Les carres*
- *Les hexagones reguliers.*

Tout ces resultats sont des resultats sur la structure de l'ensemble des isometries (transformations du plan preservant les distances) qui quand on les applique laissent un pavage regulier invariant. Cet ensemble possede une structure algebrique supplementaire: celle de *groupe*. Cela provient des fait suivant

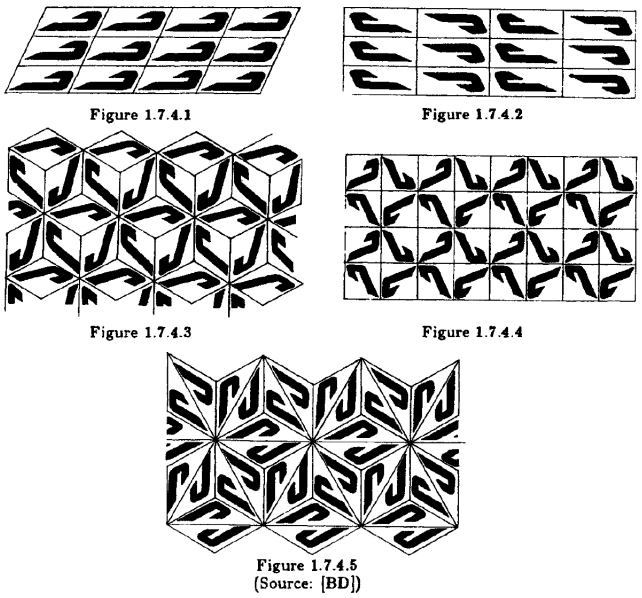


FIGURE 3. Pavages Reguliers sans symetries axiales (source Y. Brossard)

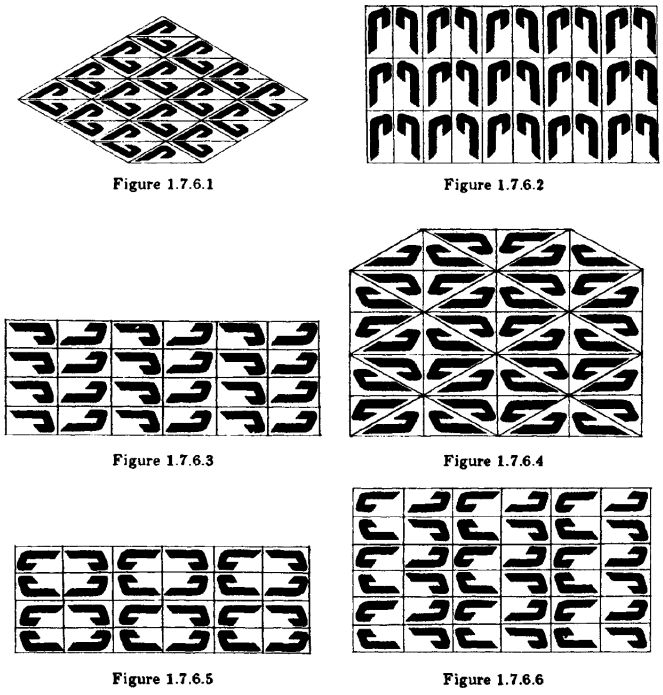


FIGURE 4. Pavages Reguliers avec symetries axiales (source Y. Brossard)

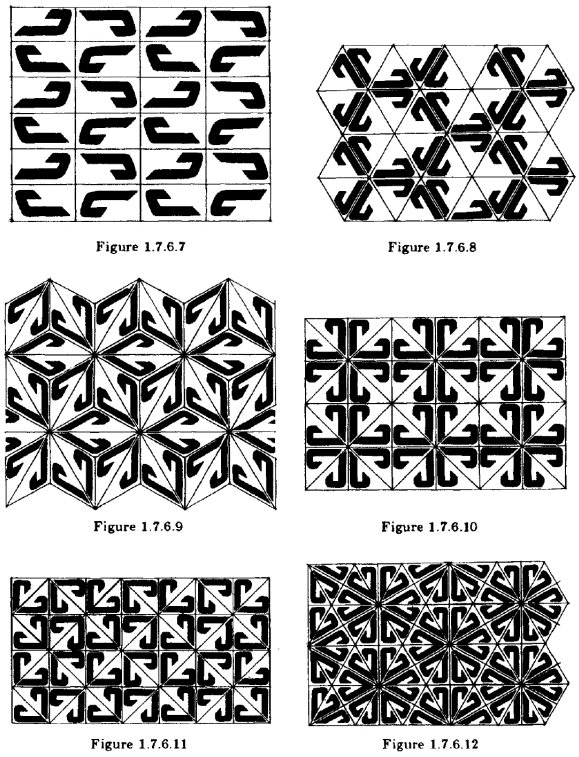


FIGURE 5. Pavages Reguliers avec symetries axiales (source Y. Brossard)

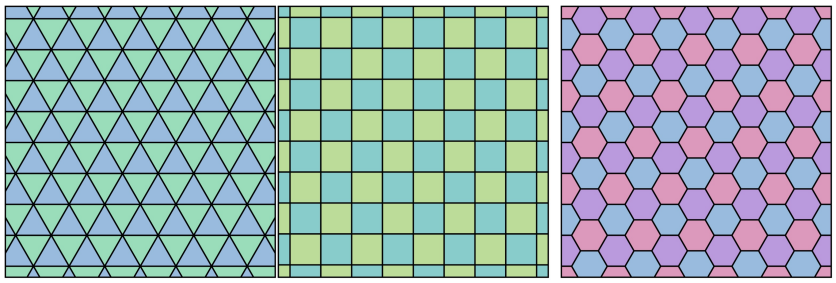

FIGURE 6. Polygones Reguliers paveurs (source wikimedia)

(1) Si deux isometries laissent un pavage invariant leur composée laisse également le pavage invariant.
(2) Si une isometries laisse un pavage invariant son inverse laisse également le pavage invariant.
(3) Transformation identité (qui envoie un point sur lui-même) est une isometrie qui laisse également le pavage invariant.

CHAPITRE 2

# Groupes

## 1. Applications entre ensembles

DÉFINITION 2.1. *Soient $E$ et $F$ des ensembles, l'ensemble produit $E \times F$ est l'ensemble forme des paires $(e, f)$ avec $e \in E$ et $f \in F$:*

$$E \times F = \{(e, f),\ e \in E,\ f \in F\}.$$

*Etant donne une paire $(e, f)$, $e$ s'appelle la premiere coordonnes et $f$ la seconde.*

DÉFINITION 2.2. *Soient $E$ et $F$ des ensembles, une application $\phi$ de $E$ vers $F$ est la donne un sous-ensemble (le "graphe")*

$$\Gamma_\phi \subset E \times F$$

*tel que:*

$$\forall e \in E,\ \exists! f \in F \text{ t.q. } (e, f) \in \Gamma_\phi,$$

*ie. l'ensemble des paires contenues dans $\Gamma_\phi$ dont la premiere coordonnee est $e$ est reduit a un element. On note la deuxieme coordonnees de cette paire $\varphi(e)$ et on l'appelle l'image de $e$ par $\phi$.*

*On note $F^E$ l'ensemble des applications de $E$ dans $F$.*

EXEMPLE 1.1. L'application identite de $E$, $\mathrm{Id}_E : E \to E$ est l'application definie par

$$\forall e \in E,\ \mathrm{Id}_E(e) = e.$$

Le graphe de $\mathrm{Id}_E$ s'appele la diagonale de $E$

$$\Delta_E = \{(e, e),\ e \in E\} \subset E \times E.$$

EXEMPLE 1.2. Etant donne le produit $E \times F$ on definit les deux applications de "projection" sur la premiere et la seconde coordonnee

$$\pi_E : \begin{array}{ccc} E \times F & \mapsto & E \\ (e, f) & \mapsto & e \end{array},\ \pi_F : \begin{array}{ccc} E \times F & \mapsto & F \\ (e, f) & \mapsto & f \end{array}.$$

EXERCICE 2.1. Decrire les graphes de ces applications ?

REMARQUE 1.1. Une raison pour la notation $F^E$ est le fait que si $E = \{e_1, \cdots, e_n\}$ possede $n$-elements, se donner une application de $\phi : E \to F$ equivaut a se donner un $n$-uplet d'elements de $F$ (un element de l'ensemble produit de $n$ termes $F \times \cdots \times F$ $n$-fois)

$$\vec{f} = (f_1, \cdots, f_n)$$

en effet on associe a un tel $n$-uplet l'application

$$\phi_{\vec{f}} : e_i \mapsto f_i,\ i = 1, \cdots, n.$$

Reciproquement a une application $\phi$ on associe

$$\vec{f_\phi} = (\phi(e_1, \cdots, \phi(e_n))$$

En particulier si $E$ et $F$ sont finis et que le nombre de leurs element est note $|E|$ et $|F|$ alors $F^E$ est fini et

$$|F^E| = |F|^{|E|}.$$

### 1.1. Composition d'applications.

DÉFINITION 2.3 (Composition). *Soit $\phi : E \to F$ et $\psi : F \to G$ des applications entre les ensembles $E$ et $F$ et $F$ et $G$, on note $\psi \circ \phi : E \to G$ l'application composee definite par*

$$\psi \circ \phi(e) = \psi(\phi(e)).$$

*La composition defini donc une application de l'ensemble produit $F^E \times G^F$ vers l'ensemble $G^E$ notee $\circ$:*

$$\begin{array}{rccc} \circ : & F^E \times G^F & \mapsto & G^E \\ & \phi \times \psi & \mapsto & \psi \circ \phi \end{array}.$$

PROPOSITION 2.1 (Formule d'associativite). *Soit $E, F, G, H$ des ensembles et $\phi : E \to F$, $\psi : F \to G$, $\omega : F \to H$ des applications, on a la formule d'associativite*

$$(\omega \circ \psi) \circ \phi = \omega \circ (\psi \circ \phi).$$

EXERCICE 2.2. Demontrer cette formule.

### 1.2. Image, pre-image, injectivite, surjectivite.

DÉFINITION 2.4 (Image/Pre-image d'un sous-ensemble). *Soit $\phi : E \mapsto F$ une application, $A \subset E$ et $B \subset F$ des sous-ensembles de $E$ et $F$.*

- *Etant donne $A \subset E$, l'image de $A$ par $\phi$ est le sous-ensemble*
$$\phi(A) = \{\phi(e),\ e \in A\} \subset F.$$
- *Etant donne $B \subset F$, la pre-image de $B$ par $\phi$ est le sous-ensemble*
$$\phi^{-1}(B) = \{e \in E,\ \phi(e) \in B\} \subset E.$$
- *Si $B = \{f\}$ est reduit a un seul element,*
$$\phi^{-1}(\{f\}) = \{e \in E|\ \phi(e) = f\}$$
*est l'ensemble des antecedents de $f$ dans $E$ pour l'application $\phi$ ou encore la "fibre" de $\phi$ au-dessus de $f$.*

DÉFINITION 2.5. *Une application $\phi : E \to F$ est*

- *Injective: si pour tout $f \in F$, l'ensemble des antecedent de $f$, $\phi^{-1}(\{f\})$ a au plus 1 element (mais peut etre l'ensemble vide $\emptyset$ qui n'a pas d'elements).*
- *Surjective: si pour tout $f \in F$, l'ensemble $\phi^{-1}(\{f\})$ a au moins 1 element.*
- *Bijective: si pour tout $f \in F$, $\phi^{-1}(\{f\})$ a exactement 1 element (ie. si $\phi$ est injective et bijective).*
- *Si $\phi$ est bijective, on defini son application reciproque $\phi^{-1} : F \to E$ comme etant l'application qui a $f \in F$ associe l'unique element de l'ensemble $\phi^{-1}(\{f\}) \subset E$. L'application $\varphi^{-1} : F \to E$ est egalement une bijection et sa reciproque est $\phi$:*
$$(\phi^{-1})^{-1} = \phi.$$
- *On a les formules de composition*
$$\phi^{-1} \circ \phi = \mathrm{Id}_E,\ \phi \circ \phi^{-1} = \mathrm{Id}_F.$$

– *Une application injective (une injection) sera notee*

$$\phi : E \hookrightarrow F.$$

– *Une application surjective (une surjection) sera notee*

$$\phi : E \twoheadrightarrow F.$$

– *Une application bijective (une bijection) sera notee*

$$\phi : E \simeq F.$$

*On note respectivement* $\mathrm{Inj}(E,F)$, $\mathrm{Surj}(E,F)$ *et* $\mathrm{Bij}(E,F)$ *l'ensemble des applications injectives, surjectives et bijectives de* $E$ *vers* $F$*:*

$$\mathrm{Bij}(E,F) = \mathrm{Inj}(E,F) \cap \mathrm{Surj}(E,F) \subset F^E.$$

DÉFINITION 2.6. *Si* $E = F$*, l'ensemble des bijections de* $E$ *vers lui-meme,* $\mathrm{Bij}(E,E)$ *sera egalement note*

$$\mathrm{Bij}(E) \text{ ou encore } \mathfrak{S}_E \text{ ou encore } S_E$$

*et sera appele l'ensemble des permutations de* $E$ *ou l'ensemble des transformations de* $E$ *ou encore le groupe symetrique de* $E$*.*

EXEMPLE 1.3. Soit $E$ un ensemble alors l'identite de $E$: $\mathrm{Id}_E : e \in E \to e \in E$ est une bijection de $E$ sur $E$ (en particulier $\mathrm{Bij}(E,E)$ est non-vide) et c'est sa propre reciproque:

$$\mathrm{Id}_E^{-1} = \mathrm{Id}_E.$$

### 1.3. Cardinal d'un ensemble.

DÉFINITION 2.7. *Soient* $E$ *et* $F$ *deux ensembles; si il existe un bijection* $\varphi : E \to F$ *entre* $E$ *et* $F$ *on dit que ces deux ensembles ont le meme cardinal. On note cette relation*

$$|E| = |F|.$$

REMARQUE 1.2. Notons que si $\phi : E \to F$ est une bijection alors l'application reciproque $\phi^{-1} : F \to E$ en est egalement une, donc la relation "avoir le meme cardinal" est une relation symetrique:

$$|E| = |F| \Longleftrightarrow |F| = |E|.$$

On a une notion un peu plus fine pour comparer des cardinaux pas forcement egaux:

DÉFINITION 2.8. *Soient* $E$ *et* $F$ *deux ensembles; si il existe un injection* $\varphi : E \hookrightarrow F$ *entre* $E$ *et* $F$ *on dit que le cardinal de* $E$ *est plus petit que celui de* $F$*. On note cette relation*

$$|E| \leqslant |F|.$$

REMARQUE 1.3. On est tente de penser que $|E| \leqslant |F|$ et si $|F| \leqslant |E|$ alors $|E| = |F|$. C'est vrai mais ce n'est pas du tout evident : c'est le Theoreme de Cantor-Bernstein-Schroeder (cf. Serie 1).

DÉFINITION 2.9. *Soit* $n \geqslant 1$ *un entier non-nul. Si un ensemble* $E$ *a meme cardinal que l'ensemble*

$$\{1, \cdots, n\}$$

*on dit que* $E$ *est de cardinal* $n$ *et on ecrit (pour simplifier et parce qu'on a l'habitude)* $|E| = n$*. On dit que l'ensemble vide* $\emptyset$ *est de cardinal* $0$*. Un ensemble* $E$ *est fini si il est de cardinal* $n$ *pour* $n \geqslant 0$*.*

EXEMPLE 1.4 (Denombrement). Soient $E$ et $F$ des ensembles finis alors $F^E$ est fini et $|F^E| = |F|^{|E|}$. On a egalement

$$|\operatorname{Bij}(E)| = |E|!$$

et si on note $\mathcal{P}(E)$ l'ensemble des sous-ensemble de $E$, on a pour $E$ fini

$$|\mathcal{P}(E)| = |\{0,1\}^E| = 2^{|E|}.$$

DÉFINITION 2.10 (Ensembles denombrables). *Un ensemble infini qui a meme cardinal que $\mathbb{N}$ est dit denombrable.*

EXEMPLE 1.5. Les ensembles $\mathbb{Z}, \mathbb{N}^2,\ \mathbb{Q},\ \mathbb{N}^3,\ \mathbb{N}^4 \cdots$ sont tous denombrables.

EXEMPLE 1.6 (Cantor). L'intervalle $[0,1[$ n'est pas denombrable. Ce resulat est obtenu par le celebre argument diagonal de cantor.

**1.4. Criteres numerique d'injectivite ou de surjectivite pour les ensembles finis.** Si les ensembles de depart ou d'arrivee sont finis on a les implications suivantes

- Si $\phi$ est injective on a $|E| \leqslant |F|$.
- Si $\phi$ est surjective on a $|E| \geqslant |F|$.
- Si $\phi$ est bijective on a $|E| = |F|$.

Par contraposee on a

- Si $|E| > |F|$ alors $\phi$ n'est pas injective (il existe deux elements $e, e' \in E$ distincts tel que $\phi(e) = \phi(e')$).
- Si $|E| < |F|$ alors $\phi$ n'est pas surjective (il existe $f \in F$ tel que $\forall e \in E,\ \phi(e) \neq f$).
- Si $|E| \neq |F|$ alors $\phi$ n'est pas bijective.

On a egalement les criteres suivants qui sont utiles:

- Si $\phi$ est injective et $|E| \geqslant |F|$ alors $\phi$ est surjective donc bijective.
- Si $\phi$ est surjective et $|E| \leqslant |F|$ alors $\phi$ est injective donc bijective.

## 2. Groupes

Etant donne un ensemble $E$ et

$$\mathfrak{S}_E = \operatorname{Aut}(E) = \operatorname{Bij}(E, E)$$

l'ensemble des bijections de $E$ sur lui meme. L'ensemble $\mathfrak{S}_E$ est equip de structures naturelles (on dit aussi "canoniques") qui meritent d'etre isolees:

(1) $\mathfrak{S}_E$ possede un element distingue, l'identite de $E$, $\operatorname{Id}_E : e \in E \mapsto e \in E$ .
(2) $\mathfrak{S}_E$ possede une operation de composition:

$$\circ : \begin{array}{ccc} \mathfrak{S}_E \times \mathfrak{S}_E & \mapsto & \mathfrak{S}_E \\ (\phi, \psi) & \mapsto & \phi \circ \psi \end{array}.$$

(3) Cette operation verifie une relation d'associativite:

$$\forall \phi, \psi, \omega \in \mathfrak{S}_E,\ (\omega \circ \psi) \circ \phi = \omega \circ (\psi \circ \phi).$$

(4) A tout element $\phi \in \mathfrak{S}_E$ est associe un element distingue, la bijection reciproque $\phi^{-1}$ qui verifie d'egalite

$$\phi^{-1} \circ \phi = \phi \circ \phi^{-1} = \operatorname{Id}_E.$$

Les mathematiciens ont realise que ces structures additionelles quoique tres simples, du fait de leur caractere completement canonique sont extremement importantes et qu'on les retrouve dans de nombreux autre objets mathematiques. Ils ont donc decide, pour les etudier, de les axiomatiser en une notion abstraite: celle de groupe.

DÉFINITION 2.11. *Un groupe $(G, \star, \cdot^{-1}, e_G)$ est un ensemble $G$ muni des structures supplementaires suivantes:*

- *d'une loi de composition interne*

$$\star : \begin{array}{ccc} G \times G & \mapsto & G \\ (a,b) & \mapsto & a \star b \end{array},$$

- *d'une application appelee inversion*

$$\cdot^{-1} : \begin{array}{ccc} G & \mapsto & G \\ g & \mapsto & g^{-1} \end{array}$$

- *d'un element distingue $e_G \in G$ appele "element neutre" ou "identite"*

*et qui verifient:*

(1) *Associativite:* $\forall a, b, c \in G,\ (a \star b) \star c = a \star (b \star c) = a \star b \star c$.
(2) *Simplification:* $\forall g \in G,\ g \star g^{-1} = g^{-1} \star g = e_G$
(3) *Neutralite:* $\forall g \in G,\ e_G \star g = g \star e_G = g$.

*L'element $g^{-1}$ est appele "element oppose" ou "symetrique" ou "inverse" de $g$.*

EXERCICE 2.3. Soit $(G, \star)$ un groupe et $g, h \in G$.

- (Unicite de l'element neutre) Montrer que si $e'_G \in G$ est tel que $g \star e'_G = g$ alors $e'_G = e_G$.
- (Unicite de l'inverse) Montrer que si $h$ verifie $g \star h = e_G$ alors $h = g^{-1}$.
- Que vaut $(g^{-1})^{-1}$ ?
- Montrer que

$$(g \star h)^{-1} = h^{-1} \star g^{-1}. \tag{2.1}$$

REMARQUE 2.1 (Commutation). Dans un groupe quelconque, on n'a pas en general l'egalite

$$a \star b = b \star a.$$

Si c'est le cas, on dit que les elements $a$ et $b$ *commutent*. Si c'est le cas pour tout $a, b \in G$, on a la definition suivante.

DÉFINITION 2.12 (Groupe commutatif). *Un groupe $(G, \star)$ est dit commutatif ou abelien si de plus la loi de composition $\star$ verifie:*

- *Commutativite:* $\forall a, b \in G,\ a \star b = b \star a$.

DÉFINITION 2.13 (Ordre d'un groupe). *Le cardinal $|G|$ d'un groupe s'appelle aussi l'ordre du groupe. Si $|G| < \infty$ est fini le groupe est dit fini.*

### 2.1. Exemples.

EXEMPLE 2.1 (Les nombres). Les ensembles des nombres

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

munis de l'addition $+$, de l'inversion $x \mapsto -x$ et de 0 comme element neutre sont des groupes et meme des groupes abeliens. En revanche $\mathbb{N}$ n'est pas un groupe car il manque l'inversion.

EXEMPLE 2.5. Soit $N \geqslant 1$ et

$$\mu_N = \{\exp(\frac{2\pi ik}{N}),\ 0 \leqslant k \leqslant N-1\} = \{\zeta \in \mathbb{C}^\times,\ \zeta^N = 1\} \subset \mathbb{C}^1$$

l'ensemble des racine $N$-iemes de l'unite muni de la multiplication est un groupe d'element neutre 1.

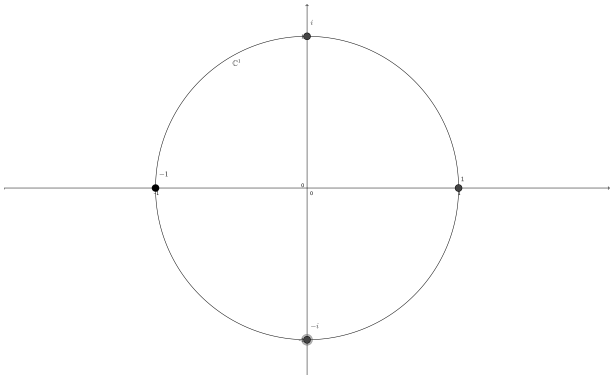

FIGURE 1. Le cercle unite et le groupe $\mu_4$

EXEMPLE 2.2 (Les nombres non-nuls). Les ensembles des nombres

$$\mathbb{Q}^\times,\ \mathbb{R}_{>0} \subset \mathbb{R}^\times \subset \mathbb{C}^\times$$

munis de la multiplication $\times$, de l'inversion $x \mapsto 1/x$ et de 1 comme element neutre sont des groupes. En revanche $\mathbb{R}_{<0}$ n'est pas un groupe car $-1 \times -1 = 1 \notin \mathbb{R}_{<0}$.

EXEMPLE 2.3 (Groupes d'un espace vectoriel). Les espaces vectoriels sur $\mathbb{R}$ pour $n \geqslant 1$, $\mathbb{R}^n$ et $\mathbb{C}^n$ munis de l'addition des vecteurs, de la multiplication par $-1$, et de l'element neutre $\vec{0} = (0, \cdots, 0)$ sont des groupes.

EXEMPLE 2.4 (Le cercle unite). On a vu que $(\mathbb{C}^\times, \times)$ est un groupe pour la multiplication; l'ensemble des nombre complexes de module 1 (aussi appele cercle unite)

$$\mathbb{C}^1 = \{z \in \mathbb{C},\ |z| = 1\}$$

est aussi un groupe pour la multiplication :

$$|1| = 1,\ |z| = 1 \Rightarrow |1/z| = 1,\ |z| = |z'| = 1 \Rightarrow |z \times z'| = |z||z'| = 1.$$

EXEMPLE 2.6. Si $E$ est un ensemble fini de cardinal $|E| = n$, on a $|\mathfrak{S}_E| = n!$.

Si $|E| \leqslant 2$ ce groupe est commutatif; il ne l'est plus des que $n \geqslant 3$. Par exemple si $E = \{1, 2, 3\}$, $\sigma = (123)$ et $\tau = (12)$ on a

$$(123) \circ (12) = (13),\ (12) \circ (123) = (23) \neq (13).$$

EXEMPLE 2.7. Groupe des matrices inversible $2 \times 2$. Soit $k = \mathbb{R}$ ou $\mathbb{C}$. On note

$$\mathrm{GL}_2(k) = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in k,\ \det(M) = ad - bc \neq 0\}.$$

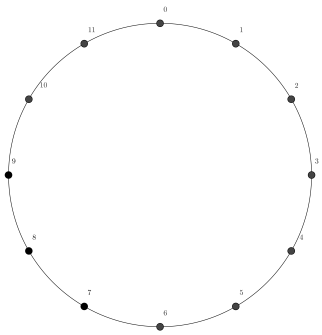


FIGURE 2. Le groupe de l'horloge

Cet ensemble forme un groupe pour la multiplication des matrices d'element neutre

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

car

(1) La multiplication des matrices est associative.
(2) $\det(M.M') = \det(M).\det(M')$ est non-nul si (et seulement si) $\det(M)$ et $\det(M')$ le sont et $M.M' \in \mathrm{GL}_2(k)$.
(3) $M.\mathrm{Id} = \mathrm{Id}.M = M$
(4) Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \in \mathrm{GL}_2(\mathbb{R})$, alors

$$M' = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

verifie $\det(M') = \det(M)^{-1} \neq 0$ et

$$M.M' = M'.M = \mathrm{Id}.$$

EXEMPLE 2.8 (Groupe de l'horloge). Soit $\mathbb{N}_{<12} := \{0, 1, 2, 3, 4, 5, \cdots, 11\}$; on defini sur cet ensemble la loi

$$a \oplus b = \text{ reste de la division de } a + b \text{ par } 12.$$

Ainsi equipe, $\mathbb{N}_{<12}$ forme un groupe commutatif d'element neutre 0.

Plus generalement pour $N \geqslant 1$ Soit $\mathbb{N}_{<N} = \{0, 1, 2, 3, 4, N - 1\}$; on defini sur cet ensemble la loi

$$a \oplus b = \text{ reste de la division de } a + b \text{ par N.}$$

Ainsi equipe, $\mathbb{N}_{<N}$ forme un groupe commutatif d'element neutre 0; l'inverse de 0 est 0 et de $n \geqslant 1$ est $N - n$.

On note ce groupe $\mathbb{Z}/N\mathbb{Z}$.

EXEMPLE 2.9 (Groupe de multiplicatif de l'horloge). Soit l'ensemble $\{1, 5, 7, 11\}$ des entier $< 12$ et premiers a 12; on pose

$$a \otimes b = \text{ reste de la division de } a \times b \text{ par } 12.$$

Muni de cette loi, on obtient un groupe commutatif d'element neutre 1.

Plus generalement pour $N \geqslant 1$, soit

$$(\mathbb{Z}/N\mathbb{Z})^\times = \{1 \leqslant a \leqslant N-1,\ (a,N)=1\}$$

; pour $a, b$ dans cet ensemble, on pose

$$a \otimes b = \text{ reste de la division de } a \times b \text{ par N},$$

on obtient un groupe commutatif d'element neutre 1. Lexistence d'un inverse est une consequence de l'identite de Bezout pour $a$ et $N$ qui sont premiers entre eux.

Exemple 2.10. Notons $d(PQ) = \sqrt{(x_P - x_Q)^2 + (y_P - x_Q)^2}$ la distance Euclidienne dans le plan $\mathbb{R}^2$. On note

$$\mathrm{Isom}(\mathbb{R}^2) = \{\phi : \mathbb{R}^2 \to \mathbb{R}^2,\ \forall P, Q \in \mathbb{R}^2,\ d(\phi(P), \phi(Q)) = d(P,Q)\}$$

l'ensemble des applications qui preservent la distance: les *isometries* de $\mathbb{R}^2$. On va montrer qu'une isometrie est une bijection. On montre egalement que Id est une isometrie et que la compose de deux isometries ainsi que leurs reciproques en sont. Ainsi $(\mathrm{Isom}(\mathbb{R}^2), \circ)$ forme un groupe contenu dans $\mathrm{Bij}(\mathbb{R}^2)$.

2.1.1. *Groupe produit.* Soient $(G, *)$ et $(H, .)$ des groupes alors l'ensemble produit

$$G \times H = \{(g,h),\ g \in G,\ h \in H\}$$

a une structure de groupe naturelle pour la loi de composition

$$(g,h) \otimes (g',h') := (g * g', h.h').$$

L'element neutre est l'element

$$e_{G\times H} = (e_G, e_H)$$

et l'inversion est donnee par

$$(g,h)^{-1} = (g^{-1}, h^{-1}).$$

## 2.2. Sous-groupe.

Définition 2.14. *Un sous-groupe $H \subset G$ d'un groupe $(G, \star)$ est un sous-ensemble verifiant*

(1) $e_G \in H$,
(2) $\forall h, h' \in H,\ h \star h' \in H$,
(3) $\forall h \in H,\ h^{-1} \in H$.

*Alors $(H, \star_{|H\times H})$ (muni de la loi de composition $\star$ restreinte a $H \times H$ et de l'element neutre $e_G$) forme un groupe.*

Exemple 2.11.
- L'element neutre $\{e_G\}$ forme un sous-groupe a lui tout seul: Le sous-groupe trivial.
- L'ensemble $\mathrm{Isom}(\mathbb{R}^2)$ est un sous-groupe de $\mathrm{Bij}(\mathbb{R}^2)$.
- L'ensemble des rotations de centre 0 et d'angle $2\pi/N$ est un sous-groupe de l'ensemble des isometries du plan.
- L'ensemble $T(\mathbb{R}^2)$ des translations du plan est un sous-groupe de l'ensemble des isometries $\mathrm{Isom}(\mathbb{R}^2)$.
- L'ensemble $\{0, 2, 4\}$ est un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$.
- L'ensemble $\{\mathrm{Id}_{\{1,2,3\}},\ (123),\ (132)\}$ est un sous-groupe de $\mathfrak{S}_3$.

PROPOSITION 2.2 (Critere de sous-groupe). *Un sous-ensemble non-vide $H$ d'un groupe $G$ est un sous-groupe (pour $\star$ et d'element neutre $e_G$) ssi*

$$\forall h, h' \in H,\ h \star h'^{-1} \in H. \tag{2.2}$$

PREUVE. Etant donne $H \subset G$ un sous-groupe et $h, h' \in H$, on a $h'^{-1} \in H$ par (3) et $h \star h'^{-1} \in H$ par (2).

Reciproquement, etant donne $H \subset G$ verifiant (2.2) et $h, h' \in H$

(1) $e_G = h \star h^{-1} \in H$.
(2) On a (1) en appliquant (2.2) a $h = h' = e_G$,
(3) (3) en appliquant (2.2) a $h = e_G, h' = h$,
(4) (2) en appliquant (2.2) a $h, h'' = h'^{-1}$ de sorte que $h''^{-1} = h'$.

□

EXEMPLE 2.12. Soit $E$ un ensemble, $F \subset E$ un sous-esemble et $(G, \circ) \subset (\mathrm{Bij}(E), \circ)$ un sous-groupe de $(\mathrm{Bij}(E), \circ)$ (le groupe des bijections de $E$ sur lui-meme, muni de la composition, de l'identite de $E$ comme element neutre et de l'application reciproque pour l'inverse). On considere

$$G_F := \{g \in G,\ g(F) = F\} \subset G$$

le sous-ensemble des application de $G$ qui laissent $F$ invariant: on note $G_F$ le *stabilisateur de $F$ dans $G$*. Alors $(G_F, \circ)$ est un sous-groupe de $(G, \circ)$.

Pour le voir on applique le critere de sous-groupe: son $g, g' \in G_F$, on veut montrer que $g \circ g'^{-1}$ appartient a $G_F$, c'est a dire

$$g \circ g'^{-1}(F) = F.$$

On a

$$g(F) = F = g'(F).$$

composant l' egalite $F = g'(F)$ avec $g'^{-1}$ on obtient

$$g'^{-1}(F) = g'^{-1}(g'(F)) = \mathrm{Id}_E(F) = F.$$

En particulier $g'^{-1} \in G_F$. On a alors

$$g \circ g'^{-1}(F) = g(g'^{-1}(F)) = g(F) = F$$

et donc $g \circ g'^{-1} \in G_F$.

Par exemple soit $E = \mathbb{R}^2$ le plan et $G = \mathrm{Isom}(\mathbb{R}^2)$ l'ensemble des isometries de $\mathbb{R}^2$ (vu au gymnase et qu'on etudiera un peu plus tard). $\mathrm{Isom}(\mathbb{R}^2)$ est un sous-groupe de $\mathrm{Bij}(\mathbb{R}^2)$. Considerons un carre dans $\mathbb{R}^2$ de centre $P$ de diagonales sont notes $D_1, D_2$ et dont les droites joingnant les milieux des cotes opposes sont notes $D'_1, D'_2$ alors

$$G_F = \{\mathrm{Id}_{\mathbb{R}^2}, r_{P,\pi/2}, r_{P,\pi}, r_{P,3\pi/2}, s_{D_1}, s_{D_2}, s_{D'_1}, s_{D'_2}\}$$

ou $r_{P,\theta}$ designe la rotation de centre $P$ et d'angle $\theta$ et $s_D$ designe la symetrie orthogonale par rapport a la droite $D$. On verifie que $G_F$ est stable par composition et inverse.

EXERCICE 2.4. Les sous-groupes de $\mathbb{Z}$ sont exactement les sous-ensembles de la forme $N\mathbb{Z}$ pour $N \in \mathbb{Z}$.

EXERCICE 2.5. Soit $N \geqslant 1$ et $M|N$ alors l'ensemble des multiples de $M$ dans $\{0, \cdots, N-1\}$ forme un sous-groupe de $\mathbb{Z}/N\mathbb{Z}$ de cardinal $N/M$ et reciproquement tout sous-groupe est de cette forme.

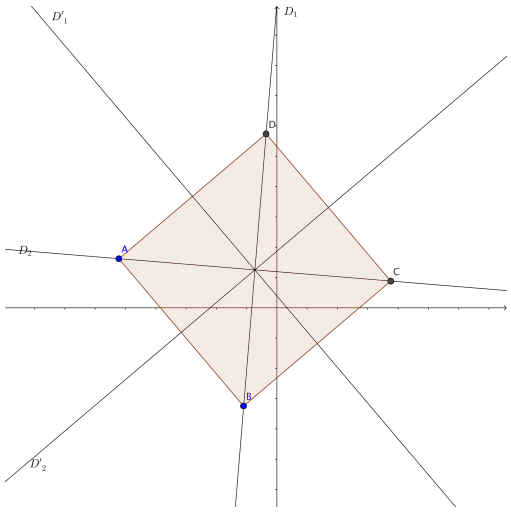


FIGURE 3.

**2.3. Table de multiplication d'un groupe.** Une maniere de representer un groupe (surtout) si il est fini est de donner sa table de multiplications: c'est un tableau a double entree avec en ligne et en colonne les elements du groupe (commencant par l'element neutre) par exemple le groupe trivial $(1, \times)$...

| $a \oplus b$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

FIGURE 4. $\mathbb{Z}/4\mathbb{Z}$

| $a \otimes b$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

| $a \oplus b$ | (0,0) | (0,1) | (1,0) | (1,1) |
|---|---|---|---|---|
| (0,0) | (0,0) | (0,1) | (1,0) | (1,1) |
| (0,1) | (0,1) | (0,0) | (1,1) | (1,0) |
| (1,0) | (1,0) | (1,1) | (0,0) | (0,1) |
| (1,1) | (1,1) | (1,0) | (0,1) | (0,0) |

FIGURE 5. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $(\mathbb{Z}/12\mathbb{Z})^\times$

## 3. Morphismes de groupes

Un morphisme de groupes est une application entre deux groupes qui est compatible avec les structures de groupes:

DÉFINITION 2.15. *Etant donnes deux groupes $(G, .)$ et $(H, \star)$ de lois respectives . et $\star$, un morphisme de groupes de $G$ vers $H$ est une application $\phi : G \mapsto H$ qui verifie*

(1) $\phi(e_G) = e_H$.
(2) $\phi(g.g') = \phi(g) \star \phi(g')$
(3) $\phi(g^{-1}) = \phi(g)^{-1}$

*Si $H = G$, on dit egalement que $\phi$ est un endomorphisme (de groupes) de $G$.*

DÉFINITION 2.16. *Soit $G$ et $H$ deux groupes, on note*

- $\mathrm{Hom}_{Gr}(G, H)$ *l'ensemble des morphismes de groupes de $G$ vers $H$.*
- $\mathrm{End}_{Gr}(G) = \mathrm{Hom}_{Gr}(G, G)$ *l'ensemble des endomorphismes (de $G$ vers lui-meme).*
- $\mathrm{Iso}_{Gr}(G, H)$ *l'ensemble des morphismes de groupes de $G$ vers $H$ qui sont bijectifs: c'est l'ensembles des isomorphismes de $G$ vers $H$.*
- $\mathrm{Aut}_{Gr}(G) = \mathrm{Iso}_{Gr}(G, G)$ *l'ensemble des isomorphismes de $G$ vers $G$: les automorphismes de $G$.*

La proposition suivante permet de reconnaitre quand une application entre groupes est un morphisme:

PROPOSITION 2.3 (Critere de morphisme). *Pour verifier qu'une application*

$$\phi : G \to H$$

*est un morphisme de groupe il suffit de verifer la deuxieme condition de la definition precedente:*

$$\phi(g.g') = \phi(g) \star \phi(g').$$

PREUVE. L'identite ci-dessus est la deuxieme condition pour avoir un morphisme; verifions la premiere et la troisieme. Appliquons l'identite precedente a $g = g' = e_G$:

$$\phi(e_G) = \phi(e_G) \star \phi(e_G)$$

et multiplions par $\phi(e_G)^{-1}$ de part et d'autre:

$$\phi(e_G)^{-1} \star \phi(e_G) = \phi(e_G)^{-1} \star \phi(e_G) \star \phi(e_G) \Longrightarrow e_H = e_H \star \phi(e_G) \Longrightarrow e_H = \phi(e_G).$$

Appliquons l'identite precedente a $g = g'$:

$$\phi(g.g^{-1}) = \phi(g) \star \phi(g^{-1}) = \phi(e_G) = e_H$$

de sorte que

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

□

EXEMPLE 3.1. Les application suivantes sont des morphisme de groupes:

$$N \in \mathbb{Z},\ [\times N] : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathbb{Z} \\ n & \mapsto & Nn \end{array}.$$

$$\exp : \begin{array}{ccc} (\mathbb{R}, +) & \mapsto & (\mathbb{R}^\times, \times) \\ x & \mapsto & \exp(x) \end{array}.$$

Ce morphisme n'est pas surjectif: en revanche celui-ci l'est

$$\exp : \begin{array}{ccc} (\mathbb{R}, +) & \mapsto & (\mathbb{R}_{>0}, \times) \\ x & \mapsto & \exp(x) \end{array}.$$

Quel est le morphisme inverse ?

$$\exp : \begin{array}{ccc} (\mathbb{R}, +) & \mapsto & (\mathbb{C}^1, \times) \\ x & \mapsto & \exp(2\pi i x) \end{array} := \cos(2\pi x) + i \sin(2\pi x).$$

**3.1. Exemple: composition de morphismes.** La notion de morphisme est stable par composition:

PROPOSITION 2.4. *Soient $G, H, K$ trois groupes et $\phi : G \to H$, $\psi : H \to K$ alors l'application composee*

$$\psi \circ \phi : \begin{array}{ccc} G & \mapsto & K \\ g & \mapsto & \psi(\phi(g)) \end{array}$$

*est un morphisme de groupes.*

PREUVE. Exercice □

**3.2. Exemple: isomorphismes de groupes.** On a defini un isomorphisme de groupes $\phi : G \to H$ comme etant une application bijective entre $G$ et $H$ qui est morphisme de groupe. Il se trouve que la reciproque $\phi^{-1}$ est encore un morphisme de groupe (de $H$ vers $G$.)

PROPOSITION 2.5. *Soit $\phi : G \mapsto H$ un morphisme de groupe qui en tant qu'application est bijectif alors l'application reciproque $\phi^{-1} : H \mapsto G$ est un morphisme de groupes.*

PREUVE. Soit $H, h' \in H$, montrons que

$$\phi^{-1}(h \star h') = \phi^{-1}(h).\phi^{-1}(h').$$

Pour cela il suffit de montrer que

$$\phi(\phi^{-1}(h \star h')) = \phi(\phi^{-1}(h).\phi^{-1}(h')).$$

On a

$$\phi(\phi^{-1}(h \star h')) = h \star h'$$

et comme $\phi$ est un morphisme

$$\phi(\phi^{-1}(h).\phi^{-1}(h')) = \phi(\phi^{-1}(h)) \star \phi(\phi^{-1}(h')) = h \star h'.$$

□

COROLLAIRE 2.1. *Soit* $\mathrm{Aut}(G)$ *l'ensemble des isomorphismes (de groupes) de $G$ sur $G$ (les automorphismes). Montrer que* $\mathrm{Aut}(G) \subset \mathrm{Bij}(G)$ *est un sous-groupe de* $(\mathrm{Bij}(G), \circ)$.

PREUVE. Exercice □

**3.3. Exemple: translation dans un groupe.** Soit $(G, .)$ un groupe et $g \in G$, l'application de translation a gauche par $g$ est l'application

$$t_g : \begin{array}{ccc} G & \mapsto & G \\ g' & \mapsto & g.g'. \end{array}$$

Cette application n'est PAS un morphisme de groupe en general: elle ne l'est que si $g = e_G$. En effet si $g = e_G$, on a $t_g(g') = e_g.g' = g'$ et $t_{e_G} = \mathrm{Id}_G$. Sinon on a

$$t_g(e_G)0g.e_G = g \neq e_G$$

donc $t_g$, 'est pas un morphisme de groupes. En revanche $t_g \in \mathrm{Bij}(G)$. En effet, $t_g$ admet $t_{g^{-1}}$ comme application reciproque:

$$t_{g^{-1}} \circ t_g(g') = g^{-1}.g.g' = g'$$

et donc $t_{g^{-1}} \circ t_g = \mathrm{Id}_G$ et de meme $t_g \circ t_{g^{-1}} = \mathrm{Id}_G$.

EXERCICE 2.6. Montrer que l'application tramslation a gauche

$$t_\cdot : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & t_g \end{array}$$

est un morphisme de groupes de $(G, .)$ vers $(\mathrm{Bij}(G), \circ)$.

**3.4. Exemple: conjugaison dans un groupe.** Soit $(G, .)$ un groupe et $g \in G$, l'application de conjugaison par $g$ est l'application

$$\mathrm{Ad}_g : \begin{array}{ccc} G & \mapsto & G \\ g' & \mapsto & g.g'.g^{-1}. \end{array}$$

EXERCICE 2.7. Montrer que cette application est un morphisme de groupe bijectif et trouver l'application reciproque.

EXERCICE 2.8. Montrer que l'application conjugaison

$$\mathrm{Ad}_\cdot : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{Ad}_g \end{array}$$

est un morphisme de groupes de $(G, .)$ vers $(\mathrm{Bij}(G), \circ)$.

**3.5. Sorite: Morphismes de structures.** Plus generalement, dans la suite on va rencontrer des ensembles munis d'une structure additionelle *Str* (ainsi les groupes, mais aussi les espaces vectoriels, les espaces euclidiens ou encore les $G$-ensembles). Ces ensembles munis de telles structures additionelles sont regroupes dans ce qu'on appelle une *categorie*: la categorie $\mathcal{EV}_{\mathbb{R}}$ des espaces vectoriels sur $\mathbb{R}$, la categorie $\mathcal{G}$ des groupes, etc...

Etant donnees $E, F$ des ensembles appartenant a une telle categorie, c'est a dire possedant une structure *Str* supplementaire donnee, on dira qu'une application $\phi : E \to F$ compatible avec *Str* est un *morphisme* ou un *homomorphisme* (de la categorie concernee).

- Si le morphisme a pour ensemble d'arrivee l'ensemble de depart $E$, on parlera d'*endomorphisme*.
- Si le morphisme est injectif on parlera de*monomorphisme* (de structure).
- Si le morphisme est surjectif on parlera d'*epimorphisme* (de structure).
- Si le morphisme est bijectif on parlera d'*isomorphisme* ou d'homeomorphismes (de structure),
- et pour un endomorphisme bijectif on parlera d'*automorphisme* (de structure)

On notera respectivement

$$\mathrm{Hom}_{Str}(E, F),\ \mathrm{Homeo}_{Str}(E, F) = \mathrm{Iso}_{Str}(E, F),\ \mathrm{Aut}_{Str}(E) = \mathrm{Isom}_{Str}(E, E)$$

les ensembles des morphismes, homeo/isomorphismes et automorphismes preservant la structure. Si la structure est evidente (d'apres le contexte) on pourra omettre de la mentionner.

EXEMPLE 3.2. Dans la categorie des $\mathbb{R}$-espaces vectoriels les morphismes sont les applications $\mathbb{R}$-lineaires.

**3.6. Noyau, Image.**

DÉFINITION 2.17. *Soient $(G, .)$ et $(H, \star)$ deux groupes et $\phi : G \to H$ un morphisme de groupes,*

- *L'image de $\phi$, est l'image de $G$ par $\phi$ au sens des ensembles*

$$\mathrm{Im}(\phi) = \phi(G) = \{\phi(g),\ g \in G\} \subset H.$$

– *Le noyau de $\phi$ est la pre-image (l'ensemble des antecedents) de l'element neutre $e_H$*

$$\ker(\phi) = \phi^{-1}(\{e_H\}) = \{g \in G,\ \phi(g) = e_H\}.$$

PROPOSITION 2.6. *Soit $\phi : G \to H$ un morphisme de groupes, $\ker(\phi)$ et $\mathrm{Im}(\phi)$ sont des sous-groupes de $G$ et $H$ respectivement.*

PREUVE. D'apres la Proposition 2.2 il suffit de verifier que

$$\forall g, g' \in \ker(\phi),\ g.(g')^{-1} \in \ker(\phi)$$

c'est a dire que $\phi(g.(g')^{-1}) = e_H$. D'autre part il suffit de montrer que

$$\forall h, h' \in \mathrm{Im}(\phi) \Rightarrow h \star (h')^{-1} \in \mathrm{Im}(\phi)$$

c'est a dire qu'il existe $g'' \in G$ tel que $\phi(g'') = h \star (h')^{-1}$. Dans le premier cas, comme $\phi$ est un morphisme, on a

$$\phi(g.(g')^{-1}) = \phi(g) \star \phi(g'^{-1}) = \phi(g) \star \phi(g')^{-1} = e_H \star e_H$$

car

$$\phi(g) = \phi(g') = e_H.$$

Dans le second cas, il existe $g, g' \in G$ tels que

$$h = \phi(g),\ h' = \phi(g'),\ \textit{et donc } h \star (h')^{-1} = \phi(g) \star \phi((g')^{-1}) = \phi(g.(g')^{-1})$$

donc $h \star (h')^{-1} \in \mathrm{Im}(\phi)$. □

L'importance du noyau tient au fait qu'il permet de resoudre des equations lineaires dans des groupes:

THÉORÈME 2.1. *Soit $\phi : G \to H$ un morphisme de groupes. Soit $h \in H$ alors l'ensemble des solution de l'equation (d'inconnue $g \in G$)*

$$Eq(\phi, h) : \quad \phi(g) = h$$

*(en d'autres termes la pre-image $\phi^{-1}(\{h\})$) est de la forme*

$$\phi^{-1}(\{h\}) = \begin{cases} \emptyset & \textit{si } h \notin \mathrm{Im}(\phi) \\ g_0.\ker(\phi) = \ker(\phi).g_0 = \{g_0.k,\ k \in \ker(\phi)\} = \{k.g_0,\ k \in \ker(\phi)\} & \textit{si } h \in \mathrm{Im}(\phi). \end{cases}$$

*Dans le second cas, $g_0$ designe n'importe quelle solution de l'equation $E(\phi, h)$, ie. $\phi(g_0) = h$.*

**Preuve**: Dans le premier cas, si $h \notin \mathrm{Im}(\phi)$ alors il n'a pas d'antecedent et l'equation $Eq(\phi, h)$ pas de solution. Supposons qu'on soit dans le second cas et soit $g_0$ une solution, alors pour tout $k \in \ker(\phi)$ on a

$$\phi(g_0.k) = \phi(g_0).\phi(k) = h.e_H = h \text{ et } \phi(k.g_0) = \phi(k).\phi(g_0) = e_H.h = h$$

donc $g_0.k$ et $k.g_0$ sont solutions. Reciproquement soit $g$ une autre solution et

$$k = g.g_0^{-1},\ k' = g_0^{-1}.g$$

alors

$$g = k \star g_0,\ g = g_0.k'$$

et

$$\phi(k) = \phi(g.g_0^{-1}) = h \star h^{-1} = e_H,\ \phi(k') = \phi(g_0^{-1}.g) = h^{-1} \star h = e_H$$

et $k, k' \in \ker(\phi)$.

Ainsi quand il est non-vide, l'ensemble des solution de $Eq(\phi, h)$ est de la forme

$$g_0 \ker(\phi) = t_{g_0}(\ker(\phi))$$

c'est a dire l'image de $\ker(\phi)$ par l'application $t_{g_0}$ de translation a gauche par $g_0$. □

REMARQUE 3.1. Ce resultat tres general recouvre plusieurs cas particuliers rencontres au gymnase: considerons par exemple le cas ou $G = \mathbb{R}^m$ et $H = \mathbb{R}^n$ sont les groupes abeliens associes a des espaces vectoriels de dimension finis et $\phi : \mathbb{R}^m \to \mathbb{R}^n$ est une application lineaire donnee par une matrice $\mathbf{a} = (a_{ij})_{i\leqslant m, j\leqslant n}$ et $h = \mathbf{y} = (y_1, \cdots, y_n)$: dans ce cas, notant $g = \mathbf{x} = (x_1, \cdots, x_m)$ l'equation devient $\phi(x_1, \cdots, x_m) = (y_1, \cdots, y_n)$ ou encore le systeme de $n$ equations lineaires a $m$ inconnues

$$Eq(\mathbf{a}, \mathbf{y}) : \begin{array}{rcl} a_{11}x_1 + \cdots + a_{1m}x_m & = & y_1 \\ \vdots & = & \vdots \\ a_{n1}x_1 + \cdots + a_{nm}x_m & = & y_n \end{array}$$

dont on sait que les solutions, si il y en a, sont de la forme

$$\mathbf{x}_0 + \mathbf{x} = (x_{01} + x_1, \cdots, x_{0m} + x_m)$$

ou $\mathbf{x}_0$ est une solution particuliere de $Eq(\mathbf{a}, \mathbf{y})$ et $\mathbf{x}$ est une solution quelconque de l'equation lineaire homogene (ie. sans second membre)

$$Eq(\mathbf{a}, \mathbf{0}) : \begin{array}{rcl} a_{11}x_1 + \cdots + a_{1m}x_m & = & 0 \\ \vdots & = & \vdots. \\ a_{n1}x_1 + \cdots + a_{nm}x_m & = & 0 \end{array}$$

Ainsi $\mathbf{x}_0$ est notre $g_0$ et $\mathbf{x}$ est un element de $\ker(\phi)$.

Un autre cas est celui des equations differentielles lineaires: si on cherche les solution de l'equation differentielle (d'ordre 1)

$$a.f'(x) + bf(x) = h(x)$$

ou $a, b \in \mathbb{R}$, $a \neq 0$, $f : x \mapsto f(x)$ est une fonction de classe $\mathcal{C}^1$ (derivable de derivee continue) sur $\mathbb{R}$ et $h : x \mapsto h(x)$ est une fonction continue sur $\mathbb{R}$ (par exemple une fonction constante) alors toute solution si elle existe est de la forme $f(x9 = f_0(x) + k(x)$ ou $f_0$ est une solution particulier de cette equation (qu'il faut trouver) et $k$ est une solution de l'equation sans second membre

$$a.f'(x) + bf(x) = 0$$

(on a $k(x) = k(0)\exp(-\frac{b}{a}x)$). Dans ce cas on a

$$G = (\mathcal{C}^1(\mathbb{R}, \mathbb{R}), +),\ G = (\mathcal{C}^0(\mathbb{R}, \mathbb{R}), +),\ \phi(f) = a.f' + b.f.$$

Le theoreme admet les corollaires suivants:

THÉORÈME 2.2 (Critere d'injectivite de morphismes). *Un morphisme de groupes $\phi : G \mapsto H$ est injectif ssi*

$$\ker(\phi) = \{e_G\}.$$

PREUVE. Si $\phi$ est injective alors par definition $\phi^{-1}(\{e_H\}) = \ker\phi$ possede au plus 1 element. Comme $\ker\phi$ contient $e_G$ (car $\phi$ est un morphisme), on a $\ker\phi = \{e_G\}$.

Reciproquement si $\ker\phi = \{e_G\}$ alors pour tout $h \in H$, ou bien $\phi^{-1}(\{h\})$ est l'ensemble vide (et possede 0 elements) ou bien

$$\phi^{-1}(\{h\}) = g_0.\ker\phi$$

mais

$$g_0.\ker\phi = g_0.\{e_G\} = \{g_0\}$$

ne possede qu'un element. en resume, tout $h \in H$ possede au plus un antecedent par $\phi$: $\phi$ est injectif.

□

Le corollaire suivant concerne les groupes finis.

THÉORÈME 2.3 (Theoreme Noyau-Image numerique pour les groupes). *Soit $G$ un groupe fini de cardinal $|G|$ et $\phi : G \to H$ un morphisme alors $\phi(G) = \mathrm{Im}(\phi)$ est un groupe fini et one a*

$$|G| = |\ker\phi||\operatorname{Im}\phi|.$$

*En particulier $|\ker\phi|$ et $|\operatorname{Im}\phi|$ divisent $|G|$.*

REMARQUE 3.2. ce theoreme admet un analogue en algebre lineaire: si $k$ est un corps et $\phi : E \to F$ est une application lineaire entre deux $k$-espaces vectoriels alors le theoreme Noyau-image dit que

$$\dim_k E = \dim_k \ker\phi + \dim_k \operatorname{Im}\phi.$$

REMARQUE 3.3. On verra plus tard une version plus precise du theoreme noyau image.

REMARQUE 3.4. On va voir un peu plus tard le *Theoreme de Lagrange* qui dit que si $G$ est un groupe fini et $G' \subset G$ est un sous-groupe ($G'$ n'est pas forcement un noyau) alors $|G'|$ divise $|G|$.

**Preuve**: comme $G$ est fini, $\operatorname{Im}\phi = \phi(G)$ est fini. Quand $h$ varie dans $\operatorname{Im}\phi$ l'ensemble des antecedents

$$\phi^{-1}(\{h\}) = \{g \in G,\ \phi(g) = h\}$$

forme une partition de $G$: pour $h \neq h'$ les ensembles $\phi^{-1}(\{h\})$ et $\phi^{-1}(\{h'\})$ sont disjoints et $G$ est la reunion des $\phi^{-1}(\{h\})$ pour $h$ parcourant $\operatorname{Im}\phi$. On note cela

$$G = \bigsqcup_{h\in\operatorname{Im}\phi} \phi^{-1}(\{h\}).$$

Alors le cardinal de $G$ est la somme des cardinaux des $\phi^{-1}(\{h\})$

$$|G| = \sum_{h\in\operatorname{Im}\phi} |\phi^{-1}(\{h\})|$$

mais on a pour $h \in \phi^{-1}(\{h\})$ et $\phi(g_0) = h$

$$|\phi^{-1}(\{h\})| = |g_0.\ker\phi| = |\{g_o k,\ k \in \ker\phi\}| = |\ker\phi|$$

car la translation a gauche $t_{g_0} : k \mapsto g_0 k$ est injective sur $G$, ainsi

$$|G| = \sum_{h\in\operatorname{Im}\phi} |\ker\phi| = |\operatorname{Im}\phi||\ker\phi|.$$

□

3.6.1. *Notion de sous-groupe distingue.*

DÉFINITION 2.18. *Soit $G$ une groupe et $K$ un sous-groupe. On dit que $K$ est distingue dans $G$ (ou est normal dans $G$) et on le note*

$$K \lhd G$$

*si pour tout $g \in G$, on a*

$$\mathrm{Ad}_g(K) = g.K.g^{-1} = K.$$

*En d'autre termes si $K$ est invariant par conjugaison par n'impote quel element de $G$.*

EXEMPLE 3.3. Les sous-groupes $\{e_G\}$ et $G$ sont distingues mais ce sont des sous-groupes distingues evidents.

REMARQUE 3.5. Cette notion est importante pour etudier la structure des groupe car elle permet de la decomposer en structure plus simple: si $K \lhd G$ est un sous-groupe distingue, on peut associe a $G$ et $K$ un groupe "quotient" $G/K$ (voir plus tard) qui est plus simple que $G$ et alors les structures de $G/K$ et $K$ permettent de retrouver la structure de $G$. On applique cette decomposition au groupes $K$ et $G/K$ jusqu'a ce que ce soit impossible: un groupe qui ne possede aucun sous-groupe distingue non-trivial est dit *simple*. Les groupes simple sont en quelque sorte les briques de base des groupes quelconques.

THÉORÈME 2.4. *soit $\phi : G \to H$ un morphisme de groupes alors $K = \ker \phi$ est distingue.*

**Preuve**: On a vu que tout $g_0 \in G$ on a

$$g_0.\ker \phi = \ker \phi.g_0$$

Multipliant cette egalite a droite par $g_0^{-1}$ on obtient

$$g_0.\ker \phi.g_0^{-1} = \ker \phi.g_0.g_0^{-1} = \ker \phi.$$

□

## 4. Le Theoreme de Lagrange

Le theoreme de Lagrange est l'un des resultats les plus importants de la theorie des groupes finis: il illustre le fait qu'en tant qu'espace un groupe est un objet "homogene": il a l'air d'etre le meme quelque soit l'endroit ou l'on se trouve.

THÉORÈME 2.5 (Theoreme de Lagrange). *Soit $(G, .)$ un groupe fini d'ordre $|G|$ alors pour tout sous-groupe $H \subset G$ l'ordre de $H$, $|H|$ divise l'ordre de $G$, $|G|$.*

PREUVE. Considerons les ensembles translates

$$g.H \subset G,\ g \in G.$$

Comme $e_G \in H$, on a $g \in g.H$ et donc

$$G = \bigcup_{g \in G} g.H$$

donc ces ensembles recouvrent entierement $G$.

On a

$$g.H \cap g'.H \neq \emptyset \Leftrightarrow g.H = g'.H.$$

En effet, supposons $g.H \cap g'.H \neq \emptyset$, il existe $h, h' \in H$ tels que $gh = g'h'$ et donc $g' = gh(h')^{-1} \in g.H$. On a donc

$$g'.H \subset g.H.H = g.H.$$

echangeant les roles de $g$ et $g'$ on obtient $gH = g'H$.

Comme les differents ensembles $g.H$ sont soit disjoints, soit egaux et que tout element de $G$ est dans un de ces ensembles (en effet $g = g.e_G \subset g.H$ car $e_G \subset H$ car $H$ est un sous-groupe), ils forment une partition de $G$: il existe un ensemble fini $\{g_i,\ i \in I\} \subset G$ tel que

$$G = \bigsqcup_i g_i.H.$$

on a donc

$$|G| = \sum_i |g_i.H|.$$

On remarque maintenant que tous ces ensembles ont le meme cardinal: en effet l'application (de translation par $g$)

$$t_g : \begin{array}{ccc} G & \mapsto & G \\ h & \mapsto & g.h \end{array}$$

est bijective et sa reciproque est la translation par $g^{-1}$

$$\begin{array}{ccc} G & \mapsto & G \\ h & \mapsto & g^{-1}.h \end{array}.$$

En particulier elle definit une bijection de $H$ vers son image $g.H$: on a donc pour tout $g \in G$

$$|g.H| = |H|$$

et ainsi

$$|G| = \sum_i |g_i.H| = \sum_i |H| = |I||H|.$$

□

Remarque 4.1. Le theoreme de Lagrange generalise le Theoreme noyau-image aux sous-groupes $H$ qui ne sont pas forcement distingues (par forcement de la forme $\ker \phi$.)

Remarque 4.2. Le quotient $|G|/|H|$ (qui est entier par le Theorem de Lagrange) a une interpretation concrete: il est egal aux nombres de sous-ensembles distincts de la forme $g.H,\ g \in G$.

Cette remarque conduit a la definition un peu plus generale suivante:

Définition 2.19. *Soit $G$ un groupe (pas forcement fini) et $H \subset G$ un sous-groupe; le nombre de sous-ensembles de $G$ de la forme $g.H$ pour $g \in G$ s'appelle l'indice de $H$ dans $G$ et se note $[G : H]$. Il n'est pas forcement fini.*

Exemple 4.1.
- Soit $N \geqslant 0$ un entier. L'indice de $N.\mathbb{Z}$ dans $\mathbb{Z}$ est $N$ si $N > 0$ et est infini si $N = 0$.
- Soit $M, N \geqslant 0$ des entiers. L'indice de $M.\mathbb{Z} \times N.\mathbb{Z}$ dans $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$ est $M.N$ si $M.N > 0$ et est infini si $M.N = 0$.
- soit $G$ un groupe fini et $\phi : G \to G'$ un morphisme, l'indice de $\ker \phi$ dans $G$ est egale a $|\operatorname{Im} \phi|$.
- L'indice de $(\mathbb{Z}, +)$ dans $(\mathbb{R}, +)$ est infini: le nombre de sous-ensembles de la forme $x + \mathbb{Z},\ x \in \mathbb{R}$ est en bijection avec l'interval $[0, 1[$.

## 5. Groupe engendre par un ensemble

DÉFINITION 2.1. *Soit $(G,\star)$ un groupe et $A\subset G$ un sous-ensemble de $G$. Il existe un sous-groupe de $G$ contenant $A$ qui est minimal pour cette propriete, c'est a dire que tout sous-groupe $H\subset G$ contenant $A$ contient egalement ce sous-groupe. On note ce sous-groupe $\langle A\rangle$ et on l'appelle le sous-groupe engendre par l'ensemble $A$.*

*Si $\langle A\rangle = G$, on dit que $A$ engendre $G$ ou que $A$ est un ensemble de generateur de $G$.*

**Preuve**: (de l'existence de $\langle A\rangle$) Soit $\mathcal{SG}_A = \{H \text{ sous-groupe de } G,\ A\subset H\}$ l'ensemble des sous-groupes de $G$ contenant $A$. Cet ensemble est non-vide car il contient $G$ et soit

$$\langle A\rangle = \bigcap_{H\in\mathcal{SG}_A} H$$

leur intersection. Alors $\langle A\rangle$ contient $A$ et si c'est un sous-groupe, il est clair que ce sera leplus petit. Montrons que c'est un sous-groupe: soient $g,g'\in\langle A\rangle$, alors

$$\forall H\in\mathcal{SG}_A,\ g,g'\in H$$

et (comme $H$ est un sous-groupe) $g.g'^{-1}\in H$ donc $g.g'^{-1}\in\langle A\rangle$. □

On va donner une seconde preuve de l'existence de $\langle A\rangle$ qui est plus constructive. On aura besoin des notations suivantes

**5.1. Notation multiplicative.** C'est celle qui s'applique la plupart du temps: soit $(G,\star)$ un groupe et $g\in G$ un element. On pose

$$g^0 := e_G$$

et pour $n\geqslant 1$ un entier on pose

$$g^n := g\star\cdots\star g\ (n \text{ fois})$$

et on pose

$$g^{-n} := g^{-1}\star\cdots\star g^{-1}\ (n \text{ fois}).$$

Cette notation est la notation *exponentielle* ou *multiplicative*. On a, pour tout $m,n\in\mathbb{Z}$, les formules suivantes

$$g^{-n} = (g^n)^{-1},\ g^m\star g^n = g^{m+n}. \tag{5.1}$$

Un element de la forme $g^n$ sera appelle une puissance de $g$ et on notera

$$g^{\mathbb{Z}} = \{g^n,\ n\in\mathbb{Z}\}\subset G$$

l'ensemble des puissances de $g$.

L'identite (5.1) montrer que

PROPOSITION 2.7. *L'application (exponentielle de base $g$) definie par*

$$\exp_g : \begin{array}{ccc}\mathbb{Z} & \mapsto & G\\ n & \mapsto & \exp_g(n)=g^n\end{array}$$

*est un morphisme de groupe. En particulier $g^{\mathbb{Z}} = \operatorname{Im}\exp_g$ est un sous-groupe de $G$.*

PROPOSITION 2.8. *On a l'egalite*

$$g^{\mathbb{Z}} = \langle\{g\}\rangle,$$

*le groupe $g^{\mathbb{Z}}$ est le sous-groupe engendre par le singleton $\{g\}$.*

**Preuve**: Comme $g^{\mathbb{Z}}$ est un groupe contenant $g$, on a $g^{\mathbb{Z}}\supset\langle\{g\}\rangle$ et comme $\langle\{g\}\rangle$ contient $g$ et que $\langle\{g\}\rangle$ est un groupe il contient $g^n$ pour tout entier $n$ et donc contient $g^{\mathbb{Z}}$. □

**5.2. Groupe engendre par un ensemble, bis.** La proposition precedente se generalise comme suit:

THÉORÈME 2.6. *Soit $(G,\star)$ un groupe et $A\subset G$ un sous-ensemble de $G$. Le sous-groupe engrendre par $A$ est l'ensemble des element de $G$ de la forme*

$$\langle A\rangle = \{g = a_1^{n_1}\star\cdots\star a_k^{n_k} \text{ avec } k\geqslant 1,\ a_1,\cdots,a_k\in A \text{ et } n_1,\cdots,n_k\in\mathbb{Z}\}-$$

*Autrement dit c'est l'ensemble de tous les produits possibles de puissance d'elements de $A$.*

On laisse la preuve de ce theoreme en exercice.

EXEMPLE 5.1. $\mathbb{Z}$ et $\mathbb{Z}/N\mathbb{Z}$ sont engendres par 1.

EXEMPLE 5.2. Considerons le groupe symetrique a $n$ elements

$$\mathfrak{S}_n = \mathfrak{S}_{\{,1,2,\cdots,n\}}.$$

Pour $a,b\in\{1,2,\cdots,n\}$ on note $(a,b)$ la permutation qui envoie $a$ sur $b$, $b$ sur $a$ et qui laisse fixe tous les autres elements de $\{1,2,\cdots,n\}$: si $a=b$, $(a,a)$ est l'identite et si $a\neq b$ on dit que $(a,b)$ est une transposition. Alors $\mathcal{S}_n$ est engendre par l'ensemble des $\frac{n(n-1)}{2}$ transpositions

$$\{(1,2),\ (1,3),\ \cdots\} = \{(a,b),\ 1\leqslant a<b\leqslant n\}.$$

(Le verifier a la main pour $n=3$).

EXEMPLE 5.3. Le groupe $(\mathbb{R},+)$ est engendre par $\mathbb{R}_{>0}$. Le groupe $(\mathbb{R}^2,+)$ est engendre par les sous-ensembles $\mathbb{R}_x := \mathbb{R}(1.0) = (\mathbb{R},0)$ et $\mathbb{R}_y := \mathbb{R}(0,1) = (0,\mathbb{R})$: en effet on a pour $(x,y)\in\mathbb{R}^2$,

$$(x,y) = (x,0)+(0,y).$$

EXEMPLE 5.4. Le groupe des isometries du plan est engendre par les translations et les symetries axiales d'axe passant par $(0,0)$: c'est connu depuis le gymnase mais on va le redemontrer en cours.

**5.3. Notation additive.** La notation exponentielle est utilisee pour un groupe general. Si le groupe est commutatif il peut etre commode d'utiliser la notation additive: si la loi de groupe commutatif est notee $\oplus$, l'element neutre $\mathbf{0}_G$ et l'oppose d'un element $g$ est note $\ominus g$, on a donc

$$g\oplus g' = g'\oplus g.$$

On pose alors

$$0.g = \mathbf{0}_G$$

et pour $n\geqslant 1$ un entier,

$$n.g := g\oplus\cdots\oplus g\ (n \text{ fois})$$

et on pose

$$(-n).g := (\ominus g)\oplus\cdots\oplus(\ominus g)\ (n \text{ fois})$$

et on a

$$(-n).g = \ominus(n.g),\ (m+n).g$$

Un element de la forme $n.g$ sera appelle un multiple de $g$ et on notera

$$\mathbb{Z}.g = \{n.g,\ n\in\mathbb{Z}\}\subset G$$

l'ensemble des multiples de $g$.

### 5.4. Ordre d'un element.

DÉFINITION 2.20. *Soit $g \in G$ et*

$$\langle g \rangle = g^{\mathbb{Z}} = \{g^n,\ n \in \mathbb{Z}\}$$

*le sous-groupe engendre par $G$.*

*Si $\langle g \rangle$ est fini, on dit que $g$ est d'ordre fini; l' ordre de $g$ est defini comme etant le cardinal de $\langle g \rangle$*

$$\mathrm{ord}(g) = |\langle g \rangle|.$$

*Sinon on dit que $g$ est d'ordre infini et on pose* $\mathrm{ord}(g) = \infty$.

Il resulte de cette definition et du theoreme de Lagrange que

PROPOSITION 2.9. *Soit $G$ un groupe fini d'ordre $|G| = N$, alors pour tout $g \in G$*

$$\mathrm{ord}(g) | N.$$

La proposition suivante est egalement tres utile.

PROPOSITION 2.10. *Si* $\mathrm{ord}(g) < \infty$ *est fini alors* $\mathrm{ord}(g)$ *est le plus petit entier $n > 0$ solution de l'equation*

$$g^n = e_G$$

*et tout entier (relatif) solution de cette equation est un multiple de* $\mathrm{ord}(g)$.

**Preuve**: L'ensemble des entier $n$ solution de l'enquation $g^n = e_G$ est le noyau du morphisme $\exp_g : \mathbb{Z} \to G$. Comme $G$ est fini et $\mathbb{Z}$ ne l'est pas ce morphisme n'est pas injectif et le noyau est $\neq \{0\}$. Soit $N$ le plus petit entier $N > 0$ dans le noyau ($N$ existe car le noyau possede au moins un element non-nul positif: si $N \neq 0$ appartient au noyau et est negatif alors $-N$ appartient au noyau et est positif). On a vu en exercice qu'est fait $\ker \exp_g = N\mathbb{Z}$ (ainsi l'ensemble des solution de l'equation est l'ensemble des multiples de $N$). Revoyons la preuve: Si $n \in \ker \exp_g$ par division euclidienne il existe $k \in \mathbb{Z}$ tel que $n - kN \in \{0, 1, \cdots, N-1\}$. On a

$$g^{n-kN} = g^n.(g^N)^k = e_G,\ n, N \in \ker \exp_g$$

donc $n - kN = 0$ car il est $\geqslant 0$et $< N$ et ne peut etre non-nul par minimalite de $N$. Montrons que $N \leqslant \mathrm{ord}(g) = |g^{\mathbb{Z}}|$: il suffit de montrer que

$$e_g = g^0, g = g^1, \cdots, g_{N-1}$$

sont tous distincts. Supposons le contraire : qu'il existe $0 \leqslant n < n' < N$ tels que

$$g^n = g^{n'}$$

alors

$$e_G = g^{n'-n}$$

mais comme $0 < n' - n < N$ cela contredit la minimalite de $N$. Montrons que

$$g^{\mathbb{Z}} = \{e_g = g^0, g = g^1, \cdots, g_{N-1}\}$$

ce qui montrera que $\mathrm{ord}(g) \leqslant N$ et donc l'egalite. Soit $g^n \in g^{\mathbb{Z}}$, par division euclidienne il existe $k \in \mathbb{Z}$ tel que $n' = n - kN \in [0, N-1]$ et

$$g^n = g^{n'+kN} = g^{n'}.(g^N)^k = g^{n'} \in \{e_g = g^0, g = g^1, \cdots, g_{N-1}\}.$$

□

COROLLAIRE 2.2. *soit $G$ un groupe fini. Pour tout $g \in G$ on a*

$$g^{|G|} = e_G.$$

**Preuve**: Exercice. □

### 5.5. Groupes cycliques.

DÉFINITION 2.21. *Un groupe $G$ engendre par un seul element $g \in G$, autrement dit,*

$$G = g^{\mathbb{Z}}$$

*est dit cyclique.*

PROPOSITION 2.11. *Soit $G$ un groupe cyclique alors ou bien $G$ est infini et il est isomorphe a $\mathbb{Z}$, ou bien $G$ est fini et il est isomorphe a $\mathbb{Z}/N\mathbb{Z}$ ou $N = |G| = \mathrm{ord}(g)$.*

PREUVE. Considerons le morphisme

$$\exp_g : \begin{array}{ccc} \mathbb{Z} & \mapsto & g^{\mathbb{Z}} = G \\ n & \mapsto & g^n \end{array}.$$

Comme $g^{\mathbb{Z}} = G$ ce morphisme est surjectif.

Considerons l'injectivite. Le sous-groupe $\ker \exp_g$ est de la forme $N\mathbb{Z}$ pour $N \geqslant 0$ (car tous les sous-groupes de $\mathbb{Z}$ sont de cette forme.)

Si $N = 0$, $\exp_g$ est injectif et est donc bijectif sur $G$. C'est un isomorphisme de groupe et donc $\mathbb{Z} \simeq G$.

Si $N > 0$ alors $N$ est la plus petite solution strictement positive de l'equation $g^n = e_G$. On a donc $N = \mathrm{ord}(g) = |G|$.

Considerons l'application

$$\exp_{g,N} : \begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \mapsto & G = g^{\mathbb{Z}} \\ r & \mapsto & g^r \end{array}.$$

Cette application est un morphisme de groupes: soient $r, r' \in \mathbb{Z}/N\mathbb{Z}$ et $r'' = r \oplus r'$ le reste de la division euclidienne de $r + r'$ par $N$, on a $r + r' = kN + r''$ et

$$g^r.g^{r'} = g^{r+r'} = g^{kN+r''} = g^{kN}.g^{r''} = g^{r''}$$

car $g^{kN} = e_G$. On a donc un morphisme de groupe. Par ailleurs comme $N$ est la plus petite solution strictement positive de l'equation $g^n = e_G$ donc si $g^r \neq e_G$ et si $0 \leqslant r < N$ cela force $r = 0$, on a donc $\ker \exp_{g,N} = \{0\}$. Le morphisme est injectif et surjectif car les deux groupes on le meme nombre d'elements et c'est donc un isomorphisme. □

PROPOSITION 2.12. *Tout sous-groupe d'un groupe cyclique est cyclique.*

PREUVE. Si $G \simeq \mathbb{Z}$ on a vu que les sous-groupes de $\mathbb{Z}$ sont de la forme $N\mathbb{Z}$ donc cyclique (engendre par $N$.1).

Supposons que $G$ est fini et soit $H \subset G$ un sous-groupe alors la preimage $\exp_g^{-1}(H) \subset \mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ donc engendre par un element $N$ et son image $H = \exp_g(\exp_g^{-1}(H))$ est engendre par $\exp_g(N)$. □

THÉORÈME 2.7. *Soit $G = \langle g \rangle$ une groupe cyclique d'ordre $N$; et $n \in \mathbb{Z}$ alors $g^n$ est d'ordre $N/(N, n)$. En particulier, si $(n, N) = 1$, $g^n$ est d'ordre $N$ et donc engendre $G$. Les generateurs de $G$ sont exactement les elements de la forme $g^n$ avec*

$$(n, N) = 1.$$

*Le nombre de ces generateurs est note $\varphi(N)$ et vaut*

$$\varphi(N) := |\{0 \leqslant n < N,\ (n, N) = 1\}|$$

*est appelle la fonction d'Euler de $N$.*

Preuve. Montrons que

$$(g^n)^{\mathbb{Z}} = (g^{(n,N)})^{\mathbb{Z}}.$$

On a $g^n = (g^{(n,N)})^{n/(n,N)}$ donc $g^n \in (g^{(n,N)})^{\mathbb{Z}}$ et

$$(g^n)^{\mathbb{Z}} \subset (g^{(n,N)})^{\mathbb{Z}}.$$

D'autre part, par l'identite de Bezout il existe $a, b \in \mathbb{Z}$ tels que

$$(n, N) = aN + bn$$

et donc

$$g^{(n,N)} = (g^N)^a.(g^n)^b = (g^n)^b \in (g^n)^{\mathbb{Z}};$$

on a donc l'inclusion inverse

$$(g^{(n,N)})^{\mathbb{Z}} \subset (g^n)^{\mathbb{Z}}$$

et donc egalite

$$(g^{(n,N)})^{\mathbb{Z}} = (g^n)^{\mathbb{Z}}$$

et donc $\mathrm{ord}(g^n) = \mathrm{ord}(g^{(n,N)})$. Notons $d$ cet ordre; c'est le plus petit entier $d > 0$ tel que

$$(g^{(n,N)})^d = g^{(n,N)d} = e_G.$$

En particulier $(n, N)d$ doit etre un multiple de $\mathrm{ord}(g) = N$ et donc (en divisant par $(n, N)$) $d$ est un multiple de $N/(n, N)$. D'autre part $g^{(n,N)(N/(n,N))} = g^N = e_G$ donc $N/(n, N)$ est un multiple de $d$. On a donc

$$\mathrm{ord}(g^n) = \mathrm{ord}(g^{(n,N)}) = N/(n, N).$$

En particulier, on a

$$\mathrm{ord}(g^n) = 1 \Longleftrightarrow (n, N) = 1.$$

Les generateur de $G$ sont donc exactement les elements de la forme $g^n$ avec $8n, N) = 1$. l'element $g^n$ engendre $G$; reciproquement si $g^n = G$ alors

$$\mathrm{ord}(g^n) = N/(N, n) = \mathrm{ord}(g) = N$$

et $(N, n) = 1$ . Maintenant si $d$ est un diviseur de $N$, alors $g^d$ et exactement d'ordre $N/d$ par la Proposition 2.10. □

Corollaire 2.3. *Soit $G$ cyclique d'ordre $N$ et engendre par $g$. L'application*

$$d|N \mapsto (g^d)^{\mathbb{Z}}$$

*est une bijection entre les diviseurs de $N$ et les sous-groupes de $G$; on a la relation*

$$|(g^d)^{\mathbb{Z}}| = \mathrm{ord}(g^d) = N/d.$$

*Le sous-groupe correspondant a $d|N$ est d'ordre $N/d$ et c'est unique sous-groupe d'ordre $N/d$ de $G$.*

*En particulier, deux elements de meme ordre engendrent le meme sous-groupe.*

**Preuve**: Soit $d$ divisant $N$. Comme $g^d$ engendre un groupe d'ordre $N/(d,N) = N/d$ deux diviseurs distincts produisent des sous-groupes d'ordre distincts donc differents. L'application est donc injective.

Montrons qu'elle est surjective.

Soit $H \subset G$ un sous-groupe de $G$. Comme $G$ est cyclique, $H$ est cyclique. Soit $g^n$ un generateur de $H$ alors on a vu que $\mathrm{ord}(g^n) = \mathrm{ord}(g^{(n,N)})$ et que

$$H = (g^n)^{\mathbb{Z}} = (g^{(n,N)})^{\mathbb{Z}}.$$

Ainsi $H = (g^{(n,N)})^{\mathbb{Z}}$ et l'application est surjective donc bijective.

Deux elements de meme ordre engendrent des sous-groupes de meme ordre; notons $N/d$ cet ordre (il divise $N$ donc peut s'ecrire sous cette forme). Les deux groupes sont egaux et correspondent a $d$ par la bijection precedente.

□

**5.6. Le cas des racines de l'unite.** Soient $N \geqslant 1$ un entier et

$$\mu_N = \{z \in \mathbb{C}^\times,\ z^N = 1\}$$

l'ensemble des racines $N$-iemes de l'unite (l'ensemble des racines du polynome $X^N - 1$ dans le corps des nombres complexes $\mathbb{C}$.

PROPOSITION 2.13. *L'ensemble $\mu_N$ muni de la multiplication est un sous-groupe du groupe multiplicatif des nombres complexes non-nuls $(\mathbb{C}^\times, \times)$. Ce groupe est cyclique d'ordre $N$ et en particulier isomorphe a $(\mathbb{Z}/N\mathbb{Z}, \oplus)$.*

PREUVE. L'application

$$\cdot^N : \begin{array}{ccc} \mathbb{C}^\times & \mapsto & \mathbb{C}^\times \\ z & \mapsto & z^N \end{array}$$

est un morphisme de groupes et $\mu_N$ est son noyau, c'est donc un sous-groupe (on peut egalement le verifier directement). Le fait que $\mu_N$ est d'ordre $N$ et est cyclique est facile si on admet les proprietes de l'exponentielle complexe: on "sait" alors

$$\mu_N = \{\exp(2\pi i \frac{n}{N}) = \exp(2\pi i \frac{1}{N})^n,\ 0 \leqslant n \leqslant N-1\}.$$

Ce qui montrer que $\mu_N$ est cyclique engendre par $\exp(2\pi i \frac{1}{N})$. D'autre part, on sait que

$$\forall x, x \in \mathbb{R},\ \exp(2\pi i x) = \exp(2\pi i x') \Longleftrightarrow x - x' \in \mathbb{Z}$$

(ie. le noyau du morphisme $\exp(2\pi i \cdot) : \mathbb{R} \to \mathbb{C}^\times$ est $\mathbb{Z}$); cela montre que $\mu_N$ est d'ordre $N$.

□On redemontrera plus tard (sans supposer l'existence de l'exponentielle complexe) que ce groupe est cyclique comme consequence d'un resulat general sur les corps.

Rappellons egalement que $\mu_N$ est contenu dans le cercle unite, ie l'ensemble des nombres complexe de module 1:

$$\mu_N \subset \mathbb{C}^1 = \{z \in \mathbb{C}^\times,\ |z| = 1\}.$$

En effet

$$\forall z \in \mu^N,\ 1 = |z^N| = |z|^N \Longrightarrow |z| = 1.$$

Le fait que $\mu_N$ soit isomorphe a $(\mathbb{Z}/N\mathbb{Z}, \oplus)$ permet de representer $(\mathbb{Z}/N\mathbb{Z}, \oplus)$ et donc tout groupe cyclique comme un ensemble de points sur le cercle unite.

Ainsi pour $N = 8$ la figure 5.6 est une representation graphique d'un groupe cyclique a 8 elements

$$G = \langle g \rangle = \{e_g, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8 = e_g\}.$$

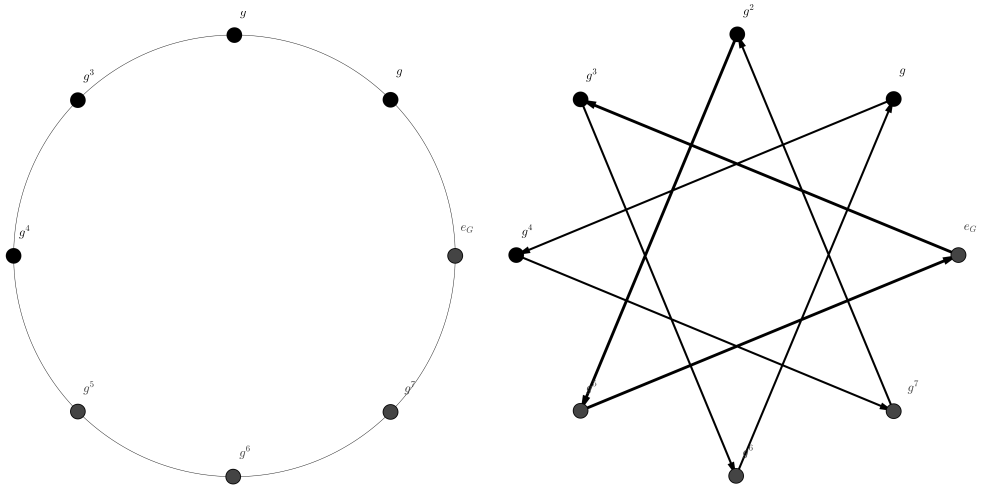


FIGURE 6. Le groupe cyclique $\langle g \rangle$ a 8 elements avec $g$ et avec $g^3$ comme generateurs

Le generateur $g$ correspondant a $\exp(2\pi i/8)$. Le deuxieme figure represente le meme groupe mais on met ici en valeur un autre generateur $g^3$. On represente les elements du groupe sous la forme

$$\{(g^3)^0 = e_G, g^3, (g^3)^2 = g^6, (g^3)^3 = g, (g^3)^4 = g^4,$$
$$(g^3)^5 = g^7, (g^3)^6 = g^{10} = g^2, (g^3)^7 = g^5, (g^3)^8 = g^8 = e_g\}.$$

Les lignes sur le dessins relient un element $g' = n$ aux elements $g'.g^3 = g^{n+3}$ et $g'.(g^3)^{-1} = g^{n-3}$.

CHAPITRE 3

# Isometries du plan

## 1. Plan vectoriel, affine, longueur et distance euclidienne

Le plan reel est le produit

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y),\ x, y \in \mathbb{R}\}$$

forme de paires de nombres reels. Etant donne un element $(x, y)$ de $\mathbb{R}^2$, $x$ et $y$ sont les coordonnes de cet element. L'element $(0, 0)$ est note $\mathbf{0}$ et est appele l'origine. Le sous-ensemble

$$\mathbb{R}_x := \{(x, 0),\ x \in \mathbb{R}\}$$

est appele axe des abscisses et l'ensemble

$$\mathbb{R}_y := \{(0, y),\ y \in \mathbb{R}\}$$

est appele axe des ordonnees.

**1.1. Espace vectoriel vs. espace affine.** Le plan $\mathbb{R}^2$ muni de l'addition

$$(x, y) + (x', y') = (x + x', y + y')$$

est un groupe commutatif dont l'element neutre est l'origine $\mathbf{0}$; avec la multiplication par les scalaires definie par

$$\lambda \in \mathbb{R},\ (x, y) \in \mathbb{R}^2,\ \lambda.(x, y) = (\lambda x, \lambda y)$$

c'est meme un espace vectoriel de dimension 2. Notons $\mathbf{e}_1 = (1, 0)$ et $\mathbf{e}_2 = (0, 1)$. L'ensemble $\{\mathbf{e}_1, \mathbf{e}_2\}$ est la *base canonique* de $\mathbb{R}^2$: tout element $(x, y) \in \mathbb{R}^2$ s'ecrit comme combinaison lineaire

$$(x, y) = x\mathbf{e}_1 + y\mathbf{e}_2$$

et cette ecriture est unique.

$\mathbb{R}^2$ *vu comme groupe de translation.* Etant donne un vecteur $(u, v)$ de $\mathbb{R}^2$, on associe a un tel vecteur une application (dite de translation) $t_{(u,v)} : \mathbb{R}^2 \mapsto \mathbb{R}^2$ definie par

$$t_{(u,v)} : P = (x, y) \mapsto P + (u, v) = (x + u, y + v).$$

L'application $t_{(u,v)}$ est une bijection de $\mathbb{R}^2$ sur lui-meme dont l'application reciproque $t^{-1}_{(u,v)}$ est la translation de vecteur oppose $t_{(-u,-v)}$, en effet pour tout point $P$

$$t_{(u,v)} \circ t_{(-u,-v)}(P) = (u, v) + ((-u, -v) + P) = (u, v) - (u, v) + P = P = \mathrm{Id}_{\mathbb{R}^2}(P)$$

et

$$t_{(-u,-v)} \circ t_{(u,v)}(P) = (-u, -v) + ((u, v) + P) = -(u, v) + (u, v) + P = P = \mathrm{Id}_{\mathbb{R}^2}(P).$$

Plus generalement on a

PROPOSITION 3.1. *L'application*

$$t : \begin{array}{ccc} (\mathbb{R}^2,+) & \mapsto & (\mathrm{Bij}(\mathbb{R}^2),\circ) \\ (u,v) & \mapsto & t_{(u,v)} \end{array}$$

*est un morphisme de groupe injectif.*

PREUVE. c'est un cas particulier de l'exercice 2.6 du chapitre precedent. Par le critere de morphisme de groupe: nous devons montrer que

$$t_{(u,v)} \circ t_{(u',v')} = t_{(u+u',v+v')}$$

Pour tout $(u,v),(u',v') \in \mathbb{R}^2$ et tout $P \in \mathbb{R}^2$ on a

$t_{(u,v)} \circ t_{(u',v')}(P) = (u,v)+((u',v')+P) = (u,v)+(u',v')+P = (u+u',v+v')+P = t_{(u+u',v+v')}(P)$.

Montrons que $t$ est injective: il suffit de montrer que $\ker(t) = \{\mathbf{0}\}$; on a $\mathbf{0} \in \ker(t)$. Soit $(u,v) \in \ker(t)$ alors pour tout $P \in \mathbb{R}^2$, on a

$$t_{(u,v)}(P) = (u,v) + P = \mathrm{Id}_{\mathbb{R}^2}(P) = P$$

mais prenant $P = \mathbf{0}$ on obtient

$$(u,v) + \mathbf{0} = (u,v) = \mathbf{0}.$$

□

DÉFINITION 3.1. *L'image de $\mathbb{R}^2$ par le morphisme $t$, est appele groupe des translations du plan et est note*

$$T(\mathbb{R}^2) = \{t_{(u,v)},\ (u,v) \in \mathbb{R}^2\} \subset \mathrm{Bij}(\mathbb{R}^2).$$

REMARQUE 1.1. Cette proposition montre que $\mathbb{R}^2$ peut se realiser comme un sous-groupe de transformations du plan. C'est en fait un cas particulier d'un phenomene completement general: tout groupe peut etre realise comme un sous-groupe de son groupe de bijections. C'est *l'action* d'un groupe sur lui-meme par translations (cf. le chapitre sur les actions de groupes).

On a la proposition elementaire suivante:

PROPOSITION 3.2. *Pour tout $P$ et $Q \in \mathbb{R}^2$, il existe un unique $(u,v) \in \mathbb{R}^2$ tel que*

$$t_{(u,v)}(P) = Q.$$

PREUVE. Notons $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, l'element $(u,v)$ recherche est donne par

$$Q - P = (x_Q - x_P, y_Q - y_P).$$

□

La proposition precedente s'exprime de maniere un peu pedante en disant que $\mathbb{R}^2$ est *un espace principal homogene sous l'action de $\mathbb{R}^2$ par translations.* Ce type de vocabulaire n'est pas tres important pour l'instant mais on le retrouvera quand on discutera des actions de groupes.

Quoiqu'il en soit on peut voir $\mathbb{R}^2$ de deux manieres: soit comme un ensemble (un espace homogene sur lequel le groupe $(\mathbb{R}^2,+)$ agit par translation) et on parlera de *plan affine* qu'on notera quelquefois $\mathbb{A}^2$; soit comme groupe de translaions agissant sur l'ensemble $\mathbb{R}^2$.

Ainsi notera les elements de $\mathbb{R}^2$ soit, sous forme de points $P = (x_P, y_P)$ (si on veut mettre en avant l'aspect espace homogene), soit sous forme de vecteurs $\vec{v} = (x_{\vec{v}}, y_{\vec{v}})$ (si on veut mettre en avant l'aspect translation).

DÉFINITION 3.2. *Etant donnes deux point $P, Q \in \mathbb{R}^2$ on notera*

$$\vec{PQ} = Q - P = (x_Q - x_P, y_Q - y_P),$$

*qui est l'unique vecteur qui envoie $P$ sur $Q$ par translation.*

Ainsi le point $P$ se note $\vec{\mathbf{0}P}$ sous forme vectorielle. Cette distinction de points de vue est assez subtile et pas indispensable pour la suite: dans la pratique on utilisera l'une ou l'autre des deux notations de maniere interchangeable.

### 1.2. Droites affines et vectorielles.

DÉFINITION 3.3. *Etant donne $\vec{v} = (\alpha, \beta) \neq (0, 0)$ et $P = (x_P, y_P) \in \mathbb{R}^2$,*

- *la droite (vectorielle) de vecteur $\vec{v}$ est le sous-ensemble*

$$\mathcal{D}(\mathbf{0}, \vec{v}) = \mathbb{R}\vec{v} = \{t.\vec{v} = (t\alpha, t\beta),\ t \in \mathbb{R}\} \subset \mathbb{R}^2.$$

  *C'est un groupe (et meme un sous-espace vectoriel de dimension 1) de $\mathbb{R}^2$. C'est la droite vectorielle de direction $\vec{v}$.*
- *Une droite affine $D$ est l'ensemble des images d'un point $P$ par les translations d'une droite vectorielle: c'est un sous-ensemble de $\mathbb{R}^2$ de la forme*

$$\mathcal{D}(P, \vec{v}) = P + \mathbb{R}\vec{v} = \{P + t.\vec{v} = (x_P + t\alpha, y_P + t\beta),\ t \in \mathbb{R}\} \subset \mathbb{R}^2.$$

  *La droite $\mathcal{D}(P, \vec{v})$ est la droite affine passant par le point $P$ et de direction $\vec{v}$.*

Soit $\vec{v} = (\alpha, \beta)$ et $P = (x_P, y_P) \in \mathbb{R}^2$ , la droite $D = D(P, \vec{v})$ en tant que sous-ensemble de $\mathbb{R}^2$ peut etre representee soit

- Soit forme *parametrique* comme ci-dessus

$$\{P + t.\vec{v} = (x_P + t\alpha, y_P + t\beta),\ t \in \mathbb{R}\},$$

- soit sous la forme d'une equation *cartesienne*: $D = D(P, \vec{v})$ est l'ensemble des solutions $(x, y)$ de l'equation

$$ax + by = c$$

  avec

$$a = \beta,\ b = -\alpha,\ c = \beta x_P - \alpha y_P.$$

REMARQUE 1.2. Notons que ces representations ne sont pas uniques: pour tout $P' \in \mathcal{D}(P, \vec{v})$ et tout $\vec{v}' \in \mathcal{D}(\mathbf{0}, \vec{v}) - \{\mathbf{0}\}$ on a

$$\mathcal{D}(P, \vec{v}) = \mathcal{D}(P', \vec{v}').$$

Rappelons egalement les definitions et resultats de base concernant les droites

PROPOSITION 3.3. *Etant donnes deux points distincts $P \neq Q$ il existe une unique droite affine passant par $P$ et $Q$,*

$$(PQ) := \mathcal{D}(P, \vec{PQ}) = \{(x_P + t(x_Q - x_P), y_P + t(y_Q - y_P)),\ t \in \mathbb{R}\} \subset \mathbb{R}^2.$$

*Etant donnes deux droites $D = D(P, \vec{v}), D' = (P', \vec{v}')$ alors l'intersection $D \cap D'$ est*

- *soit reduite a un point,*
- *soit l'ensemble vide,*
- *soit egale a $D = D'$.*

*Dans le premier cas les droites sont dites secantes et ce cas a lieu si et seulement si $\vec{v}$ et $\vec{v}'$ ne sont pas multiples l'un de l'autre ($\vec{v}' \neq \lambda.\vec{v}$ pour tout $\lambda \in \mathbb{R}^\times$) ; dans le deuxieme cas les droites sont dites paralleles et dans le troisieme elles sont confondues.*

DÉFINITION 3.4. *Trois points $P, Q, R \in \mathbb{R}^2$ sont alignes si ils font partie d'une meme droite affine ou de maniere equivalente si $\vec{PR}$ et $\vec{QR}$ font partie de la meme droite vectorielle.*

### 1.3. La distance euclidienne.

DÉFINITION 3.5. *La longueur euclidienne d'un vecteur $\vec{u} = (x, y)$ est donnee par*

$$\|\vec{u}\| = \|(x, y)\| = (x^2 + y^2)^{1/2}.$$

*La distance euclidienne dans le plan affine $\mathbb{R}^2$ est la fonction*

$$d_2(\cdot, \cdot) : \mathbb{R}^2 \times \mathbb{R}^2 \mapsto \mathbb{R}_{\geqslant 0}$$

*donnee pour $P = (x, y)$ et $Q = (x', y')$ par*

$$d_2(P, Q) = ((x - x')^2 + (y - y')^2)^{1/2} = \|\vec{PQ}\|.$$

THÉORÈME 3.1. *La fonction longueur (resp. distance) a les proprietes suivantes*

- *Separation des points: pour tout $\vec{u} \in \mathbb{R}^2$, $P, Q \in \mathbb{R}^2$*
$$\|\vec{u}\| = 0 \Longleftrightarrow \vec{u} = \mathbf{0},\ d_2(P, Q) = 0 \Longleftrightarrow P = Q.$$
- *Symetrie: pour tout $\vec{u} \in \mathbb{R}^2$, $P, Q \in \mathbb{R}^2$*
-
$$\| - \vec{u}\| = \{\vec{u}\},\ d_2(P, Q) = d_2(Q, P).$$
- *Inegalite du triangle: our tout $\vec{u}, \vec{v} \in \mathbb{R}^2$, $P, Q, R \in \mathbb{R}^2$*
$$\|\vec{u} + \vec{v}\| \leqslant \|\vec{u}\| + \|\vec{v}\|,\ d_2(P, R) \leqslant d_2(P, Q) + d_2(Q, R)$$
*avec egalite si et seulement $\vec{u}$ et $\vec{v}$ sont proportionels et que le facteur de proportionalite est $\geqslant 0$/ssi $P, Q, R$ sont alignes (cad $\vec{PQ}$ et $\vec{PR}$ sont proportionels) et $Q$ est "entre" $P$ et $R$.*
- *Homogeneite:*
$$\|\lambda\vec{u}\| = |\lambda|\|\vec{u}\|,\ d_2(\lambda.P, \lambda.Q) = |\lambda| d_2(P, Q)$$
*avec $\lambda.P$ l'image de $P$ par l'homothetie de centre $\mathbf{0}$ et de rapport $\lambda$:*
$$[\times\lambda] : \begin{array}{ccc} \mathbb{R}^2 & \mapsto & \mathbb{R}^2 \\ (x, y) & \mapsto & (\lambda x, \lambda y) \end{array}.$$

Les trois premieres proprietes sont constitutives de ce qu'on appelle une distance:

DÉFINITION 3.6. *Soit $X$ un ensemble. Une distance est une application*

$$d(\cdot, \cdot) : \begin{array}{ccc} X \times X & \mapsto & \mathbb{R}_{\geqslant 0} \\ (P, Q) & \mapsto & d(P, Q) \end{array}$$

*qui verifie les proprietes suivantes*

- *Separation des points: pour tout $P, Q \in X$,*
$$d(P, Q) = 0 \Longleftrightarrow P = Q.$$
- *Symetrie: pour tout $P, Q \in X$,*
$$d(P, Q) = d(Q, P).$$

– *Inegalite du triangle: pour tout $P, Q, R \in X$,*

$$d(P,R) \leqslant d(P,Q) + d(Q,R).$$

EXEMPLE 1.1. Soit $X$ un ensemble; la distance triviale sur $X$ est l'application definie par

$$d_X(P,Q) = \begin{cases} 1 & \text{si } P \neq Q \\ 0 & \text{si } P = Q. \end{cases}$$

Elle permet seulement de mesurer si deux elements sont egaux ou pas.

REMARQUE 1.3. La notion generale de distance est tres importante: elle permet de mesurer si deux elements d'un ensemble sont "proches" l'un de l'autre ou non; elle est utilisee pour des enembles tres generaux: ainsi on peut definir une notion de distance sur des espaces de fonctions abstraits. Dans ce cours on ne parlera que de la distance euclidienne.

Cette notion permet d'introduire de nouveaux lieux geometriques:

DÉFINITION 3.7. *Etant donne $P \in \mathbb{R}^2$ et $r \geqslant 0$, le cercle de centre $P$ et de rayon $r$ est l'ensemble des points du plan a distance $r$ de $P$*

$$\mathcal{C}(P,r) = \{Q \in \mathbb{R}^2,\ d(P,Q) = r\} = \{(x,y) \in \mathbb{R}^2,\ (x-x_P)^2 + (y-y_P)^2 = r^2\}.$$

**Produit scalaire euclidien.** Dans le theoreme **??**ci-dessus, le seul point non evident est de montrer l'inegalite du triangle. Elle peut etre verifiee "a la main" mais il est plus utile (notamment en vue de generalisations) de la demontrer en introduisant une structure supplementaire:

DÉFINITION 3.8. *Le produit scalaire euclidien de deux vecteurs $\vec{u} = (x,y)$, $\vec{v} = (x',y')$ est definit par*

$$\langle \vec{u}, \vec{v} \rangle = \vec{u}.\vec{v} := xx' + yy'.$$

*On a donc*

$$\langle \vec{u}, \vec{u} \rangle = \|\vec{u}\|^2.$$

Rappelons que

PROPOSITION 3.4. *le produit scalaire euclidien a les proprietes suivantes:*

– *symetrique:*

$$\forall \vec{u}, \vec{v},\ \langle \vec{u}, \vec{v} \rangle = \langle \vec{v}, \vec{u} \rangle,$$

– *bilineaire:*

$$\forall \vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^2,\ \lambda \in \mathbb{R},\ \langle \lambda \vec{u} + \vec{v}, \vec{w} \rangle = \lambda \langle \vec{u}, \vec{w} \rangle + \langle \vec{v}, \vec{w} \rangle$$

$$\langle \vec{w}, \lambda \vec{u} + \vec{v} \rangle = \lambda \langle \vec{w}, \vec{u} \rangle + \langle \vec{w}, \vec{v} \rangle.$$

– *defini-positif:*

$$\forall \vec{u} \in \mathbb{R}^2,\ \langle \vec{u}.\vec{u} \rangle \geqslant 0$$

*et*

$$\langle \vec{u}.\vec{u} \rangle = 0 \iff \vec{u} = \mathbf{0}.$$

Prenant $\lambda = \pm 1$, on en deduit la relation

$$\|\vec{u} \pm \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2 \pm 2\langle \vec{u}, \vec{v}\rangle \tag{1.1}$$

On obtient donc

$$\langle \vec{u}, \vec{v}\rangle = \pm\frac{1}{2}(\|\vec{u} \pm \vec{v}\|^2 - \|\vec{u}\|^2 - \|\vec{v}\|^2)$$

et combinant les cas + et − de ces deux identites, on a

$$\langle \vec{u}, \vec{v}\rangle = \frac{1}{4}(\|\vec{u} + \vec{v}\|^2 - \|\vec{u} - \vec{v}\|^2). \tag{1.2}$$

Ainsi le produit scalaire $\langle \cdot, \cdot \rangle$ peut etre retrouve a partir de la fonction longueur $\| \cdot \|^2$.

On va maintenant montrer l'inegalite du triangle. Pour cela on aura besoin de l'inegalite fondamentale:

PROPOSITION 3.5 (Inegalite de Cauchy-Schwarz). *On a*

$$|\langle \vec{u}, \vec{v}\rangle| \leqslant \|\vec{u}\|\|\vec{v}\|$$

*avec egalite si et seulement si $\vec{u}$ et $\vec{v}$ sont proportionels: ie. si $\vec{u} \neq \mathbf{0}$ il existe $\lambda \in \mathbb{R}$ tel que*

$$\vec{v} = (x', y') = \lambda\vec{u} = (\lambda x, \lambda y).$$

*(si $\vec{u} = \mathbf{0}$ alors $\vec{u} = \mathbf{0} = 0.\vec{v}$ est colineaire a $\vec{v}$).*

PREUVE. On peut supposer $\vec{u} \neq 0$ (sinon l'inegalite est verifiee trivialement). Considerons la fonction

$$P : \lambda \in \mathbb{R} \mapsto \|\lambda\vec{u} + \vec{v}\|^2 = \|\lambda\vec{u}\|^2 + \|\vec{v}\|^2 + 2\langle \lambda\vec{u}, \vec{v}\rangle = \lambda^2\|\vec{u}\|^2 + 2\lambda\langle \vec{u}, \vec{v}\rangle + \|\vec{v}\|^2.$$

C'est un polynome a coefficients reels de degree 2 et a valeurs positives ou nulles (car c'est une longueur). La derivee de $P$, $P'(\lambda) = 2\lambda\|\vec{u}\|^2 + 2\langle \vec{u}, \vec{v}\rangle$ s'annule en

$$\lambda_0 = -\langle \vec{u}, \vec{v}\rangle/\|\vec{u}\|^2$$

et

$$P(\lambda_0) = (\langle \vec{u}, \vec{v}\rangle)^2 - 2(\langle \vec{u}, \vec{v}\rangle)^2/\|\vec{u}\|^2 + \|\vec{v}\|^2 = -(\langle \vec{v}, \vec{u}\rangle)^2/\|\vec{u}\|^2 + \|\vec{v}\|^2 \geqslant 0$$

d'ou l'inegalité $\langle \vec{u}, \vec{v}\rangle^2 \leqslant \|\vec{u}\|^2\|\vec{v}\|^2$. En cas d'egalité

$$P(\lambda_0) = \|\lambda_0\vec{v} + \vec{u}\|^2 = 0 \Rightarrow \vec{u} = -\lambda_0\vec{v}.$$

□

PREUVE. (de l'inegalite du triangle): soient $\vec{u}, \vec{v} \in \mathbb{R}^2$, on a par l'inegalite de Cauchy-Schwarz

$$\|\vec{u} + \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2\langle \vec{u}, \vec{v}\rangle \leqslant \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2\|\vec{u}\|\|\vec{v}\| = (\|\vec{u}\| + \|\vec{v}\|)^2.$$

□

### 1.4. Decomposition dans une base orthogonale.

DÉFINITION 3.9. *Etant donne $\vec{u}, \vec{v} \in \mathbb{R}^2$, si $\langle \vec{u}, \vec{v} \rangle = 0$, on dit que $\vec{u}$ et $\vec{v}$ sont orthogonaux ou perpendiculaires*

PROPOSITION 3.6. *Soient $\vec{u}, \vec{v} \in \mathbb{R}^2$ deux vecteurs perpendiculaires tous deux non-nuls, alors tout vecteur $\vec{w}$ s'ecrit de maniere unique sous la forme d'une combinaison lineaire*

$$\vec{w} = \lambda \vec{u} + \mu \vec{v}$$

*avec $\lambda, \mu \in \mathbb{R}$. En particulier $\mathbb{R}^2$ en tant que groupe additif est engendre par la reunion des deux droites vectorielles $\mathbb{R}.\vec{u} \cup \mathbb{R}.\vec{v}$.*

PREUVE. Supposons que $\vec{w}$ soit de la forme ci-dessus: on a necessairement (par linearite et orthogonalite)

$$\langle \vec{u}, \vec{w} \rangle = \langle \vec{u}, \lambda \vec{u} + \mu \vec{v} \rangle = \lambda \langle \vec{u}, \vec{u} \rangle + \mu \langle \vec{u}, \vec{v} \rangle = \lambda \|\vec{u}\|^2$$
$$\langle \vec{v}, \vec{w} \rangle = \langle \vec{v}, \lambda \vec{u} + \mu \vec{v} \rangle = \lambda \langle \vec{v}, \vec{u} \rangle + \mu \langle \vec{v}, \vec{v} \rangle = \mu \|\vec{v}\|^2.$$

Ainsi si $\vec{w} = \lambda \vec{u} + \mu \vec{v}$, $\lambda$ et $\mu$ sont uniquement definis. En particulier si

$$\lambda \vec{u} + \mu \vec{v} = \mathbf{0}$$

alors $\lambda = \mu = 0$: dans la terminologie de l'algebre lineaire la famille $\{\vec{u}, \vec{v}\}$ est libre.

Etant donne $\vec{w} = (x, y)$ montrons que $\vec{w}$ est de la forme $\vec{w} = \lambda \vec{u} + \mu \vec{v}$: posons $\vec{u} = (a, b)$, $\vec{v} = (c, d)$, on doit resoudre le systeme lineaire

$$\lambda a + \mu c = x$$
$$\lambda b + \mu d = y$$

On a $\langle \vec{u}, \vec{v} \rangle = ac + bd = 0$ de sorte que multipliant la premiere ligne par $c$ et la seconde par $d$ et additionnant on obtient

$$\mu(c^2 + d^2) = cx + dy$$

et de meme multipliant la premiere ligne par $a$ et la seconde par $b$ et additionnant on obtient

$$\lambda(a^2 + b^2) = ax + by$$

ce qui determine $\lambda$ et $\mu$ car $a^2 + b^2 = \|\vec{u}\|^2 \neq 0$ et $c^2 + d^2 = \|\vec{v}\|^2 \neq 0$.

□

DÉFINITION 3.10. *Si $\vec{u}, \vec{v}$ sont deux vecteurs orthogonaux et non-nuls, la paire $(\vec{u}, \vec{v})$ forme une base orthogonale (BO) de $\mathbb{R}^2$. Si de plus*

$$\|\vec{u}\| = \|\vec{v}\| = 1,$$

*on dit que $(\vec{u}, \vec{v})$ forme une base orthonormee (BON) de $\mathbb{R}^2$.*

*Pour tout $\vec{w} \in \mathbb{R}^2$ on a alors*

$$\vec{w} = \frac{\langle \vec{w}, \vec{u} \rangle}{\|\vec{u}\|^2} \vec{u} + \frac{\langle \vec{w}, \vec{v} \rangle}{\|\vec{v}\|^2} \vec{v} \quad \textit{si } (\vec{u}, \vec{v}) \textit{ est orthogonale et}$$
$$\vec{w} = \langle \vec{w}, \vec{u} \rangle \vec{u} + \langle \vec{w}, \vec{v} \rangle \vec{v} \quad \textit{si } (\vec{u}, \vec{v}) \textit{ est orthonormee.} \tag{1.3}$$

*Les nombres*

$$\lambda = \frac{\langle \vec{w}, \vec{u} \rangle}{\|\vec{u}\|^2}, \ \mu = \frac{\langle \vec{w}, \vec{v} \rangle}{\|\vec{v}\|^2}$$

*sont les composantes du vecteur $\vec{w}$ dans la base $(\vec{u}, \vec{v})$ (ou encore les composantes du vecteur $\vec{w}$ le long des droites perpendiculaires $(\vec{u})$, $(\vec{v})$)*

EXEMPLE 1.2. La base canonique

$$\mathcal{B}_0 := (\mathbf{e}_1, \mathbf{e}_2),\ \mathbf{e}_1 = (1,0),\ \mathbf{e}_2 = (0,1)$$

est orthonormee.

## 2. La structure du groupe des isometries

Dans cette section on etudie plus precisement la structure de l'ensemble des isometries du plan euclidien, c'est a dire les applications qui preservent la distance euclidienne:

$$\phi : \mathbb{R}^2 \mapsto \mathbb{R}^2 \text{ telles que } \forall P, Q \in \mathbb{R}^2,\ d(\phi(P), \phi(Q)) = d(P, Q).$$

On note

$$\mathrm{Isom}(\mathbb{R}^2) = \{\phi : \mathbb{R}^2 \mapsto \mathbb{R}^2 \text{ telles que } \forall P, Q \in \mathbb{R}^2,\ d(\phi(P), \phi(Q)) = d(P, Q)\}$$

l'ensemble des isometries du plan. Cet ensemble est non-vide: $\mathrm{Id}_{\mathbb{R}^2}$ est une isometrie. Une autre famille importante est l'ensemble des translations:

LEMME 3.1. *Soit $\vec{u} \in \mathbb{R}^2$ un vecteur et $t_{\vec{u}}$ la translation correspondante alors $t_{\vec{u}}$ est une isometrie*

**Preuve**: Soit $P = (x_P, y_P),\ Q = (x_Q, y_Q)$ deux points, on a

$$d(t_{\vec{u}}(P), t_{\vec{u}}(Q)) = d(P+\vec{u}, Q+\vec{u}) = \|\overrightarrow{P + \vec{u}Q + \vec{u}}\| = \|Q+\vec{u}-(P+\vec{u})\| = \|Q-P\| = d(P, Q).$$

□

Mais il existe d'autres isometries et on va les determiner toutes. Pour cela on introduit le sous-ensemble

$$\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}} = \{\phi \in \mathrm{Isom}(\mathbb{R}^2,\ \phi(\mathbf{0}) = \mathbf{0})\},$$

des isometries qui fixent le vecteur nul $\mathbf{0}$. On va montrer le

THÉORÈME 3.2. *Les ensembles $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$, $T(\mathbb{R}^2)$ et $\mathrm{Isom}(\mathbb{R}^2)$ sont contenus dans $\mathrm{Bij}(\mathbb{R}^2)$ et en forment des sous-groupes. Le sous-groupe $T(\mathbb{R}^2)$ est distingue et $\mathrm{Isom}(\mathbb{R}^2)$ est egal au produit de ses deux sous-groupes,*

$$\mathrm{Isom}(\mathbb{R}^2) = T(\mathbb{R}^2) \circ \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}.$$

*Plus precisement, toute isometrie $\phi$ se decompose de maniere unique sous la forme*

$$\phi = t \circ \phi_0,\ t = t_{\phi(\mathbf{0})} \in T(\mathbb{R}^2),\ \phi_0 = t_{-\phi(\mathbf{0})} \circ \phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}.$$

*L'isometrie $\phi_0$ s'appelle la partie lineaire de l'isometrie $\phi$.*

La preuve commence par le resultat non-moins important suivant.

THÉORÈME 3.3. *Soit $\phi$ une isometrie fixant l'origine $\mathbf{0}$; alors $\phi$ est lineaire: pour tout $\vec{u}$, $\vec{v}$ et $\lambda \in \mathbb{R}$ on a*

$$\phi(\lambda\vec{u} + \vec{v}) = \lambda\phi(\vec{u}) + \phi(\vec{v}).$$

*De plus $\phi$ est bijective et sa reciproque $\phi^{-1}$ est une isometrie fixant l'origine et est lineaire. En particulier on a*

$$\mathrm{Isom}_{\mathbf{0}}(\mathbb{R}^2) \subset \mathrm{GL}(\mathbb{R}^2).$$

Le theoreme precedent induit la definition suivante:

DÉFINITION 3.11. *L'ensemble $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ s'appelle l'ensemble des isometrie lineaires du plan. Par opposition un element general de $\mathrm{Isom}(\mathbb{R}^2)$ sera parfois appele "isometrie affine".*

La preuve de ce theoreme repose sur la

PROPOSITION 3.7. *Soit $\phi \in \mathrm{Isom}_{\mathbf{0}}(\mathbb{R}^2)$, alors $\phi$ preserve la longueur des vecteurs ainsi que leur produit scalaire:*

$$\forall \vec{v}, \vec{w} \in \mathbb{R}^2,\ \|\phi(\vec{v})\| = \|\vec{v}\|,\ \langle \phi(\vec{v}), \phi(\vec{w})\rangle = \langle \vec{v}, \vec{w}\rangle$$

PREUVE. Soit $\phi \in \mathrm{Isom}_{\mathbf{0}}(\mathbb{R}^2)$, et $\vec{v} = \mathbf{0}\vec{P}$ un vecteur, on a

$$\|\phi(\vec{v})\| = d(\mathbf{0}, \phi(P)) = d(\phi(\mathbf{0}), \phi(P)) = d(\mathbf{0}, P) = \|\vec{v}\|.$$

On a pour $\vec{w} = \mathbf{0}\vec{Q}$

$$\langle \phi(\vec{v}), \phi(\vec{w})\rangle = \frac{1}{2}(\|\phi(\vec{v})\|^2 + \|\phi(\vec{w})\|^2 - \|\phi(\vec{v}) - \phi(\vec{w})\|^2) = \frac{1}{2}(\|\vec{v}\|^2 + \|\vec{w}\|^2 - d(\phi(P), \phi(Q))^2)$$

$$= \frac{1}{2}(\|\vec{v}\|^2 + \|\vec{w}\|^2 - d(P, Q)^2) = \frac{1}{2}(\|\vec{v}\|^2 + \|\vec{w}\|^2 - \|\vec{v} - \vec{w}\|^2) = \langle \vec{v}, \vec{w}\rangle.$$

□

**Preuve du Theoreme 3.3.** Soit $\vec{u}, \vec{v} \in \mathbb{R}^2$ et $\lambda \in \mathbb{R}$.

$$\|\phi(\lambda\vec{u} + \vec{v}) - (\lambda\phi(\vec{u}) + \phi(\vec{v}))\|^2 = \|\phi(\lambda\vec{u} + \vec{v})\|^2 + \|\lambda\phi(\vec{u})\|^2 + \|\phi(\vec{v}))\|^2$$

$$-2\langle \phi(\lambda\vec{u} + \vec{v}), \lambda\phi(\vec{u})\rangle - 2\langle \phi(\lambda\vec{u} + \vec{v}), \phi(\vec{v})\rangle + 2\langle \lambda\phi(\vec{u}), \phi(\vec{v})\rangle$$

$$= \|\lambda\vec{u} + \vec{v}\|^2 + \lambda^2\|\vec{u}\|^2 + \|\vec{v}\|^2 - 2\lambda\langle \lambda\vec{u} + \vec{v}, \vec{u}\rangle - 2\langle \lambda\vec{u} + \vec{v}, \vec{v}\rangle + 2\lambda\langle \vec{u}, \vec{v}\rangle$$

$$= \|\lambda\vec{u} + \vec{v} - (\lambda\vec{u} + \vec{v})\|^2 = 0$$

et donc

$$\phi(\lambda\vec{u} + \vec{v}) = \lambda\phi(\vec{u}) + \phi(\vec{v}).$$

De plus $\phi$ est bijective car elle est injective: soient $P, Q \in \mathbb{R}^2$

$$\phi(P) = \phi(Q) \Rightarrow d(\phi(P), \phi(Q)) = 0 = d(P, Q) \Rightarrow P = Q$$

et une application lineaire entre espaces vectoriels de meme dimension finie (ici 2) qui est injective est surjective[1].

On va donner un preuve directe la surjectivite: etant donne $\vec{v} \in \mathbb{R}^2$, il existe $\vec{u} \in \mathbb{R}^2$ tel que

$$\varphi(\vec{u}) = \vec{v}.$$

Soit $\mathcal{B}_0 = (\mathbf{e}_1, \mathbf{e}_2)$ la base canonique de $\mathbb{R}^2$; comme on l'a vu c'est une base orthonormee de $\mathbb{R}^2$ et considerons son image $\varphi(\mathcal{B}_0) = (\varphi(\mathbf{e}_1), \varphi(\mathbf{e}_2))$ alors on a

$$\|\varphi(\mathbf{e}_1)\| = \|\mathbf{e}_1\| = 1,\ \|\varphi(\mathbf{e}_2)\| = \|\mathbf{e}_2\| = 1,\ \langle \varphi(\mathbf{e}_1), \varphi(\mathbf{e}_2)\rangle = \langle \mathbf{e}_1, \mathbf{e}_2\rangle = 0$$

donc $\varphi(\mathcal{B}_0)$ est une base orthonormee. Par la Proposition 3.6 il existe $\lambda, \mu \in \mathbb{R}$ tel que

$$\vec{v} = \lambda\varphi(\mathbf{e}_1) + \mu\varphi(\mathbf{e}_2) = \varphi(\lambda\mathbf{e}_1 + \mu\mathbf{e}_2)$$

(par linearite de $\varphi$); ainsi $\phi$ est bijective.

Montrons que $\phi^{-1}$ est lineaire et une isometrie fixant $\mathbf{0}$. Comme $\phi(\mathbf{0}) = \mathbf{0}$ on a $\phi^{-1}(\mathbf{0}) = \mathbf{0}$.

Soient $P, Q \in \mathbb{R}^2$

$$d(\phi^{-1}(P), \phi^{-1}(Q)) = d(\phi(\phi^{-1}(P)), \phi(\phi^{-1}(Q))) = d(P, Q) \tag{2.1}$$

et donc $\phi^{-1} \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$; en particulier $\phi^{-1}$ est lineaire.

[1] C'est un resultat qui est demontre dans le cours d'algebre lineaire.

Notons que la linearite de la reciproque d'une application lineaire bijective est un phenomene general: soit $\lambda \in \mathbb{R}$, $\vec{u}, \vec{v} \in \mathbb{R}^2$, on a

$$\varphi(\lambda\phi^{-1}(\vec{u}) + \phi^{-1}(\vec{v})) = \lambda\varphi(\phi^{-1}(\vec{u})) + \varphi(\phi^{-1}(\vec{v})) = \lambda\vec{u} + \vec{v}$$

et

$$\varphi(\varphi^{-1}(\lambda\vec{u} + \vec{v})) = \lambda\vec{u} + \vec{v}$$

donc $\lambda\phi^{-1}(\vec{u}) + \phi^{-1}(\vec{v})$ et $\varphi^{-1}(\lambda\vec{u} + \vec{v})$ ont la meme image par $\phi$ et par injectivite ils sont egaux.

$$\varphi^{-1}(\lambda\vec{u} + \vec{v}) = \lambda\phi^{-1}(\vec{u}) + \phi^{-1}(\vec{v}).$$

□

On a montrer qu'une isometrie fixant l'origine etait lineaire. Voici des moyen d'identifier quelles applications lineaires sont des isometries.

EXERCICE 3.1. Soit $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ une application lineaire.

(1) Montrer que si $\phi$ preserve la longueur ($\forall \vec{u} \in \mathbb{R}^2,\ \|\phi(\vec{u})\| = \|\vec{u}\|$) alors $\phi$ est une isometrie.
(2) Soit $\mathcal{B}_0 = (\mathbf{e}_{0,1} = (1,0), \mathbf{e}_{0,2} = (0,1))$ la base canonique. Montrer que si sa transformee par $\phi$, $\phi(\mathcal{B}_0) = (\phi(\mathbf{e}_{0,1}), \phi(\mathbf{e}_{0,2}))$ est orthonormee alors $\phi$ est une isometrie.
(3) Etant donne une base orthonormee $\mathcal{B}$, montrer qu'il existe une isometrie $\phi$ qui envoie $\mathcal{B}_0$ sur $\mathcal{B}$ (on chargera une application lineaire).
(4) Etant donne deux bases orthonormees $\mathcal{B}, \mathcal{B}'$, montrer qu'il existe une isometrie $\phi$ qui envoie $\mathcal{B}$ sur $\mathcal{B}'$.

Voici la solution de la premiere question:

PROPOSITION 3.8. *Soit $\phi : \mathbb{R}^2 \mapsto \mathbb{R}^2$ une application lineaire. Si $\phi$ transforme la base canonique $\mathcal{B}_0$ en une base orthonormee alors $\phi$ est une isometrie lineaire.*

**Preuve**: En effet, $\forall \vec{u} = (x, y) \in \mathbb{R}^2$ on a $\phi(\vec{u}) = x\phi(\mathbf{e}_1) + y\phi(\mathbf{e}_2)$ et donc

$$\begin{aligned} \|\phi(\vec{u})\|^2 &= \langle x\phi(\mathbf{e}_1) + y\phi(\mathbf{e}_2), x\phi(\mathbf{e}_1) + y\phi(\mathbf{e}_2)\rangle \\ &= x^2\langle\phi(\mathbf{e}_1), \phi(\mathbf{e}_1)\rangle + 2xy\langle\phi(\mathbf{e}_1), \phi(\mathbf{e}_2)\rangle + y^2\langle\phi(\mathbf{e}_2), \phi(\mathbf{e}_2)\rangle \\ &= x^2 + y^2 = \|\vec{u}\|^2. \end{aligned}$$

Comme $\phi$ est lineaire et preserve la longueur, c'est une isometrie: on a $\forall P, Q \in \mathbb{R}^2$

$$d(\phi(P), \varphi(Q)) = \|\phi(P) - \phi(Q)\| = \|\phi(P - Q)\| = \|P - Q\| = d(P, Q).$$

□

**Preuve du Theoreme 3.2.**

- L'identite $\mathrm{Id}_{\mathbb{R}^2}$ est une isometrie.
- Si $\phi$ et $\psi$ sont des isometries alors $\phi \circ \psi$ est une isometrie:

$$\forall P, Q,\ d(\phi \circ \psi(P), \phi \circ \psi(Q)) = d(\psi(P), \psi(Q)) = d(P, Q)$$

- Si de plus $\phi$ et $\psi$ sont des translations $\phi \circ \psi$ en est une et si $\phi$ et $\psi$ fixent l'origine $\mathbf{0}$ alors $\phi \circ \psi$ egalement.
- Ainsi $\mathrm{Isom}(\mathbb{R}^2), \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ et $T(\mathbb{R}^2)$ contiennent l'identite et sont stables par composition. Il reste a montrer que ces ensembles sont formes de bijections et qu'ils sont stable par passage a l'application reciproque.
- On a deja vu que c'etait le cas pour les translations et les isometries lineaires. Ce sont donc des sous-groupes de $\mathrm{Bij}(\mathbb{R}^2)$.

– Soit $\phi$ une isometrie generale: montrons que $\phi$ est la composee d'une translation et d'une isometrie lineaire. Considerons $\phi_{\mathbf{0}} = t_{-\phi(\mathbf{0})} \circ \phi$ est une isometrie et comme

$$\phi_{\mathbf{0}}(\mathbf{0}) = t_{-\phi(\mathbf{0})}(\phi(\mathbf{0})) = \phi(\mathbf{0}) - \phi(\mathbf{0}) = \mathbf{0}$$

elle est lineaire et en particulier est bijective. De plus

$$\phi = t_{\phi(\mathbf{0})} \circ \phi_{\mathbf{0}}$$

et donc $\phi$ est bijective (comme composee d'applications bijectives) et sa reciproque est une isometrie en repetant l'argument (2.1)

Ainsi $\mathrm{Isom}(\mathbb{R}^2)$ est un sous-groupe de $\mathrm{Bij}(\mathbb{R}^2)$ et $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ et $T(\mathbb{R}^2)$ sont des sous-groupes.

– Montrons que la decomposition translation/isometrie lineaire

$$\phi = t \circ \phi_0$$

est unique: supposons que $\phi$ se decompose de deux manieres

$$\phi = t \circ \phi_0 = t' \circ \phi_0'.$$

On a alors

$$t'^{-1} \circ t = \phi_0' \circ \phi_0^{-1}$$

et donc l'element $\psi_0 = t'^{-1} \circ t = \phi_0' \circ \phi_0^{-1}$ appartient a la fois a $T(\mathbb{R}^2)$ et a $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ : on a $\psi_0 = t_{\vec{u}}$ pour un certain vecteur $\vec{u} \in \mathbb{R}^2$ et donc

$$\psi_0(\mathbf{0}) = \mathbf{0} = t_{\vec{u}}(\mathbf{0}) = \mathbf{0} + \vec{u},\ \vec{u} = \mathbf{0} \text{ et } \phi_0 = \mathrm{Id}_{\mathbb{R}^2}.$$

Il en resulte que

$$t = t',\ \phi_0 = \phi_0'.$$

– Le sous-groupe $T(\mathbb{R}^2)$ est distingue: $T(\mathbb{R}^2)$ est stable par conjugaisons

$$\forall \phi \in \mathrm{Isom}(\mathbb{R}^2),\ \mathrm{Ad}(\phi)(T(\mathbb{R}^2)) = T(\mathbb{R}^2)$$

et plus precisement

$$\forall \phi \in \mathrm{Isom}(\mathbb{R}^2),\ \forall \vec{u} \in \mathbb{R}^2,\ \mathrm{Ad}(\phi)(t_{\vec{u}}) = t_{\phi(\vec{u})} \in T(\mathbb{R}^2).$$

On commence par supposer que $\phi = \phi_0 \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$. Par linearite de $\phi_0$,

$$\begin{aligned}\mathrm{Ad}(\phi_0)(t_{\vec{u}})(\vec{v}) = \phi_0(t_{\vec{u}}(\phi_0^{-1}(\vec{v}))) = \phi_0(\vec{u} + \phi_0^{-1}(\vec{v})) \\ = \phi_0(\vec{u}) + \phi_0(\phi_0^{-1}(\vec{v})) = \phi_0(\vec{u}) + \vec{v} = t_{\phi_0(\vec{u})}(\vec{v}).\end{aligned}$$

On traite le cas general: $\phi = t \circ \phi_0$, on a

$$\mathrm{Ad}(\phi)(t_{\vec{u}}) = \mathrm{Ad}(t)(\mathrm{Ad}(\phi_0)(t_{\vec{u}})) = \mathrm{Ad}(t)(t_{\phi_0(\vec{u})}) = t_{\phi_0(\vec{u})}$$

car $T(\mathbb{R}^2) \simeq \mathbb{R}^2$ est un groupe commutatif.

□

On deduit de cette decomposition le corollaire suivant qui sera tres utile:

THÉORÈME 3.4. *L'application "partie lineaire"*

$$\mathrm{lin} = \cdot_0 : \begin{array}{ccc} \mathrm{Isom}(\mathbb{R}^2) & \mapsto & \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}} \\ \phi & \mapsto & \phi_0 \end{array}$$

*qui a une isometrie associe sa partie lineaire est un morphisme de groupe surjectif.*

**Preuve**: L'application est surjective: si $\phi_0$ est une isometrie lineaire alors c'est sa propre partie lineaire. Il s'agit de montrer que si $\phi$ et $\psi$ sont deux isometries de partie lineaires $\phi_0$ et $\psi_0$ alors

$$\mathrm{lin}(\phi \circ \psi) = (\phi \circ \psi)_0 = \phi_0 \circ \psi_0 = \mathrm{lin}(\phi) \circ \mathrm{lin}(\psi).$$

On a

$$\phi = t \circ \phi_0,\ \psi = t' \circ \psi_0$$

avec $t$ et $t'$ des translation et

$$\phi \circ \psi = t \circ \phi_0 \circ t' \circ \psi_0 = t \circ \phi_0 \circ t' \circ (\phi_0^{-1} \circ \phi_0) \circ \psi_0 = (t \circ \phi_0 \circ t' \circ \phi_0^{-1}) \circ (\phi_0 \circ \psi_0).$$

Comme le groupe des translations est distingue $t'' = \phi_0 \circ t' \circ \phi_0^{-1}$ est une translation et donc

$$\phi \circ \psi = (t \circ t'') \circ (\phi_0 \circ \psi_0)$$

se decompose en une translation et une isometrie lineaire. Par unicite de cette decomposition $\phi_0 \circ \psi_0$ est la partie lineaire de $\phi \circ \psi$.

□

Ainsi si on doit identifier une isometrie affine qui est un produits d'isometries connues, on obtient sa partie lineaire en composant les parties lineaires de ses constituants. On peut calculer ensuite la partie translation.

Remarque 2.1. L'existence et l'unicite de la decomposition d'une isometrie en translation et en partie lineaire est equivalente au fait que l'application

$$\begin{array}{ccc} T(\mathbb{R}^2) \times \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}} & \mapsto & \mathrm{Isom}(\mathbb{R}^2) \\ (t, \phi_0) & \mapsto & t \circ \phi_0 \end{array}$$

est une bijection. Par contre ce n'est pas un isomorphisme entre le groupe produit "abstrait" $T(\mathbb{R}^2) \times \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ et le groupe $\mathrm{Isom}(\mathbb{R}^2)$ On verra plus tard que si l'on equipe le produit $T(\mathbb{R}^2) \times \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ d'une loi de groupe adequate (dite de "produit semi-direct") on obtient un isomorphisme de groupes.

**2.1. Matrice associee a une isometrie lineaire.** Soit $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ une isometrie lineaire; soit $\mathcal{B}_0 = (\mathbf{e}_1, \mathbf{e}_2)$, $\mathbf{e}_1 = (1, 0)$, $\mathbf{e}_2 = (0, 1)$ les deux vecteurs de la base canonique de $\mathbb{R}^2$. Comme $\phi$ est lineaire elle est completement determinee par les valeurs $\phi(\mathbf{e}_1)$, $\phi(\mathbf{e}_2)$: soit $(x, y) \in \mathbb{R}^2$, on a a

$$\phi(x, y) = \phi(x\mathbf{e}_1 + y\mathbf{e}_2) = x\phi(\mathbf{e}_1) + y\phi(\mathbf{e}_2).$$

Ecrivant

$$\mathbf{e}_1' := \phi(\mathbf{e}_1) = (a, c),\ \mathbf{e}_2' := \phi(\mathbf{e}_2) = (b, d),\ a, b, c, d \in \mathbb{R}$$

on a

$$\phi(x, y) = x(a, c) + y(b, d) = (ax + by, cx + dy) = (X, Y).$$

On associe a $\phi$ une matrice (la matrice de $\phi$ dans la base canonique)

$$M_\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

L'image du vecteur $(x, y)$ par $\phi$, $\phi(x, y) = (X, Y)$ peut se calculer comme le produit matriciel

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Utilisant le fait que $\phi$ est une isometrie on va pouvoir donner des precisions sur la forme des coefficients de la matrice (de $\phi$ dans la base $\mathcal{B}_0$)

$$M_\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

On rappelle la

DÉFINITION 3.12. *Soit* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{R}$ *une matrice quelconque (pas forcement associee a une isometrie lineaire), son determinant* $\det M$ *est defini par*

$$\det(M) = ad - bc.$$

THÉORÈME 3.5. *Soit* $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ *et*

$$M_\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

*sa matrice associee. La matrice de l'application reciproque* $\phi^{-1}$ *est donnee par*

$$M_{\phi^{-1}} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \tag{2.2}$$

*et les coefficients* $a, b, c, d$ *verifient les egalites*

$$a^2 + c^2 = b^2 + d^2 = a^2 + b^2 = c^2 + d^2 = 1,\ ab + cd = ac + bd = 0 \tag{2.3}$$

$$\det(M_\phi) = ad - bc = \pm 1. \tag{2.4}$$

**Preuve**: On a

$$\varphi(\mathbf{e}_1) = (a, c) = a\mathbf{e}_1 + c\mathbf{e}_2,\ \varphi(\mathbf{e}_2) = (b, d) = b\mathbf{e}_1 + d\mathbf{e}_2.$$

donnc $\mathcal{B}_0$ est orthonormee on a par (1.3)

$$a = \langle \varphi(\mathbf{e}_1), \mathbf{e}_1 \rangle,\ c = \langle \varphi(\mathbf{e}_1), \mathbf{e}_2 \rangle,\ b = \langle \varphi(\mathbf{e}_2), \mathbf{e}_1 \rangle,\ d = \langle \varphi(\mathbf{e}_2), \mathbf{e}_2 \rangle.$$

On va faire de meme avec les coefficients de $M_{\phi^{-1}} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$: ce sont les coefficients de $\mathbf{e}'_1 = \phi^{-1}(\mathbf{e}_1)$, $\mathbf{e}'_2 = \phi^{-1}(\mathbf{e}_2)$ dans la base $\mathcal{B}_0$. Par (1.3), on a les formules

$$a' = \langle \phi^{-1}(\mathbf{e}_1), \mathbf{e}_1 \rangle,\ c' = \langle \phi^{-1}(\mathbf{e}_1), \mathbf{e}_2 \rangle,\ b' = \langle \phi^{-1}(\mathbf{e}_2), \mathbf{e}_1 \rangle\ d' = \langle \phi^{-1}(\mathbf{e}_2), \mathbf{e}_2 \rangle.$$

On invoque alors le Lemme tres simple suivant:

LEMME 3.2 (Formule d'adjonction). *Soit* $\varphi$ *une isometrie lineaire et* $\vec{u}, \vec{v} \in \mathbb{R}^2$, *on a*

$$\langle \varphi(\vec{u}), \vec{v} \rangle = \langle \vec{u}, \varphi^{-1}(\vec{v}) \rangle.$$

**Preuve**: Comme $\varphi^{-1}$ est une isometrie lineaire on a

$$\langle \varphi(\vec{u}), \vec{v} \rangle = \langle \varphi^{-1}(\varphi(\vec{u})), \varphi^1(\vec{v}) \rangle = \langle \vec{u}, \varphi^{-1}(\vec{v}) \rangle.$$

□

Appliquant ce lemme on trouve

$$a' = \langle \phi^{-1}(\mathbf{e}_1), \mathbf{e}_1 \rangle = \langle \mathbf{e}_1, \phi(\mathbf{e}_1) \rangle = \langle \phi(\mathbf{e}_1), \mathbf{e}_1 \rangle = a.$$

De meme on trouve que

$$c' = \langle \phi^{-1}(\mathbf{e}_1), \mathbf{e}_2 \rangle = \langle \mathbf{e}_1, \phi(\mathbf{e}_2) \rangle = b$$

et egalement on obtient que

$$b' = c,\ d' = d.$$

D'autre part comme $(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2))$ est orthonormee, on a

$$1 = \langle \phi(\mathbf{e}_1), \phi(\mathbf{e}_1)\rangle = a^2 + c^2,\ 1 = \langle \phi(\mathbf{e}_2), \phi(\mathbf{e}_2)\rangle = b^2 + d^2, 0 = \langle \phi(\mathbf{e}_1), \phi(\mathbf{e}_2)\rangle = ab + cd.$$

Appliquant ce resultat a $(a', b', c', d') = (a, c, b, d)$ (les coefficients de la matrice de l'isometrie $M_{\phi^{-1}}$, on obtient

$$1 = a^2 + b^2, 1 = c^2 + d^2, 0 = ac + bd.$$

Enfin pour (2.4), on a

$$(ad-bc)^2 = a^2d^2 - 2abcd + b^2c^2 = a^2d^2 + 2a^2c^2 + b^2c^2 = a^2(d^2+c^2) + c^2(b^2+a^2) = a^2 + c^2 = 1.$$

□

Définition 3.13. *Une matrice* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *est dite orthogonale si c'est la matrice associee a une isometrie lineaire. Une matrice orthogonale est dite speciale si son determinant vaut* $+1$ *et elle est dite non-speciale si son determinant vaut* $-1$. *On note respectivement* $\mathrm{O}_2(\mathbb{R}), \mathrm{O}_2(\mathbb{R})^+ = \mathrm{SO}_2(\mathbb{R}), \mathrm{O}_2(\mathbb{R})^-$ *l'ensemble des matrices orthogonales, orthogonales speciales, orthogonales non-speciales. On a donc*

$$\mathrm{O}_2(\mathbb{R}) = \mathrm{O}_2(\mathbb{R})^+ \sqcup \mathrm{O}_2(\mathbb{R})^-.$$

Définition 3.14. *Soit*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}).$$

*Une matrice* $2 \times 2$. *La transposee de* $M$ *notee* ${}^tM$ *est la matrice obtenue en echangeant les coefficients de part et d'autre de la diagonale:*

$${}^tM = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

On a donc montre que

Proposition 3.9. *Une matrice orthogonale est inversible et son inverse est donnee par la matrice transposee* ${}^tM$.

Reciproquement, on a

Proposition 3.10. *Soit* $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ *une matrice vérifiant*

$$a^2 + c^2 = b^2 + d^2 = 1,\ ab + cd = 0$$

*alors* $M$ *est orthogonale. En particulier* $M^{-1} = {}^tM$

**Preuve**: Soit $\varphi$ l'application lineaire telle que

$$\varphi(\mathbf{e}_1) = (a, c),\ \varphi(\mathbf{e}_1) = (b, d)$$

(ie. $\varphi(x, y) = x(a, c) + y(b, d) = (ax + by, cx + dy)$. Sa matrice associee est $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Alors $(\varphi(\mathbf{e}_1), \varphi(\mathbf{e}_2)) = ((a, c), (b, d))$ est une BON et $\varphi$ transforme donc une BON en une BON: en vertu de la Proposition 3.8 c'est une isometrie lineaire. □

On va expliciter la forme des matrices orthogonales.

PROPOSITION 3.11. *Une matrice $M = M_\varphi$ est orthogonale si et seulement si il existe $\mathrm{c}, \mathrm{s} \in \mathbb{R}$ verifiant $\mathrm{c}^2 + \mathrm{s}^2 = 1$ tel que $M$ est de l'une des deux formes suivante:*

$$\textit{si } M \textit{ est speciale } M = \begin{pmatrix} \mathrm{c} & -\mathrm{s} \\ \mathrm{s} & \mathrm{c} \end{pmatrix}$$

*et*

$$\textit{si } M \textit{ est non-speciale } M = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix}.$$

*–Si $M$ est speciale son inverse $M^{-1} = M_{\varphi^{-1}}$ est egale a sa transposee ${}^tM$ qui est encore speciale*

$$M^{-1} = {}^tM = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ -\mathrm{s} & \mathrm{c} \end{pmatrix}$$

*– Si $M$ est non-speciale son inverse $M^{-1} = M_{\varphi^{-1}}$ est egale a sa transposee ${}^tM$ et est egale a $M$; en d'autres termes $M$ est d'ordre 2 exactement*

$$M^{-1} = {}^tM = M = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix}, \ M^2 = \mathrm{Id} \textit{ et } M \neq \mathrm{Id}.$$

**Preuve**: Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice orthogonale et posons $\mathrm{c} = a, \mathrm{s} = c$. On a donc

$$\mathrm{c}b + \mathrm{s}d = 0.$$

Comme $\mathrm{c}^2 + \mathrm{s}^2 = 1$ et donc $(\mathrm{c}, \mathrm{s}) \neq (0, 0)$, les solutions $(b, d)$ du systeme lineaire ci-dessus sont toutes de la forme (c'est l'ensemble des points d'une droite passant par l'origine)

$$(b, d) = \lambda(-\mathrm{s}, \mathrm{c}), \ \lambda \in \mathbb{R}.$$

On a

$$\det M = \pm 1 = ad - bc = \lambda(\mathrm{c}^2 + \mathrm{s}^2) = \lambda(a^2 + c^2) = \lambda$$

et la matrice est de la forme annoncee pour $\lambda = +1$ ou $-1$.

Reciproquement soit $M$ de l'une des deux formes ci-dessus: elle verifie les condition de la Proposition 3.10; c'est donc une matrice orthogonale.

Soit $M$ une matrice speciale, son inverse est egale a sa transposee qui vaut $\begin{pmatrix} \mathrm{c} & \mathrm{s} \\ -\mathrm{s} & \mathrm{c} \end{pmatrix}$ qui est encore une matrice speciale.

Soit $M = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix}$ une matrice non-speciale alors $M \neq \mathrm{Id}$ car on aurait $\mathrm{s} = 0$ et les coordonnees sur la diagonale sont differentes. Son inverse est egale a sa transposee qui vaut

$${}^tM = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix} = M.$$

On a donc

$$M^2 = M.M = M.M^{-1} = \mathrm{Id}_2.$$

□

REMARQUE 2.2. Notons que si $M$ est non-speciale elle est s'ecrit comme produit d'une matrice non-speciale et d'une matrice speciale:

$$M = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ -\mathrm{s} & \mathrm{c} \end{pmatrix}.$$

La premiere matrice est non-speciale[2] et la seconde est speciale. Alternativement on a

$$M = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix} = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ -\mathrm{s} & \mathrm{c} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

REMARQUE 2.3. comme on le verra plus tard les matrices speciales sont appelees matrices de rotations (les non-speciales matrices de symetrie). Dans le cas des rotations, $\mathrm{c}, \mathrm{s}$ sont respectivement le cosinus et le sinus de (l'angle de) cette rotation.

**2.2. Applications lineaires et matrices.** On a associe a chaque isometrie lineaire $\phi$ une certaine matrice $M_\phi$ dont les coefficients sont les coefficient des images $\phi(\mathbf{e}_1), \phi(\mathbf{e}_2)$ des deux vecteurs de la base canonique $\mathbf{e}_1, \mathbf{e}_2$ dans la base canonique $(\mathbf{e}_1, \mathbf{e}_2)$. Pour faire cette association il suffit juste que $\phi$ soit lineaire et on va donner des precisions supplementaires quand a cette association:

2.2.1. *L'algebre des applications lineaires.*

DÉFINITION 3.15. *Une application $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ est $\mathbb{R}$-lineaire si*

$$\forall \vec{v}, \vec{w} \in \mathbb{R}^2,\ \forall \lambda, \mu \in \mathbb{R},\ \phi(\lambda\vec{v} + \mu\vec{w}) = \lambda\phi(\vec{v}) + \mu\phi(\vec{w}).$$

*On note $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ l'ensemble des applications lineaires de $\mathbb{R}^2$ dans $\mathbb{R}^2$ (l'ensemble des endomorphismes de $\mathbb{R}^2$) vu comme $\mathbb{R}$-espace vectoriel.*

L'ensemble $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ est munis de structures supplementaires

- Une loi d'addition: si $\phi, \psi$ sont lineaires alors l'application $\phi + \psi$ definie par
$$(\phi + \psi)(\vec{v}) = \phi(\vec{v}) + \psi(\vec{v})$$
est lineaire.
- La loi de composition des applications: si $\phi, \psi$ sont lineaires alors l'application composee $\phi \circ \psi$ definie par
$$(\phi \circ \psi)(\vec{v}) = \phi(\psi(\vec{v}))$$
est lineaire.
- Une loi de multiplication par les scalaires: pour $\phi$ lineaire et $\lambda \in \mathbb{R}$, l'application $\lambda.\phi$ definie par
$$(\lambda.\phi)(\vec{v}) = \lambda.\phi(\vec{v})$$
est lineaire.

De plus

- L'addition est commutative et associative
$$\phi + \psi = \psi + \phi.$$
- La composition est associative:
$$\phi \circ (\psi \circ \varphi) = (\phi \circ \psi) \circ \varphi.$$
- La composition est distributive par rapport a l'addition:

$$\forall \phi, \varphi, \psi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2),\ \phi \circ (\varphi + \psi) = \phi \circ \varphi + \phi \circ \psi,\ (\varphi + \psi) \circ \phi = \varphi \circ \phi + \psi \circ \phi.$$

- La multiplication est distributive par rapport a l'addition:
$$\forall \varphi, \psi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2),\ \lambda.(\varphi + \psi) = \lambda.\varphi + \lambda.\psi.$$

Enfin $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ possede deux elements distingues

[2] c'est la matrice de la symetrie par rapport a l'axe des abscisses

– L'application constante nulle

$$0_{\mathbb{R}^2} : \vec{v} \to 0_{\mathbb{R}^2}$$

qui est l'element neutre de $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ pour l'addition:

$$\forall \varphi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2),\ \phi + 0_{\mathbb{R}^2} = \phi.$$

– L'application identite

$$\mathrm{Id}_{\mathbb{R}^2} : \vec{v} \to \vec{v}$$

qui est l'element neutre de $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ pour la composition:

$$\forall \phi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2),\ \phi \circ \mathrm{Id}_{\mathbb{R}^2} = \mathrm{Id}_{\mathbb{R}^2} \circ \phi = \phi.$$

2.2.2. *L'algebre des matrice* $2 \times 2$.

Définition 3.16. *Une matrice reelle* $2 \times 2$ *est un tableau carre a* 4 *entrees reelles*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in \mathbb{R}.$$

*On note* $M_2(\mathbb{R})$ *l'ensemble des matrice* $2 \times 2$

L'ensemble $M_2(\mathbb{R})$ est munis de structures supplementaires

– Une loi d'addition: si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ sont des matrices on defini la matrice $M + M'$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}.$$

– Une loi de multiplication matricielle: si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ sont des matrices on defini la matrice produit $M.M'$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

– Un loi de multiplication par les scalaires: pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice et $\lambda \in \mathbb{R}$, la matrice $\lambda.M$ est definie par

$$\lambda. \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}.$$

De plus

– L'addition est commutative

$$M + M' = M' + M.$$

– La multiplication matricielle est distributive par rapport a l'addition:

$$\forall M, M', M",\ M.(M' + M") = M.M' + M.M",\ (M' + M").M = M'.M + M".M.$$

– La multiplication par les scalaires est distributive par rapport a l'addition:

$$\forall M, M',\ \lambda.(M + M') = \lambda.M + \lambda.M'.$$

Enfin $M_2(\mathbb{R})$ possede deux elements distingues

– La matrice nulle
$$\mathbf{0}_{\mathrm{M}_2(\mathbb{R})} = 0_2 := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
qui est l'element neutre de $M_2(\mathbb{R})$ pour l'addition:
$$\forall M,\ M + 0_2 = M.$$
– La matrice identite
$$\mathrm{Id}_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
qui est l'element neutre de $M_2(\mathbb{R}^2)$ pour la multiplication matricielle:
$$\forall M,\ M.\mathrm{Id}_2 = \mathrm{Id}_2.M = M.$$

Des ensembles tels que l'ensemble des endomorphismes ou celui des matrices munis des structures supplementaires $(\mathrm{End}_{\mathbb{R}}(\mathbb{R}^2), +, \circ, 0_{\mathbb{R}^2}, \mathrm{Id}_{\mathbb{R}^2})$, $(M_2(\mathbb{R}^2), +, ., 0_2, \mathrm{Id}_2)$ sont appeles de $\mathbb{R}$-algebres.

Soit $\phi$ une application lineaire, on lui associe la matrice
$$M_\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ avec } \phi(\mathbf{e}_1) = (a, c),\ \phi(\mathbf{e}_1) = (b, d).$$
L'interet de definir la multiplication des matrices telle qu'on l'a definie est apparent dans le Theoreme suivant:

THÉORÈME 3.6. *L'application*
$$M. : \begin{array}{ccc} \mathrm{End}(\mathbb{R}^2) & \mapsto & M_2(\mathbb{R}) \\ \phi & \mapsto & M_\phi \end{array}$$
*est un isomorphisme de $\mathbb{R}$-algebres, ie. une bijection compatible avec les structures d'algebres et qui verifie notamment*
$$M_{\phi+\psi} = M_\phi + M_\psi,\ M_{\phi\circ\psi} = M_\phi.M_\psi,\ M_{\lambda.\phi} = \lambda.M_\phi$$
*ainsi que*
$$M_{0_{\mathbb{R}^2}} = \mathbf{0}_{\mathrm{M}_2(\mathbb{R})},\ M_{\mathrm{Id}^2_{\mathbb{R}}} = \mathrm{Id}_2.$$

2.2.3. *Isomorphismes lineaires et matrices inversibles.*

DÉFINITION 3.17. *Un isomorphisme lineaire de $\phi : \mathbb{R}^2 \to \mathbb{R}^2$, ou encore un automorphisme lineaire, est une application lineaire qui est bijective. Sa reciproque $\phi^{-1}$ est alors automatiquement lineaire. On dit egalement que $\phi$ est inversible. On note*
$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^2) = \mathrm{GL}(\mathbb{R}^2) = \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2) \cap \mathrm{Bij}(\mathbb{R}^2)$$
*l'ensemble des isomorphismes lineaires. L'ensemble $(\mathrm{GL}(\mathbb{R}^2), \circ)$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{R}^2), \circ)$ appelle le groupe lineaire de $\mathbb{R}^2$.*

Rappelons comment on montre que $\phi^{-1}$ est lineaire: on a
$$\phi(\phi^{-1}(\lambda\vec{u} + \vec{v})) = \lambda\vec{u} + \vec{v}$$
et
$$\phi(\lambda\phi^{-1}(\vec{u}) + \phi^{-1}(\vec{v})) = \lambda\phi(\phi^{-1}(\vec{u})) + \phi(\phi^{-1}(\vec{v})) = \lambda\vec{u} + \vec{v}$$
et donc comme $\phi$ est injective
$$\phi^{-1}(\lambda\vec{u} + \vec{v}) = \lambda\phi^{-1}(\vec{u}) + \phi^{-1}(\vec{v}).$$

DÉFINITION 3.18. *L'image par l'application "matrice dans la base canonique " du groupe des applications lineaire inversibles de $\mathbb{R}^2$ est l'ensemble des matrices inversibles:*

$$\mathrm{GL}_2(\mathbb{R}) = \{M \in M_2(\mathbb{R}),\ \exists M^{-1} \in M_2(\mathbb{R}) \text{ tel que } M.M^{-1} = M^{-1}.M = \mathrm{Id}_2\}.$$

*Si $M = M_\phi$ alors*

$$M^{-1} = M_{\phi^{-1}}.$$

*cette matrice est donc unique: c'est inverse de $M$.*

DÉFINITION 3.19. *L'ensemble des matrices inversibles est note $\mathrm{GL}(\mathbb{R}^2)$. C'est un groupe pour la multiplication des matrices (isomorphe au groupe $\mathrm{GL}(\mathbb{R}^2)$). On l'appelle le groupe lineaire (des matrices $2 \times 2$.)*

2.2.4. *Le determinant et l'inversion des matrices.*

DÉFINITION 3.20. *Le determinant est la fonction $\det : M_2(\mathbb{R}^2) \to \mathbb{R}$ definie par*

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc.$$

Elle permet entre-autres de detecter si une matrice est inversible.

PROPOSITION 3.12. *Le determinant a les proprietes suivantes:*

(1) *Il est multiplicatif:*

$$\det(M.M') = \det(M).\det(M')\ \ \det(\mathrm{Id}_2) = 1.$$

(2) *Une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible ssi $\det M \neq 0$ et alors*

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

2.2.5. *La transposition.* La premiere partie de la definition suivante a deja ete vue:

DÉFINITION 3.1. *Soit*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}),$$

*la matrice*

$${}^tM = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$$

*s'appelle la transposee de $M$ et l'application*

$${}^t\cdot : M \in \mathrm{M}_2(\mathbb{R}) \mapsto {}^tM \in \mathrm{M}_2(\mathbb{R})$$

*est l'application de transposition.*

PROPOSITION 3.13. *L'application de transposition a les proprietes suivantes*

(1) *${}^t$ est lineaire:*

$${}^t(\lambda M + N) = \lambda {}^tM + {}^tN.$$

(2) *${}^t$ est involutive:*

$${}^t\cdot \circ {}^t\cdot = \mathrm{Id}_{\mathrm{M}_2(\mathbb{R})},\ \ {}^t({}^tM) = M.$$

(3) *La transposition est multiplicative:*

$${}^tM.N = {}^tN.{}^tM.$$

(4) *La transposition preserve le determinant* $\det(M) = ad - bc$.

$$\det({}^tM) = \det(M).$$

**Preuve**: Exercice. □

PROPOSITION 3.14. *Une matrice $M$ est orthogonale si et seulement si est verifie*

$${}^tM.M = \mathrm{Id}_2.$$

*Elle verifie alors egalement*

$$M.{}^tM = \mathrm{Id}_2.$$

**Preuve**: Supposons que ${}^tM.M = \mathrm{Id}_2$, cela s'ecrit

$${}^tM.M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & bc+ad \\ ab+cd & b^2+d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ce qui montre que les vecteurs $(a, c)$, $(b, d)$ forment une base orthonormee. Ainsi $\phi$ l'application lineaire associee a $M$ transforme la base canonique en une base orthonormee. C'est donc une isometrie. □

### 2.3. Le groupe des matrices orthogonales.

THÉORÈME 3.7. *On a les proprietes suivantes*

(1) *L'ensemble des matrices orthogonales* $\mathrm{O}_2(\mathbb{R})$ *est un sous-groupe du groupe des matrices inversibles* $\mathrm{GL}_2(\mathbb{R})$.
(2) *L'ensemble des matrices speciales orthogonales* $\mathrm{O}_2(\mathbb{R})^+$ *est un sous-groupe distingue de* $\mathrm{O}_2(\mathbb{R})$.
(3) *Le groupe des matrices speciales orthogonales est commutatif.*
(4) *L'ensemble des matrices de non-speciales* $\mathrm{O}_2(\mathbb{R})^-$ *est le translate multiplicatif (a gauche ou a droite) de* $\mathrm{O}_2(\mathbb{R})^+$ *par n'importe quelle matrice non-speciale (par exemple la matrice* $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$*):*

$$\forall M^- \in \mathrm{O}_2(\mathbb{R})^-, \text{ on a } \mathrm{O}_2(\mathbb{R})^- = M^-.\mathrm{O}_2(\mathbb{R})^+ = \mathrm{O}_2(\mathbb{R})^+.M^-.$$

*En d'autres termes, etant donne $M^- \in \mathrm{O}_2(\mathbb{R})^-$, toute matrice de $\mathrm{O}_2(\mathbb{R})^-$ est de la forme $M^-.M^+$ (resp. ${M'}^+.M^-$) pour un unique $M^+$ (resp. ${M'}^+$) de $\mathrm{O}_2(\mathbb{R})^+$.*
(5) *Toute matrice orthogonale s'ecrit comme produit de une matrice non-speciale (si la matrice est non-speciale) ou de deux matrices non-speciales (si la matrice est speciale). En particulier le groupe* $\mathrm{O}_2(\mathbb{R})$ *est engendre par* $\mathrm{O}_2(\mathbb{R})^-$*, l'ensemble des matrices orthogonales non-speciales.*

PREUVE. Les matrices orthogonales sont exactement les matrices associees a des isometries lineaires dans la base canonique et le produit de deux telles matrices est la matrice associee a la composee de ces isometries. Comme l'ensemble des isometries lineaires forme un groupe, la composee est encore une isometrie lineaire et donc le produit des deux matrices orthogonale est encore orthogonale. Pour la meme raison, une matrice orthogonale $M$ correspondant a $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ est inversible et son inverse $M^{-1}$ est orthogonale car c'est la matrice associee a $\phi^{-1}$. Cela montre que $\mathrm{O}_2(\mathbb{R})$ est un sous-groupe du groupe des matrices inversibles $\mathrm{GL}_2(\mathbb{R})$.

Pour voir que $\mathrm{O}_2(\mathbb{R})^+$ est un sous-groupe, on a deux possibilites.

La premiere est de verifier par un calcul explicite que si $M, M' \in \mathrm{O}_2(\mathbb{R})^+$, $M.M'$ appartient a $\mathrm{O}_2(\mathbb{R})^+$:

– Soient $M = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}$ et $M' = \begin{pmatrix} c' & -s' \\ s' & c' \end{pmatrix}$ deux matrices speciales, on a

$$M.M' = \begin{pmatrix} cc' - ss' & -cs' - sc' \\ sc' + cs' & -ss' + cc' \end{pmatrix} = \begin{pmatrix} c'' & -s'' \\ s'' & c'' \end{pmatrix}$$

avec

$$c'' = cc' - ss',\ s'' = cs' + sc'.$$

La matrice appartient a $O_2(\mathbb{R})$ et donc a $O_2(\mathbb{R})^+$ puisqu'elle est de la bonne forme.

Ainsi $O_2(\mathbb{R})^+$ est stable par multiplication et comme il est stable par inversion c'est un sous-groupe de $GL_2(\mathbb{R})$. On remarque que les coordonnees de $M.M'$ ne changent pas si on echange $c \leftrightarrow c'$ et $s \leftrightarrow s'$ donc

$$M.M' = M'.M$$

Le groupe $O_2(\mathbb{R})^+$ est commutatif.

Rappelons la reunion disjointe

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

– Soit $M^- \in O_2(\mathbb{R})^-$ et $M^+ \in O_2(\mathbb{R})^-$ alors $M^+.M^-$ et $M^-.M^+$ sont dans $O_2(\mathbb{R})$ mais ne peuvent appartenir a $O_2(\mathbb{R})^+$ car cela impliquerait (en multipliant par $(M^+)^{-1}$) que $M^- \in O_2(\mathbb{R})^-$ car $O_2(\mathbb{R})^+$ est un groupe. Ainsi

$$M^-.O_2(\mathbb{R})^+,\ O_2(\mathbb{R})^+.M^- \subset O_2(\mathbb{R})^-.$$

Montrons l'inclusion inverse: soit $M \in O_2(\mathbb{R})^-$ alors $M.M^- \in O_2(\mathbb{R})$ et

$$M.M^- = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}.\begin{pmatrix} c' & s' \\ s' & -c' \end{pmatrix} = \begin{pmatrix} cc' + ss' & cs' - sc' \\ -(cs' - sc') & cc' + ss' \end{pmatrix} \in O_2(\mathbb{R})^+$$

car elle n'est pas non-speciale. Cela montre que

$$O_2(\mathbb{R})^-.M^- \subset O_2(\mathbb{R})^+ \Longrightarrow O_2(\mathbb{R})^- \subset O_2(\mathbb{R})^+.(M^-)^{-1} = O_2(\mathbb{R})^+.M^-$$

(car $(M^-)^{-1} = M^-$) et donc

$$O_2(\mathbb{R})^- = O_2(\mathbb{R})^+.M^- \text{ et on a de meme } O_2(\mathbb{R})^- = M^-.O_2(\mathbb{R})^+.$$

Ainsi pour $M \in O_2(\mathbb{R})^-$, il existe $M^+ \in O_2(\mathbb{R})^+$ tel que $M = M^+.M^-$. L'element $M^+$ est unique car equal a $M.M^{--1}$.

–Montrons que le groupe $O_2(\mathbb{R})^+$ est distingue:

$$\forall M \in O_2(\mathbb{R}),\ \mathrm{ad}(M)(O_2(\mathbb{R})^+) = MO_2(\mathbb{R})^+M^{-1} = O_2(\mathbb{R})^+.$$

Si $M \in O_2(\mathbb{R})^+$ c'est evident. Si $M \in O_2(\mathbb{R})^-$ on a

$$MO_2(\mathbb{R})^+M^{-1} = O_2(\mathbb{R})^-M^{-1} = O_2(\mathbb{R})^+.M.M^{-1} = O_2(\mathbb{R})^+.$$

Soit $M$ un matrice orthogonale; si $M$ est non-speciale est est le produit d'une matrice non-speciale: elle-meme. Si $M$ est orthogonale, soit $M^-$ une matrice non-speciale fixee quelconque alors

$$M^-.O_2(\mathbb{R})^- = M^-.M^-.O_2(\mathbb{R})^+ = O_2(\mathbb{R})^+ \ni M$$

Ainsi $M$ s'ecrit sous la forme $M^-.M'$ avec $M' \in O_2(\mathbb{R})^-$ et c'est donc bien le produit de deux matrices non-speciales.

□

**Preuve**: (alternative) Toute matrice de $O_2(\mathbb{R})$ est inversible et son inverse est sa transposee ${}^tM$ qui appartient a $O_2(\mathbb{R})$; donc $O_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ et est stable par inversion.

– Si $M, N \in \mathrm{O}_2(\mathbb{R})$, alors

$$(M.N)^t(M.N) = M.N.{}^tN.{}^tM = M.\mathrm{Id}_2.{}^tM = M.{}^tM = \mathrm{Id}_2$$

donc l'inverse de $M.N$ est sa transposee ce qui implique que $M.N$ est orthogonale. Ainsi $\mathrm{O}_2(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

– On rappelle que le determinant $\det : \mathrm{GL}_2(\mathbb{R}) \mapsto \mathbb{R}^\times$ verifie

$$\det(MN) = \det(M)\det(N),\ \det(M^{-1}) = \det(M)^{-1}.$$

En d'autre terme c'est un morphisme du groupe $(\mathrm{GL}_2(\mathbb{R}), \times)$ vers le groupe multiplicatif $(\mathbb{R}^\times, \times)$. En particulier la restriction de det au sous-groupe $\mathrm{O}_2(\mathbb{R})$ est un morphisme de groupes (dont image est le sous-groupe d'ordre 2 $\{\pm 1\}$). L'ensemble des matrices speciales orthogonales

$$\mathrm{O}_2(\mathbb{R})^+ = \{M \in \mathrm{O}_2(\mathbb{R}),\ \det M = 1\} = \ker(\det(\cdot)_{|\mathrm{O}_2(\mathbb{R})})$$

est le noyau de ce morphisme (restreint au sous-groupe $\mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$), c'est donc un sous-groupe qui est de plus distingue.

– Soit $M^- \in \mathrm{O}_2(\mathbb{R})^-$ (par exemple $w = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) et $M^+ \in \mathrm{O}_2(\mathbb{R})^+$ alors $M = M^+.M^-$ verifie

$$\det(M) = \det(M^+)\det(M^-) = -1$$

et $M \in \mathrm{O}_2(\mathbb{R})^-$: on a $\mathrm{O}_2(\mathbb{R})^+.M^- \subset \mathrm{O}_2(\mathbb{R})^-$. Reciproquement soit $M \in \mathrm{O}_2(\mathbb{R})^-$ et $M' = M.(M^-)^{-1}$ alors

$$\det(M') = \det(M)\det((M^-)^{-1}) = -1.-1 = 1$$

et $M' \in \mathrm{O}_2(\mathbb{R})^+$ et $M = M'.M^-$ donc $\mathrm{O}_2(\mathbb{R})^- \subset \mathrm{O}_2(\mathbb{R})^+.M^-$ et $\mathrm{O}_2(\mathbb{R})^- = \mathrm{O}_2(\mathbb{R})^+.M^-$. De meme on montre que $\mathrm{O}_2(\mathbb{R})^- = M^-.\mathrm{O}_2(\mathbb{R})^+$.

□

## 3. Classification des isometries lineaires

On a vu que l'application

$$\begin{array}{ccc} \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}} & \mapsto & \mathrm{O}_2(\mathbb{R}) \\ \phi & \mapsto & M_\phi \end{array}$$

qui a une isometrie lineaire associe sa matrice (dans la base $(\mathbf{e}_1, \mathbf{e}_2)$) est une bijection. On defini alors les isometries lineaires speciales ou non-speciales comme etant celles donc la matrice associee est speciale ou non:

Définition 3.2. *On notera*

$$\mathrm{Isom}(\mathbb{R}^2)^\pm_{\mathbf{0}} = \{\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}},\ M_\phi \in \mathrm{O}_2(\mathbb{R})^\pm\}$$

*les sous-ensembles des isometries lineaires speciales (resp. non-speciales). On a donc*

$$\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}} = \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}} \sqcup \mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}.$$

On deduit du Theoreme 3.7 le

Théorème 3.8. *On a les proprietes suivantes*

1. *L'ensemble des isometrie lineaires speciales* $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ *est un sous-groupe distingue du groupe* $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ *des isometries lineaires.*
2. *Le groupe* $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ *est commutatif.*

(3) *L'ensemble des isometrie lineaires non-speciales* $\mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}$ *est le translate pour le composition (a gauche ou a droite) de* $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ *par n'importe quelle isometrie lineaire non-speciale :*

$\forall \phi^- \in \mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}$, *on a* $\mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}} = \phi^- \circ \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}} = \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}.\phi^-$.

*En d'autres termes, etant donne* $\phi^- \in \mathrm{O}_2(\mathbb{R})^-$, *toute isometrie lineaire non-speciale est de la forme* $\phi^- \circ \phi^+$ *(resp.* $\phi'^+ \circ \phi^-$*) pour un unique* $\phi^+$ *(resp.* $\phi'^+$*) de* $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$.

(4) *Une isometrie lineaire non-speciale est d'ordre 2:* $\forall \phi \in \mathrm{Isom}(\mathbb{R}^2)^-$, *on a*

$$\phi \neq \mathrm{Id},\ \phi \circ \phi = \mathrm{Id}.$$

(5) *Toute isometrie lineaire s'ecrit comme produit de une ou deux isometrie lineaires non-speciales. En particulier le groupe* $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ *est engendre par* $\mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}$.

**3.1. Point fixes des isometries lineaires.** On va maintenant classifier les differentes isometries lineaires. On effectue cette classification a l'aide de leurs points fixes.

DÉFINITION 3.21. *Soit* $X$ *un ensemble et* $\phi \in \mathrm{Bij}(X)$ *une bijection sur cet ensemble; l'ensemble des points fixes de* $\phi$ *est defini par*

$$\mathrm{Fix}(\phi) = \{x \in X,\ \phi(x) = x\}.$$

On considere le cas $X = \mathbb{R}^2$ et $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$.

PROPOSITION 3.15. *Soit* $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ *une isometrie lineaire alors l'ensemble de ses points fixes* $\mathrm{Fix}(\phi)$ *est un sous-espace vectoriel de* $\mathbb{R}^2$ *et donc est soit*

$$\{\mathbf{0}\},\ \textit{Une droite } \mathbb{R}.\vec{u},\ \mathbb{R}^2.$$

**Preuve**: On a

$$\vec{x} \in \mathrm{Fix}(\phi) \Longleftrightarrow \phi(\vec{x}) = \vec{x} \Longleftrightarrow \phi(\vec{x}) - \vec{x} = (\phi - \mathrm{Id}_{\mathbb{R}^2})(\vec{x}) = \mathbf{0}.$$

ainsi

$$\mathrm{Fix}(\phi) = \ker(\phi - \mathrm{Id}_{\mathbb{R}^2})$$

: c'est donc un sous-espace vectoriel de $\mathbb{R}^2$ et sa dimension est $0, 1$ ou $2$. □

PROPOSITION 3.16. *Soit* $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ *une isometrie lineaire alors un et un seul des cas suivant se presente*

- $\phi = \mathrm{Id}$ *et* $\mathrm{Fix}(\phi) = \mathbb{R}^2$,
- $\phi \in \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ *et* $\mathrm{Fix}(\phi) = \{\mathbf{0}\}$,
- $\phi \in \mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}$ *et* $\mathrm{Fix}(\phi) = \mathbb{R}.\vec{u}$ *avec* $\vec{u} \neq \mathbf{0}$.

**Preuve**: Soit $M$ la matrice associee a $\phi$; l'ensemble des points fixes $\mathrm{Fix}(\phi)$ est l'ensemble des solution du systeme lineaire

$$M.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \Longleftrightarrow \begin{cases} (a-1)x + by = 0 \\ cx + (d-1)y = 0 \end{cases},$$

- Si $\phi = \mathrm{Id}$, alors $a - 1 = b = c = d - 1 = 0$ et $\mathrm{Fix}(\phi) = \mathbb{R}^2$.
- Supposons $\phi$ speciale et $\neq \mathrm{Id}$ le systeme devient ($\mathrm{c}^2 + \mathrm{s}^2 = 1$)

$$\begin{cases} (\mathrm{c}-1)x - \mathrm{s}y = 0 \\ \mathrm{s}x + (\mathrm{c}-1)y = 0 \end{cases}$$

et le determinant de ce systeme vaut

$$(\mathrm{c}-1)^2+\mathrm{s}^2\neq 0$$

(car sinon $\mathrm{c}-1=0=\mathrm{s}$ ce qui est exclu) dont la seule solution est $\mathbf{0}$. Alternativement on a

$$0=(\mathrm{c}-1)((\mathrm{c}-1)x-\mathrm{s}y)+\mathrm{s}(\mathrm{s}x+(\mathrm{c}-1)y)=((\mathrm{c}-1)^2+\mathrm{s}^2)x$$

et donc $x=0$ ce qui implique $y=0$.

– Supposons $\phi$ non-speciale, le systeme devient $(\mathrm{c}^2+\mathrm{s}^2=1)$

$$\begin{cases}(\mathrm{c}-1)x+\mathrm{s}y=0\\ \mathrm{s}x-(\mathrm{c}+1)y=0\end{cases}$$

et le determinant de ce systeme vaut

$$(\mathrm{c}^2-1)-\mathrm{s}^2=0.$$

Le systeme est degenere (les deux lignes sont proportionelles) mais le systeme est non-trivial (si $\mathrm{s}=0$ alors $\mathrm{c}-1$ ou $\mathrm{c}+1$ est non-nul) et donc le systeme est equivalent a une de ses lignes (une de celles qui est non-nulle). L'ensemble des solutions est donc de la forme $\mathbb{R}\vec{u}$ avec $\nu=(-\mathrm{s},\mathrm{c}-1)$ si $(\mathrm{c},\mathrm{s})\neq(1,0)$ et $\vec{u}=(1,0)$ si $(\mathrm{c},\mathrm{s})=(1,0)$. □

**3.2. Les symetries.** On etudie le cas ou $\phi$ est non-speciale.

LEMME 3.3. *Soit $\vec{u}\in\mathbb{R}^2-\{\mathbf{0}\}$ un vecteur non-nul l'ensemble des vecteurs perpendiculaires à $\vec{u}$,*

$$\vec{u}^{\perp}=\{\vec{v},\ \langle\vec{u},\vec{v}\rangle=0\}=\mathbb{R}.\vec{v}$$

*est une droite vectorielle (ie. un sous-espace vectoriel de dimension 1.)*

PREUVE. Si $\vec{u}=(a,b)$ les elements de $\vec{u}^{\perp}$ sont les vecteurs $\vec{v}=(x,y)$ verifiant le systeme lineaire

$$ax+by=0$$

c'est a dire l'ensemble

$$\mathbb{R}(-b,a)=\{\lambda(-b,a),\ \lambda\in\mathbb{R}\}.$$

□

THÉORÈME 3.9. *Soit $\phi\in\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}^-$ et $\mathrm{Fix}(\phi)=\mathbb{R}\vec{u}$ la droite de ces points fixes. Soit $\vec{v}$ un vecteur non-nul perpendiculaire a $\vec{u}$ alors on a pour tout $\vec{w}\in\mathbb{R}^2$*

$$\phi(\vec{w})=\vec{w}-2\frac{\langle\vec{w},\vec{v}\rangle}{\langle\vec{v},\vec{v}\rangle}\vec{v}.$$

*En particulier*

$$\phi(\vec{u})=\vec{u},\ \phi(\vec{v})=-\vec{v}. \tag{3.1}$$

*Reciproquement pour $\vec{v}\neq 0$, l'application $\phi:\mathbb{R}^2\to\mathbb{R}^2$ donnee par*

$$\phi(\vec{w})=\vec{w}-2\frac{\langle\vec{w},\vec{v}\rangle}{\langle\vec{v},\vec{v}\rangle}\vec{v}$$

*est une isometrie lineaire non-speciale.*

**Preuve**: Considerons $\phi(\vec{v})$: on a

$$\langle \phi(\vec{v}), \vec{u}\rangle = \langle \phi(\vec{v}), \phi(\vec{u})\rangle = \langle \vec{v}, \vec{u}\rangle = 0$$

donc $\phi(\vec{v}) \in \vec{u}^{\perp}$ et donc

$$\phi(\vec{v}) = \lambda \vec{v},\ \lambda \in \mathbb{R}.$$

On a alors

$$\langle \vec{v}, \vec{v}\rangle = \langle \phi(\vec{v}), \phi(\vec{v})\rangle = \langle \lambda\vec{v}, \lambda\vec{v}\rangle = \lambda^2 \langle \vec{v}, \vec{v}\rangle$$

donc $\lambda = \pm 1$ (car $\langle \vec{v}, \vec{v}\rangle \neq 0$) mais $\lambda \neq 1$ car sinon $\vec{v}$ serait un point fixe et donc proportionnel a $\vec{u}$. On a donc demontre (3.1).

Soit $\vec{w}$ un vecteur quelconque, la paire $(\vec{u}, \vec{v})$ forme une base orthogonale de $\mathbb{R}^2$ et on a donc

$$\vec{w} = \frac{\langle \vec{w}, \vec{u}\rangle}{\langle \vec{u}, \vec{u}\rangle}\vec{u} + \frac{\langle \vec{w}, \vec{v}\rangle}{\langle \vec{v}, \vec{v}\rangle}\vec{v}$$

et

$$\phi(\vec{w}) = \frac{\langle \vec{w}, \vec{u}\rangle}{\langle \vec{u}, \vec{u}\rangle}\phi(\vec{u}) + \frac{\langle \vec{w}, \vec{v}\rangle}{\langle \vec{v}, \vec{v}\rangle}\phi(\vec{v})$$

$$= \frac{\langle \vec{w}, \vec{u}\rangle}{\langle \vec{u}, \vec{u}\rangle}\vec{u} - \frac{\langle \vec{w}, \vec{v}\rangle}{\langle \vec{v}, \vec{v}\rangle}\vec{v} = \vec{w} - 2\frac{\langle \vec{w}, \vec{v}\rangle}{\langle \vec{v}, \vec{v}\rangle}\vec{v}.$$

Reciproquement si $\phi$ est de cette forme elle est lineaire (par bilineaire du produit scalaire) donc $\phi(\mathbf{0}) = \mathbf{0}$ et pour tout $\vec{w} \in \mathbb{R}^2$

$$\langle \phi(\vec{w}), \phi(\vec{w})\rangle = \langle \vec{w}, \vec{w}\rangle + 4\frac{\langle \vec{w}, \vec{v}\rangle^2}{\langle \vec{v}, \vec{v}\rangle^2}\langle \vec{v}, \vec{v}\rangle - 4\frac{\langle \vec{w}, \vec{v}\rangle}{\langle \vec{v}, \vec{v}\rangle}\langle \vec{w}, \vec{v}\rangle = \langle \vec{w}, \vec{w}\rangle$$

donc c'est une isometrie lineaire. Par ailleurs si $\vec{w}$ est perpendiculaire a $\vec{v}$ on a

$$\phi(\vec{w}) = \vec{w} + \mathbf{0} = \vec{w}$$

elle admet donc une droite de points fixes (et pas tout le plan puisque $\phi(\vec{w}) = -\vec{w}$) c'est donc une isometrie non-speciale. □

DÉFINITION 3.3. *Une isometrie lineaire non-speciale dont l'ensemble des points fixes est la droite $\mathbb{R}\vec{u}$ ($\vec{u} \neq \mathbf{0}$) sera appellee la symetrie orthogonale d'axe $\mathbb{R}\vec{u}$.*

*Les isometries lineaires non-speciales sont appellees symetries et les matrices non-speciales, matrices de symetrie.*

**3.3. Explicitation des symetries.** On a le formulaire suivant

THÉORÈME 3.10. *Soit $s$ une symetrie lineaire de matrice associee*

$$M = \begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix}$$

*avec* $\mathrm{c}, \mathrm{s} \in \mathbb{R}$ *verifiants* $\mathrm{c}^2 + \mathrm{s}^2 = 1$. *Les vecteurs non-nuls definis par*

$$\begin{cases} \vec{u} = (1,0),\ \vec{v} = (0,1) & \text{si } \mathrm{c} = 1, \\ \vec{u} = (0,1),\ \vec{v} = (1,0) & \text{si } \mathrm{c} = -1 \\ \vec{u} = (\mathrm{s}, -(\mathrm{c}-1)),\ \vec{v} = (\mathrm{s}, -(\mathrm{c}+1)). \end{cases} \tag{3.2}$$

*verifient*

$$s(\vec{u}) = \vec{u},\ s(\vec{v}) = -\vec{v}$$

*et plus generalement pour tout* $\vec{w} \in \mathbb{R}^2$

$$s(\vec{w}) = \vec{w} - 2\frac{\langle \vec{v}, \vec{w}\rangle}{\|\vec{v}\|^2}\vec{v}. \tag{3.3}$$

*Reciproquement etant donnes deux vecteurs* $\vec{u}, \vec{v}$ *perpendiculaires non nuls et*

$$\mathrm{sym}_{\vec{u}} : \vec{w} \mapsto \vec{w} - 2\frac{\langle \vec{v}, \vec{w}\rangle}{\|\vec{v}\|^2}\vec{v}$$

*la symetrie correspondante; si les composantes de* $\vec{v}$ *sont* $\vec{v} = (C, S)$*, les composantes* c *et* s *de la matrice* $M$ *de* $\mathrm{sym}_{\vec{u}}$ *sont de la forme*

$$\mathrm{c} = 1 - 2\frac{C^2}{C^2+S^2},\ \mathrm{s} = -2\frac{CS}{C^2+S^2}. \tag{3.4}$$

**Preuve**: Pour trouver $\vec{u}$ et $\vec{v}$ on doit resoudre les systeme lineaire

$$\begin{cases}(c-1)x + sy = 0\\ sx - (c+1)y = 0\end{cases} \qquad \begin{cases}(c+1)x' + sy' = 0\\ sx' - (c-1)y' = 0\end{cases}.$$

Si $c = \pm 1$, on a $s = 0$ et des solutions sont pour $c = 1$, de la forme

$$\vec{u} = \alpha\mathbf{e}_1 = (\alpha, 0),\ \vec{v} = \beta\mathbf{e}_2 = (0, \beta),\ \alpha, \beta \in \mathbb{R}.$$

et pour $c = -1$

$$\vec{u} = \alpha\mathbf{e}_2 = (0, \alpha),\ \vec{v} = \beta\mathbf{e}_1 = (\beta, 0),\ \alpha, \beta \in \mathbb{R}.$$

Si $\mathrm{c} \neq \pm 1$, utilisant le fait que

$$\mathrm{c}^2 + \mathrm{s}^2 - 1 = (\mathrm{c}-1)(\mathrm{c}+1) + \mathrm{s}^2 = 0$$

on trouve que ses systemes sont equivalents a

$$\begin{cases}(\mathrm{c}-1)x + \mathrm{s}y = 0\\ 0 = 0\end{cases} \qquad \begin{cases}(\mathrm{c}+1)x' + \mathrm{s}y' = 0\\ 0 = 0\end{cases}$$

et les solutions sont de la forme

$$\vec{u} = \alpha(\mathrm{s}, -(\mathrm{c}-1)),\ \vec{v} = \beta(\mathrm{s}, -(\mathrm{c}+1)),\ \alpha, \beta \in \mathbb{R}.$$

On peut verifier directement que $\vec{u}$ et $\vec{v}$ sont bien perpendiculaire mais un argument plus general (sans coordonnees) sera utile plus tard: on a

$$\langle \vec{u}, \vec{v}\rangle = \langle s(\vec{u}), s(\vec{v})\rangle = \langle \vec{u}, -\vec{v}\rangle = -\langle \vec{u}, \vec{v}\rangle$$

et donc $\langle \vec{u}, \vec{v}\rangle = 0$. □

Reciproquement, etant donne $\vec{u}$ et $\vec{v}$ deux vecteurs perpendiculaires non-nuls, considerons la symetrie orthogonale (3.3); on veut calculer sa matrice. Notons que cette definition ne depend pas du choix du vecteur orthogonal $\vec{v}$: si $\vec{v}' \perp \vec{u}$ alors $\vec{v}' = \lambda\vec{v}$ pour un certain $\lambda \neq 0$ et

$$\frac{\langle \vec{u}, \vec{v}'\rangle}{\|\vec{v}'\|^2}\vec{v}' = \frac{\langle \vec{u}, \lambda\vec{v}\rangle}{\|\lambda\vec{v}\|^2}\lambda\vec{v} = \frac{\lambda^2\langle \vec{u}, \vec{v}\rangle}{\lambda^2\|\vec{v}\|^2}\vec{v}.$$

On peut donc supposer que $\|\vec{v}\| = 1$ et donc

$$\vec{v} = (C, S) = (\langle \vec{v}, \mathbf{e}_1\rangle, \langle \vec{v}, \mathbf{e}_2\rangle),\ C^2 + S^2 = 1.$$

Calculons

$$\mathrm{sym}_{\vec{u}}(\mathbf{e}_1) = \mathbf{e}_1 - 2C(C\mathbf{e}_1 + S\mathbf{e}_2) = (1 - 2C^2)\mathbf{e}_1 - 2CS\mathbf{e}_2 = \mathrm{c}\mathbf{e}_1 + \mathrm{s}\mathbf{e}_2$$

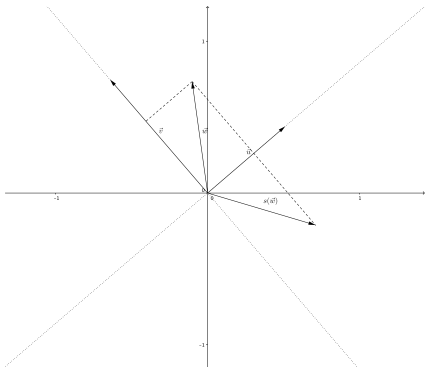

FIGURE 1. Exemple de symetrie lineaire.

$$\mathrm{sym}_{\vec{u}}(\mathbf{e}_2) = \mathbf{e}_2 - 2S(C\mathbf{e}_1 + S\mathbf{e}_2) = -2CS\mathbf{e}_1 + (1-2S^2)\mathbf{e}_2 = \mathrm{s}\mathbf{e}_1 - \mathrm{c}\mathbf{e}_2$$

en posant $\mathrm{c} = (1-2C^2)$ et $\mathrm{s} = -2CS$ car

$$(1-2C^2) + (1-2S^2) = 2 - 2(C^2+S^2) = 0.$$

Ainsi la matrice de $\mathrm{sym}_{\vec{u}}$ est de la forme

$$\begin{pmatrix} \mathrm{c} & \mathrm{s} \\ \mathrm{s} & -\mathrm{c} \end{pmatrix} \text{ avec } \mathrm{c}^2 + \mathrm{s}^2 = 1 - 4C^2 + 4C^4 + 4C^2(1-S^2) = 1.$$

□

**3.4. Rotations.** On considere maintenant le cas des isometries speciales

DÉFINITION 3.4. *Une isometrie lineaire speciale $\phi$ sera appellee rotation de centre $\mathbf{0}$. On dira egalement que sa matrice est une matrice de rotation. Le groupe $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ des isometries speciales est encore appele le groupe des rotations de centre $\mathbf{0}$.*

Le groupe des rotations a la propriete fondamentale suivante:

THÉORÈME 3.11. *Soit*

$$\mathbf{C}^1 = \{P \in \mathbb{R}^2,\ d(\mathbf{0}, P) = 1\} = \{(x,y) \in \mathbb{R}^2,\ x^2 + y^2 = 1\}$$

*le cercle unite (le cercle de rayon 1 centre en $\mathbf{0}$). Soient $P, Q \in \mathbf{C}^1$ il existe une unique rotation lineaire $r = r_{P,Q}$ telle que*

$$r(P) = Q.$$

*En particulier, pour tout $P \in \mathbf{C}^1$ (par exemple $P = \mathbf{e}_1 = (1,0)$) l'application*

$$\mathrm{ev}_P : \begin{array}{ccc} \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}} & \mapsto & \mathbf{C}^1 \\ r & \mapsto & r(P) \end{array}$$

*est une bijection.*

**Preuve**: Montrons ce resultat pour $P = \mathbf{e}_1 = (1,0)$. Soit $Q = (\mathrm{c}, \mathrm{s}) \in \mathbf{C}^1$ un point du cercle unite ($\mathrm{c}^2 + \mathrm{s}^2 = 1$) alors la rotation $r_{(0,1),Q}$ de matrice

$$\begin{pmatrix} \mathrm{c} & -\mathrm{s} \\ \mathrm{s} & \mathrm{c} \end{pmatrix}$$

envoie $(1,0)$ sur $Q$ et c'est la seule possible (puisque qu'une matrice de rotation est determinee entierement par sa premiere colonne). En general, soit $P \in \mathbf{C}^1$ un point du cercle alors pour tout point $Q$ la rotation

$$r_{P,Q} = r_{(0,1),Q} \circ r^{-1}_{(0,1),P}$$

est l'unique rotation envoyant $P$ sur $Q$: si $r(P) = r'(P) = Q$ alors $r^{-1} \circ r'$ a $\mathbf{0}$ et $P$ comme point fixe et est donc l'identite. □

Le Theoreme precedent permet donc d'identifier le groupe des rotations lineaires avec cercle unite. En particulier cette identification confere au cercle unite $\mathbb{C}^1$ une structure de groupe commutatif.

On reverra plus tard cette identification et cette structure de groupe avec les nombres complexes.

3.4.1. *Angle de deux vecteurs.*

Définition 3.5. *L'angle*

- *de deux vecteurs unitaire $\vec{u}, \vec{v} \in \mathbf{C}^1$ (de longueur 1) est l'unique rotation $r_{\vec{u},\vec{v}}$ qui envoie $\vec{u}$ sur $\vec{v}$.*
- *de deux vecteurs non-nuls, $\vec{u}, \vec{v}$, est l'unique rotation $r_{\vec{u},\vec{v}}$ qui envoie $\vec{u}/\|\vec{u}\|$ sur $\vec{v}/\|\vec{v}\|$.*
- *de deux demi-droites $\mathbb{R}_{\geqslant 0}\vec{u}$ et $\mathbb{R}_{\geqslant 0}\vec{v}$ est la rotation $r_{\vec{u},\vec{v}}$ qui envoie $\vec{u}/\|\vec{u}\|$ sur $\vec{v}/\|\vec{v}\|$ et donc $\mathbb{R}_{\geqslant 0}\vec{u}$ sur $\mathbb{R}_{\geqslant 0}\vec{v}$. On note cet angle*

$$\widehat{\vec{u}\vec{v}}.$$

- *de deux segments orientes $[P,Q]$ et $[P',Q']$ est l'angle*

$$\widehat{\overrightarrow{PQ}\overrightarrow{P'Q'}}.$$

- *de deux droites passant par l'origine $\mathbb{R}\vec{u}, \mathbb{R}\vec{v}$ est l'ensemble des deux rotations*[3] *$\{r_{\vec{u},\vec{v}}, -r_{\vec{u},\vec{v}}\}$ qui envoient la droite $\mathbb{R}\vec{u}$ sur la droite $\mathbb{R}\vec{v}$.*

*On fait egalement les definitions suivantes*

- *Un angle entre vecteurs ou deux demi-droites sera aussi appelle "angle oriente". Un angle entre deux droites (ie. un ensemble de deux angles orientes) sera appelle "angle non-oriente".*
- *L'ensemble des angles (orientes) est l'ensemble des rotations $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$; c'est donc un groupe abelien et etant donne $r, r'$ deux angles, la "somme" de ces angles est la rotation composee $r \circ r' = r' \circ r$.*
- *On defini de meme la somme de deux angles non-orientes comme la paire $\{r \circ r', -r \circ r'\}$.*
- *On peut identifier une rotation $r$ (donc un angle) avec sa matrice $M_r = \begin{pmatrix} \mathrm{c} & -\mathrm{s} \\ \mathrm{s} & \mathrm{c} \end{pmatrix}$ et donc representer un angle par le vecteur de $\mathbf{C}^1$, $(\mathrm{c}, \mathrm{s})$. Le nombre $\mathrm{c}$ s'appelle le cosinus de l'angle $r$ et le nombre $\mathrm{s}$ s'appelle son sinus et on les note*

$$\mathrm{c} = \cos(r),\ \mathrm{s} = \sin(r).$$

[3] Si $r$ est une rotation de matrice $M$, $-r$ est la rotation de matrice $-M$

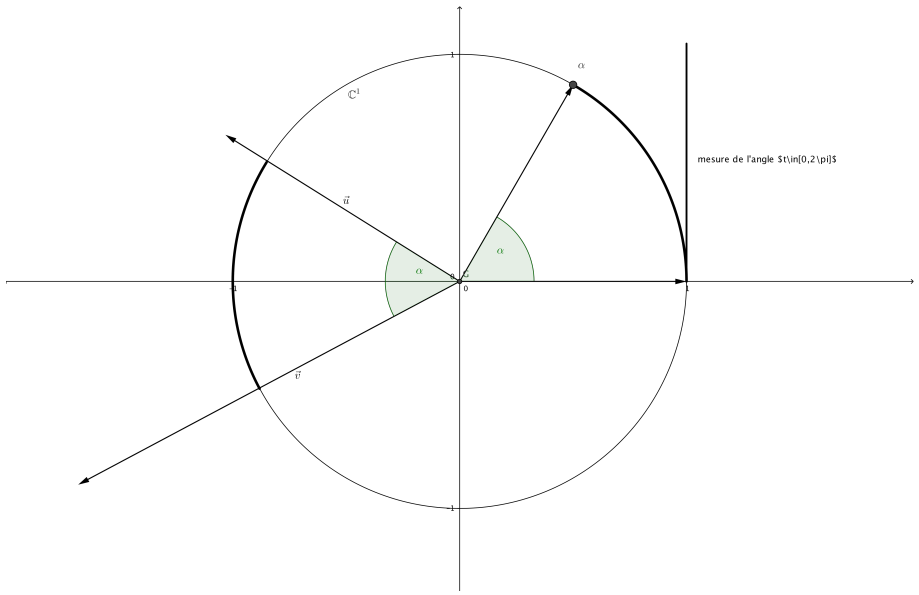


FIGURE 2. Deux paires de vecteurs representant le meme angle

*Avec cette representation sous la forme cosinus, sinus, la "somme" des deux angles* $(\mathrm{c}, \mathrm{s})$ *et* $(\mathrm{c}', \mathrm{s}')$ *est l'angle*

$$(\mathrm{c}", \mathrm{s}") = (\mathrm{cc}' - \mathrm{ss}', \mathrm{sc}' + \mathrm{cs}').$$

On a les correspondance suivante entre rotations et angles exprimes en degree radians

- Angle 0 $\iff r = \mathrm{Id}$, $(\mathrm{c}, \mathrm{s}) = (1, 0)$.
- Angle 180 ou $\pi \iff r = -\mathrm{Id}$ , $(\mathrm{c}, \mathrm{s}) = (-1, 0)$.
- Angle 90 ou $\pi/2 \iff$ rotation de parametres $(\mathrm{c}, \mathrm{s}) = (0, 1)$.
- Angle 270 ou $3\pi/2 \iff$ rotation de parametres $(\mathrm{c}, \mathrm{s}) = (0, -1)$.
- Angle 120 ou $2\pi/3 \iff$ rotation de parametres $(\mathrm{c}, \mathrm{s}) = (-1/2, \sqrt{3}/2)$.
- Angle 60 ou $2\pi/6 \iff$ rotation de parametres $(\mathrm{c}, \mathrm{s}) = (1/2, \sqrt{3}/2)$.
- Angle 30 ou $2\pi/12 \iff$ rotation de parametres $(\mathrm{c}, \mathrm{s}) = (\sqrt{3}/2, 1/2)$.

EXERCICE 3.2. Etant donne une rotation $r$, montrer qu'il existe deux rotations $r^{1/2}, -r^{1/2}$ telles que

$$(r^{1/2})^2 = (-r^{1/2})^2 = r;$$

on dira que la paire $\{r^{1/2}, -r^{1/2}\}$ est l'angle moitie.

3.4.2. *Formule du produit scalaire.*

PROPOSITION 3.17. *Soit* $\vec{u}$ *et* $\vec{v}$ *deux vecteurs non-nul et* $r = \widehat{\vec{u}\vec{v}}$ *alors on a*

$$\frac{\langle \vec{u}, \vec{v} \rangle}{\|\vec{u}\| \|\vec{v}\|} = \cos(r)$$

**Preuve**: Exercice. □

DÉFINITION 3.6. *Soient* $r, r'$ *deux angles (deux rotations lineaires).*

- *Si* $r' = r^{-1}$ *on dit que les angles sont inverses l'une de l'autre.*

- *Si* $r' = -r$ *on dit que les angles sont opposes.*
- *Si* $r.r' = -\mathrm{Id}$ *(ie.* $r' = -r^{-1}$*) on dit que les angles sont supplementaires (*$-\mathrm{Id}$ *est la rotation d'angle* 180 *degrees).*
- *Si* $r.r'$ *est la rotation de parameter* $(\mathrm{c}, \mathrm{s}) = (0, 1)$ *ont dit que les angles sont complementaires (c'est la rotation d'angle* 90 *degrees.)*

3.4.3. *Mesure d'un angle.*

Définition 3.7. *La mesure d'un angle* $r$ *represente par* $(\mathrm{c}, \mathrm{s})$ *est la longueur de l'arc du cercle unite allant de* $(1, 0)$ *a* $(\mathrm{c}, \mathrm{s})$ *parcouru dans le sens inverse des aiguilles d'une montre; c'est un nombre reel compris entre* 0 *et* $2\pi$ *(la longueur du cercle unite).*

Le probleme avec cette definition est qu'il faut d'abord definir les notiens de

- "longueur de l'arc du cercle unite allant de...",
- "parcouru dans le sens inverse des aiguilles d'une montre"

Pour cela on a besoin de la notion de courbe parametree et de longueur d'une telle courbe.

Définition 3.8. *Soit* $\mathbb{R}/2\pi\mathbb{Z}$ *l'ensemble* $[0, 2\pi[$ *muni de la loi de composition*

$$\theta \oplus \theta' = \text{ l'unique element de l'intersection } [0, 2\pi[ \cap \theta + \theta' + 2\pi\mathbb{Z}.$$

*Alors*

$$\mathbb{R}/2\pi\mathbb{Z} = ([0, 2\pi[, \oplus)$$

*est un groupe abelien en bijection avec* $\mathrm{C}^1$ *et* $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$.

**3.5. Classification des isometries affines.** On classifie maintenant les isometrie affines generales composees d'une translation et d'une isometrie lineaire:

$$\phi = t_{\phi(\mathbf{0})} \circ \phi_0.$$

On defini d'abord les notion d'isometries affines speciales et non-speciales

Définition 3.9. *Une isometrie affine generale (pas forcement lineaire)* $\phi = t_{\phi(\mathbf{0})} \circ \phi_0$ *sera dite speciale (resp. non-speciale) si sa partie lineaire est speciale (resp. non-speciale).*

- *Une isometrie speciale sera egalement appellee rotation affine.*
- *Une isometrie non-speciale sera egalement appellee symetrie affine.*

*On notera*

$$\mathrm{Isom}(\mathbb{R}^2)^+ \text{ et } \mathrm{Isom}(\mathbb{R}^2)^-$$

*les ensembles d'isometries speciales ou non (rotations ou symetries affines). On a donc*

$$\mathrm{Isom}(\mathbb{R}^2) = \mathrm{Isom}(\mathbb{R}^2)^+ \sqcup \mathrm{Isom}(\mathbb{R}^2)^-.$$

Le resultat suivant est en grande partie laisse en exercice:

Théorème 3.12. *L'ensemble* $\mathrm{Isom}(\mathbb{R}^2)^+$ *est un sous-groupe distingue du groupe* $\mathrm{Isom}(\mathbb{R}^2)$ *et l'ensemble* $\mathrm{Isom}(\mathbb{R}^2)^-$ *est le translate (a gauche ou a droite) de* $\mathrm{Isom}(\mathbb{R}^2)^+$ *par un element quelconque de* $\mathrm{Isom}(\mathbb{R}^2)^-$*: pour toute symetrie affine* $s \in \mathrm{Isom}(\mathbb{R}^2)^-$*, on a*

$$\mathrm{Isom}(\mathbb{R}^2)^- = s \circ \mathrm{Isom}(\mathbb{R}^2)^+ = \mathrm{Isom}(\mathbb{R}^2)^\circ s.$$

**Preuve**: Exercice; Indication: utiliser le theoreme de structure du groupe des isometries directes et la fait que l'application partie lineaire $\mathrm{lin} : \mathrm{Isom}(\mathbb{R}^2) \to \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ est un morphisme de groupe surjectif. □

Remarque 3.1. Attention !

- Le groupe $\mathrm{Isom}(\mathbb{R}^2)^+$ n'est pas commutatif.
- Une symetrie affine n'est pas forcement d'ordre 2.

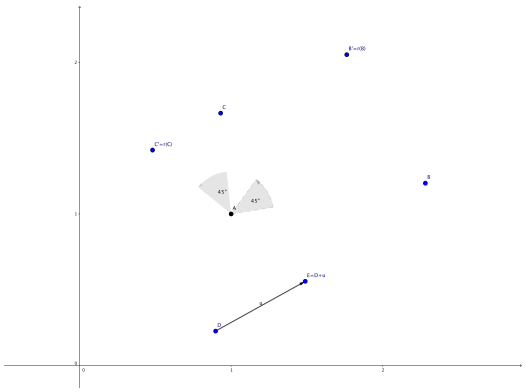

FIGURE 3. Exemple de translation, rotation ...

### 3.6. Rotations affines.

THÉORÈME 3.13. *Soit $r \in \mathrm{Isom}(\mathbb{R}^2)^+$ une rotation affine.*

*–Si la partie lineaire de $r$ est l'identite $r$ est une translation et $\mathrm{Fix}(r) = \emptyset$ sauf si le vecteur de translation est le vecteur nul: on a alors $r = \mathrm{Id}_{\mathbb{R}^2}$ et $\mathrm{Fix}(r) = \mathbb{R}^2$.*

*–Si la partie lineaire de $r$ n'est pas l'identite l'ensemble $\mathrm{Fix}(r)$ des points fixes de $r$ est reduit a un seul point; on l'appelle le centre de $r$ et on le notera $P_r$.*

PREUVE. Ecrivons

$$r = t_{r(\mathbf{0})} \circ r_0,$$

$r(\mathbf{0}) = (x_0, y_0)$ et

$$M = M_{r_0} = \begin{pmatrix} \mathrm{c} & -\mathrm{s} \\ \mathrm{s} & \mathrm{c} \end{pmatrix},\ \mathrm{c}^2 + \mathrm{s}^2 = 1$$

la matrice de la partie lineaire de $r$; on a $\mathrm{c} \neq 1$ (sinon $M$ serait la matrice identite). Nous devons resoudre l'equation

$$(x, y) = (x_0 + \mathrm{c}x - \mathrm{s}y, y_0 + \mathrm{s}x + \mathrm{c}y)$$

ou encore

$$\begin{cases} (1-\mathrm{c})x + \mathrm{s}y = x_0 \\ -\mathrm{s}x + (1-\mathrm{c})y = y_0 \end{cases} \iff \begin{cases} ((1-\mathrm{c})^2 + \mathrm{s}^2)x = (1-\mathrm{c})x_0 - \mathrm{s}y_0 \\ ((1-\mathrm{c})^2 + \mathrm{s}^2)y = (1-\mathrm{c})y_0 + \mathrm{s}x_0 \end{cases} \iff \begin{cases} x = \frac{(1-\mathrm{c})x_0 - \mathrm{s}y_0}{(1-\mathrm{c})^2+\mathrm{s}^2} \\ y = \frac{(1-\mathrm{c})y_0 + \mathrm{s}x_0}{(1-\mathrm{c})^2+\mathrm{s}^2} \end{cases}$$

car $(1-\mathrm{c})^2 + \mathrm{s}^2 > 0$. Le point fixe est donc unique. □

PROPOSITION 3.18. *Soit $P \in \mathbb{R}^2$ et $\mathrm{Isom}(\mathbb{R}^2)^+_P$ l'ensemble des rotations de centre $P$ alors $\mathrm{Isom}(\mathbb{R}^2)^+_P$ est un groupe conjugue au groupe des rotations lineaires $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ (en particulier ils sont isomorphes.)*

**Preuve**: Exercice; considerer la conjugaison par la translation qui envoie $\mathbf{0}$ sur $P$. □

**3.7. Symetries affines.** Soit $s = t_{s(\mathbf{0})} \circ s_0$ une symetrie affine de partie lineaire $s_0$ d'axe $\mathbb{R}.\vec{u}$ et $\vec{v} \neq \mathbf{0}$ perpendiculaire a $\vec{u}$.

THÉORÈME 3.14. *L'ensemble des points fixes $\mathrm{Fix}(s)$ est soit l'ensemble vide, soit une droite affine (la translatee d'une droite vectorielle). Ce dernier cas a lieu si et seulement si $s(\mathbf{0})$ est perpendiculaire a l'axe $\mathbb{R}.\vec{u}$.*

*Dans ce cas* $\mathrm{Fix}(s)$ *est la droite affine*

$$D_s = D(P_0, \vec{u}) = P_0 + \mathbb{R}\vec{u}$$

*paralelle a l'axe* $\mathbb{R}\vec{u}$ *et passant le point* $P_0 = \frac{1}{2}s(\mathbf{0})$*, milieu du segment* $[\mathbf{0}, s(\mathbf{0})]$*. L'image* $s(P)$ *d'un point quelconque* $P \in \mathbb{R}^2$ *est alors caracterisee uniquement par les proprietes suivantes*

- *Le vecteur* $\overrightarrow{Ps(P)}$ *est perpendiculaire a* $\vec{u}$
- *Le milieu* $\frac{1}{2}(P + s(P))$ *du segment* $[P, s(P)]$ *appartient a la droite* $D_s$*.*

*La droite* $D_s$ *est l'axe de la symetrie* $s$ *et* $s$ *est d'ordre* 2*:*

$$s \circ s = \mathrm{Id}.$$

Définition 3.10. *Une symetrie affine* $s$ *est appellee:*

- *symetrie glissee si* $\mathrm{Fix}(s) = \emptyset$*.*
- *symetrie orthogonale (ou axiale) si* $\mathrm{Fix}(s)$ *est une droite affine. Cette droite l'axe de la symetrie.*

Preuve. On a vu que tout point $P$ s'ecrit de maniere unique

$$P = \lambda(P)\vec{u} + \mu(P)\vec{v} = \frac{\langle P, \vec{u}\rangle}{\|\vec{u}\|^2}\vec{u} + \frac{\langle P, \vec{v}\rangle}{\|\vec{v}\|^2}\vec{v}.$$

La symetrie $s = t_{s(\mathbf{0})} \circ s_0$ s'exprime de la maniere suivante (cf. (3.3))

$$s(P) = s(\mathbf{0}) + P - 2\frac{\langle P, \vec{v}\rangle}{\|\vec{v}\|^2}\vec{v} = s(\mathbf{0}) + \frac{\langle P, \vec{u}\rangle}{\|\vec{u}\|^2}\vec{u} - \frac{\langle P, \vec{v}\rangle}{\|\vec{v}\|^2}\vec{v}.$$

Resolvons l'equation

$$s(P) = P \Longleftrightarrow s(\mathbf{0}) = 2\frac{\langle P, \vec{v}\rangle}{\|\vec{v}\|^2}\vec{v} \tag{3.5}$$

Ainsi l'equation n'a de solution que si $s(\mathbf{0})$ est colineaire a $\vec{v}$ (ie. perpendiculaire a $\vec{u}$). Dans ce cas on obtient On obtient donc

$$\frac{1}{2}s(\mathbf{0}) = \frac{\langle P, \vec{v}\rangle}{\|\vec{v}\|^2}\vec{v}$$

et $P$ est de la forme

$$P = \frac{1}{2}s(\mathbf{0}) + \lambda\vec{u},\ \lambda \in \mathbb{R}.$$

$P$ appartient donc a la droite $\frac{1}{2}s(\mathbf{0}) + \mathbb{R}\vec{u}$; reciproquement on verifie de meme que tout point de cette droite verifie l'equation (3.5). D'autre part

$$s(P) - P = \overrightarrow{Ps(P)} = s(\mathbf{0}) - 2\frac{\langle P, \vec{v}\rangle}{\|\vec{v}\|^2}\vec{v}$$

est proportionel a $\vec{v}$ donc perpendiculaire a $\vec{u}$ et le milieu du segment $[Ps(P)]$ verifie bien

$$\frac{1}{2}(P + s(P)) = \frac{1}{2}s(\mathbf{0}) + P - \mu(P)\vec{v} = \frac{1}{2}s(\mathbf{0}) + \lambda(P)\vec{u} \in D(\frac{1}{2}s(\mathbf{0}), \vec{u}).$$

Compte-tenu de la caracterisation de $s(P)$ ($[P, s(P)]$ est perpendiculaire a $\vec{u}$ et son milieu est sur l'axe de $s$) on voit que $s$ envoie $s(P)$ sur $P$ donc $s(s(P)) = P$. □

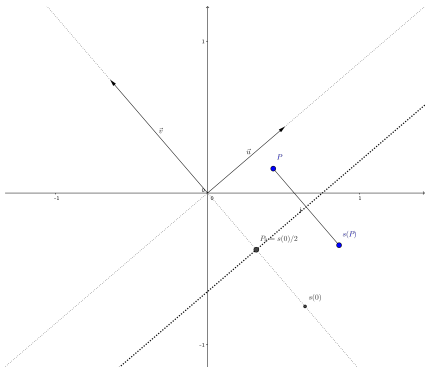

FIGURE 4. Exemple de symetrie affine axiale.

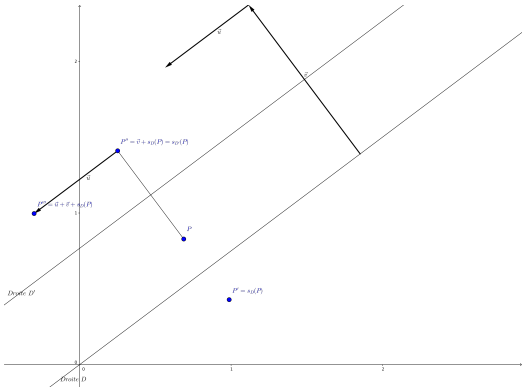

FIGURE 5. Exemple de symetrie affine glissee: $P''' = t_{\vec{u}} \circ t_{\vec{v}} \circ s_D$.

COROLLAIRE 3.1. *Une symetrie affine $s$ se decompose sous la forme suivante:*

$$s = t' \circ s'$$

*ou $t' = t_{\vec{u}'}$ est une translation de vecteur $\vec{u}'$ paralelle a l'axe $\mathbb{R}\vec{u}$ de la partie lineaire de $s$ et $s'$ est une symetrie axiale d'axe paralelle a $\mathbb{R}\vec{u}$. De plus $t'$ et $s'$ commutent.*

*La decomposition est unique et la symetrie $s$ est glissee si et seulement si la translation $t'$ est non-triviale.*

*On a*

$$s^2 = t_{2\vec{u}'}.$$

**Preuve**: Soient $\vec{u}$ et $\vec{v}$ comme ci-dessus. Decomposons $s(\mathbf{0})$ dans la base $(\vec{u}, \vec{v})$

$$s(\mathbf{0}) = \lambda_0\vec{u} + \mu_0\vec{v}$$

alors

$$s = t_{s(\mathbf{0})} \circ s_0 = t_{\lambda_0\vec{u}} \circ (t_{\mu_0\vec{v}} \circ s_0) = t' \circ s'.$$

Par le resultat precedent $s'$ est une symetrie axiale et $s$ est une symetrie axiale si et seulement si $\lambda_0\vec{u} = \mathbf{0}$ (et $s = s'$). Par ailleurs

$$t' \circ s' = t_{\lambda_0\vec{u}} \circ t_{\mu_0\vec{v}} \circ s_0 = t_{\mu_0\vec{v}} \circ s_0 = t_{\mu_0\vec{v}} \circ t_{\lambda_0\vec{u}} \circ s_0 \circ t_{\lambda_0\vec{u}} = s' \circ t'$$

car $(s_0(\vec{u}) = \vec{u})$

$$s_0 \circ t_{\lambda_0 \vec{u}}(\vec{w}) = s_0(\lambda_0 \vec{u} + \vec{w}) = \lambda_0 s_0(\vec{u}) + s_0(\vec{w}) = \lambda_0 \vec{u} + s_0(\vec{w}) = t' \circ s_0(\vec{w}).$$

On a alors par commutation

$$s^2 = t' \circ s' \circ t' \circ s' = t' \circ t' \circ s' \circ s' = t'^2.$$

L'unicite de la decomposition decoule du fait que si $s = t' \circ s'$ alors $s_0 = s'_0$ et de l'unicite de la decomposition d'un vecteur dans une base orthogonale $(\vec{u}, \vec{v})$.

□

3.7.1. *Exemple.* Considerons les deux symetries $s_1$, $s_2$ par rapport aux droites d'equation:

$$3x + 4y = 2,\ -2x + 5y = 3.$$

On veut calculer l'isometrie composee $s_1 \circ s_2$. Il s'agit d'une rotation $r_3$ (car sa partie lineaire composee de deux symetries est une rotation). Les directions perpendiculaires aux axes sont données par les vecteurs

$$\vec{v}_1 = (3, 4),\ \vec{v}_2 = (-2, 5).$$

Ainsi les matrices associés sont données par

$$\begin{pmatrix} c_1 & s_1 \\ s_1 & -c_1 \end{pmatrix},\ \begin{pmatrix} c_2 & s_2 \\ s_2 & -c_2 \end{pmatrix}$$

avec

$$c_1 = \frac{7}{25},\ s_1 = -\frac{24}{25},\ c_2 = \frac{21}{29},\ s_2 = \frac{20}{29}.$$

Ainsi la partie lineaire de $s_1 \circ s_2$ qui est une rotation a pour matrice

$$\begin{pmatrix} c_3 & -s_3 \\ s_3 & c_3 \end{pmatrix} \text{ avec } c_3 = c_1 c_2 + s_1 s_2 = -\frac{333}{725},\ s_3 = s_1 c_2 - c_1 s_2 = -\frac{644}{725}.$$

Soit $P$ l'intersection des deux droites, alors $P$ est un point fixe pour $s_1$ et $s_2$ et donc pour $s_1 \circ s_2$ c'est donc le centre de $r_3$. On resoud donc le systeme

$$3x + 4y = 2,\ -2x + 5y = 3$$

et on trouve

$$P = (\frac{-2}{23}, \frac{13}{23}).$$

## 4. Conclusion

Pour resumer, les isometries du plan sont constituees des

- **translations**: les elements de $T(\mathbb{R}^2)$; elles appartiennent a $\mathrm{Isom}(\mathbb{R}^2)^+$ et ce sont les rotations dont la partie lineaire est l'identite. Elles n'ont aucun point fixe sauf la translation par le vecteur nul $\mathbf{0}$ (c'est l'identite) et alors l'ensemble de ses points fixes est $\mathbb{R}^2$ tout entier.
- **les rotations**: ce sont les elements de $\mathrm{Isom}(\mathbb{R}^2)^+$; elles sont composees d'une translation et d'une rotation lineaire; et si leur partie lineaire n'est pas l'identite (si ce ne sont pas des translations), elles ont exactement un point fixe, le centre de la rotation.

– **les symetries axiales**: elles appartiennent a $\mathrm{Isom}(\mathbb{R}^2)^-$ et sont composees d'une translation et d'une symetrie lineaire telle que le vecteur de la translation est perpendiculaire a celui de l'axe de la symetrie. L'ensemble des points fixes est la droite paralelle a l'axe de la symetrie lineaire et passant par le milieu du segment de translation. Elles sont d'ordre 2.
– **les symetries glissees**: elles appartiennent a $\mathrm{Isom}(\mathbb{R}^2)^-$ et sont composees d'une translation et d'une symetrie lineaire telle que le vecteur de la translation n'est pas perpendiculaire au vecteur directeur de l'axe de la symetrie. Elles sont d'ordre infini (leur carre est une translation par un vecteur non-nul) et n'ont pas de point fixe.

CHAPITRE 4

# Isometries et nombres complexes

Nous commencons par rappeler la construction des nombres complexes.

## 1. Construction des nombres complexes

L'ensemble des nombres complexes $\mathbb{C}$ s'obtient "concretement", comme un sous-anneau de l'anneau des matrices $2 \times 2$: posont

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ qui verifie } I^2 = -\mathrm{Id}_2$$

L'ensemble des nombres complexes est l'ensemble des combinaisons lineaires de Id et $I$, c'est a dire l'ensemble des matrices de la forme

$$Z = x\mathrm{Id} + yI = \begin{pmatrix} x & -y \\ y & x \end{pmatrix},\ x, y \in \mathbb{R}.$$

en d'autre termes

$$\mathbb{C} = \mathbb{R}\mathrm{Id} + \mathbb{R}I \subset \mathrm{M}_2(\mathbb{R}),$$

1.0.1. *Structure d'espace vectoriel.* C'est un $\mathbb{R}$-espace vectoriel de dimension 2 (engendré par la famille libre $(\mathrm{Id}, I)$): en particulier $\mathbb{C}$ est stable par addition et multiplication par les scalaires

$$\forall Z, Z' \in \mathbb{C},\ Z + Z' = \begin{pmatrix} x + x' & -(y + y') \\ y + y' & x + x' \end{pmatrix} = (x + x')\mathrm{Id} + (y + y')I \in \mathrm{C},$$

$$\forall Z \in \mathbb{C},\ \lambda \in \mathbb{R},\ \lambda.Z = \begin{pmatrix} \lambda.x & -\lambda y \\ \lambda y & \lambda x \end{pmatrix} = \lambda x\mathrm{Id} + \lambda yI \in \mathbb{C}.$$

Définition 4.1. *Les coordonnees de $Z \in \mathbb{C}$ dans la base $(\mathrm{Id}, I)$ sont appellees parties reeles et imaginaire de $Z$:*

$$Z = x\mathrm{Id} + yI,\ x = \mathrm{Re}(Z),\ y = \mathrm{Im}(Z).$$

L'application

$$\mathrm{ReIm} : Z = x\mathrm{Id} + yI \in \mathbb{C} \mapsto (x, y) = (\mathrm{Re}Z, \mathrm{Im}\, Z) \in \mathbb{R}^2 \tag{1.1}$$

est un isomorphisme d'espace vectoriels et permet donc d'identifier $\mathbb{C}$ avec le plan reel $\mathbb{R}^2$.

1.0.2. *Structure d'anneau.* Comme $I^2 = -\mathrm{Id} \in \mathbb{C}$ on a pour $Z, Z' \in \mathbb{C}$

$$Z.Z' = (x\mathrm{Id} + yI).(x'\mathrm{Id} + y'I) = (xx' - yy')\mathrm{Id} + (xy' + x'y)I \in \mathrm{C}(\mathbb{R}).$$

Ainsi $\mathbb{C}$ est stable par produit. C'est donc un sous-anneau de $\mathrm{M}_2(\mathbb{R})$ qui est de plus commutatif:

$$\forall Z, Z' \in \mathbb{C},\ Z.Z' = Z'.Z.$$

1.0.3. *Conjugaison complexe.* On a

$$^tI = -I \in \mathbb{C}$$

donc l'ensemble des complexes est stable par l'application de transposition

$$^t. : Z = x\mathrm{Id} + yI \in \mathbb{C} \mapsto {}^tZ = x\mathrm{Id} - yI \in \mathbb{C}.$$

DÉFINITION 4.2. *La restriction de la transposee a* $\mathbb{C}$ *defini une bijection de* $\mathbb{C}$ *sur* $\mathbb{C}$ *(de reciproque la transposee)qu'on l'appelle la conjugaison complexe et on la note*

$$Z \in \mathbb{C} \mapsto \overline{Z} \in \mathbb{C}.$$

On a

$$\overline{Z+Z'} = \overline{Z} + \overline{z'}, \overline{Z.Z'} = \overline{Z'}.\overline{Z} = \overline{Z}.\overline{Z'},\ \overline{\overline{Z}} = Z.$$

Par ailleurs

$$Z.\overline{Z} = (x^2+y^2)\mathrm{Id} = \det(Z)\mathrm{Id}. \tag{1.2}$$

La quantite

$$|Z| := (x^2+y^2)^{1/2} = \det(Z)^{1/2}$$

s' appelle le module de $Z$ et on a donc la formule

$$Z.\overline{Z} = |Z|^2\mathrm{Id}.$$

1.0.4. *Structure de corps.* Un complexe $Z$ est non-nul ssi $x^2+y^2 \neq 0$ et dans ce cas l'identite (1.2) montrer que $Z$ est inversible et que son inverse est

$$Z^{-1} = (x^2+y^2)^{-1}\overline{Z} \in \mathbb{C}. \tag{1.3}$$

Comme toute matrice $Z \in \mathbb{C}$ non-nulle est inversible, $\mathbb{C}$ est un corps(commutatif).

1.0.5. *Structure euclidienne.* L'ensemble des nombres complexes est muni d'un produit scalaire (bilineaire, symetrique, defini positif) donne par

$$\langle Z, Z'\rangle_{\mathbb{C}} := \mathrm{Re}(Z\overline{Z'}) = xx' + yy'$$

et on a

$$\|Z\|^2_{\mathbb{C}} = \langle Z, Z\rangle_{\mathbb{C}} = |Z|^2 = x^2+y^2.$$

Ainsi l'isomorphisme (1.1) interchange les produits scalaires $\langle .,.\rangle_{\mathbb{C}}$ et le produit scalaire usuel $\langle .,.\rangle_{\mathbb{R}^2}$: pour $Z, Z' \in \mathbb{C}$, si on note $x, x'$ leurs parties reelles et $y, y'$ leurs parties imaginaires, on a

$$\langle Z, Z'\rangle_{\mathbb{C}} = xx' + yy' = \langle (x,y),(x',y')\rangle_{\mathbb{R}^2}.$$

On dit que (1.1) est une isometrie entre $(\mathbb{C}, \langle .,.\rangle_{\mathbb{C}})$ et $(\mathbb{R}^2, \langle .,.\rangle_{\mathbb{R}^2})$.

**1.1. Notation simplificatrice.** L'application

$$x \in \mathbb{R} \hookrightarrow x\mathrm{Id} \in \mathbb{C}$$

est un morphisme d'anneau

$$(x+x')\mathrm{Id} = x.\mathrm{Id} + x'.\mathrm{Id},\ (x.x')\mathrm{Id} = x\mathrm{Id}x'\mathrm{Id}$$

qui est injectif ($x\mathrm{Id} = \mathbf{0} \Longleftrightarrow x = 0$) qui donc envoie l'element neutre 1 sur la matrice identite Id: le corps des nombres reels $\mathbb{R}$ s'identifie donc a un sous-corps du corps des nombres complexes.

On simplifiera les notations en notant 1 a la place de l'identité et $i$ a la place de la matrice $I$: ainsi un nombre complexe s'ecrira sous la forme

$$z = x + iy.$$

Avec ces notations on a donc

$$z+z'=(x+x')+i(y+y'),\ z.\overline{z}=x^2+y^2=|z|^2,\ z^{-1}=\overline{z}/|z|^2$$

## 2. Interpretation des isometries en termes de nombres complexes

L'isomorphisme (1.1) identifie le corps des complexes $\mathbb{C}$ avec le plan reel $\mathbb{R}^2$. On va voir que plusieurs transformations du plan (notamment les isometries) admettent une interpretation simple en terme de nombres complexes.

–*Translations.* Soit $\vec{u}=(u,v)\in\mathbb{R}^2$, la translation $t_{\vec{u}}$ est la transformation

$$t_{\vec{u}}:\vec{x}=(x,y)\in\mathbb{R}^2\mapsto\vec{u}+\vec{x}=(u,v)+(x,y)=(x+u,y+v).$$

Il lui correspond la translation dans le corps des complexes: pour $\nu=u+iv\in\mathbb{C}$

$$t_\nu:z\in\mathbb{C}\mapsto z+\nu\in\mathbb{C}.$$

–*Rotations lineaires.* Soit $\rho=\mathrm{c}+i\mathrm{s}\in\mathbb{C}$, considerons l'application

$$[\times\rho]:\begin{array}{ccc}\mathbb{C}&\mapsto&\mathbb{C}\\ z&\mapsto&\rho z\end{array}.$$

Cette application est lineaire:

$$\forall z,z'\in\mathbb{C},\ \lambda\in\mathbb{R},\ [\times\rho](\lambda z+z')=\lambda\rho z+\rho z'=\lambda[\times\rho]z+[\times\rho]z'$$

et on a

$$[\times\rho]1_{\mathbb{C}}=\mathrm{c}+i\mathrm{s},\ [\times\rho]i=(\mathrm{c}+i\mathrm{s})i=-\mathrm{s}+i\mathrm{c}$$

et la matrice de cette application dans la base $\{1,i\}$ s'ecrit

$$M_{[\times\rho]}=\begin{pmatrix}\mathrm{c}&-\mathrm{s}\\ \mathrm{s}&\mathrm{c}\end{pmatrix}=\mathrm{c}.\mathrm{Id}+\mathrm{s}.I$$

(c'est a dire le nombre complexe $\rho$ dans la notation non-simplifiee). En effet

$$\rho.1=\rho=\mathrm{c}+i\mathrm{s},\ \rho.i=-\mathrm{s}+\mathrm{c}.i$$

En particulier si

$$|\rho|^2=\mathrm{c}^2+\mathrm{s}^2=1$$

et $M_\rho$ est la matrice d'une isometrie de $\mathrm{SO}_2(\mathbb{R})$ qu'on appelera rotation de parametre complexe $\rho$ et qu'on notera $r_\rho$. On peut voir ceci directement:

$$\langle\rho.w,\rho.w'\rangle_{\mathbb{C}}=\mathrm{Re}(\rho.w\overline{\rho}.w')=\mathrm{Re}(\rho.\overline{\rho}w.w')=|\rho|^2\mathrm{Re}(w.w')=|\rho|^2\langle\rho.w,\rho.w'\rangle_{\mathbb{C}}.$$

On botient donc une isometrie lineaire pour $(\mathbb{C},\langle\cdot,\cdot\rangle_{\mathbb{C}})$ si et seuelemt si $\rho\in\mathbb{C}^1$.

On note

$$\mathbb{C}^1=\{\rho=\mathrm{c}+i\mathrm{s},\ \mathrm{c},\mathrm{s}\in\mathbb{R},\ |\rho|^2=\mathrm{c}^2+\mathrm{s}^2=1\}$$

l'ensemble des nombres complexes de module 1. L'ensemble $(\mathbb{C}^1,\times)$ est un groupe pour la multiplication et $\mathbb{C}^1$ s'identifie au cercle de rayon 1. On a

PROPOSITION 4.1. *L'application*

$$\begin{array}{ccc}(\mathbb{C}^1,\times)&\mapsto&(\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}},\circ)\\ \rho&\mapsto&r_\rho\end{array}$$

*est un isomorphisme de groupes. En particulier (car $\rho^{-1}=\overline{\rho}$ pour $\rho\in\mathbb{C}^1$)*

$$r_\rho^{-1}=r_{\rho^{-1}}=r_{\overline{\rho}}.$$

–*Symetries lineaires.* La conjugaison complexe est definie (en notation simplifiee) est definie par

$$z = x + iy \mapsto \overline{z} = x - iy.$$

Elle verifie

- Linearite:
$$\forall z, z' \in \mathbb{C},\ \lambda \in \mathbb{R},\ \overline{\lambda z + z'} = \lambda \overline{z} + \overline{z}'.$$
- Involutivité: $\overline{\overline{z}} = z$.
- Multiplicativite:
$$\overline{zz'} = \overline{z'z} = \overline{z}.\overline{z}'.$$
- Norme:
$$z\overline{z} = x^2 + y^2 = \|(x, y)\|^2.$$
Le nombre $(z\overline{z})^{1/2} = (x^2 + y^2)^{1/2}$ s'appelle le module de $z$ et est note $|z|$. I verifie
$$|z.z'| = |z||z'|.$$
- Calcul de l'inverse: si $z \neq 0$, on a
$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$
En particulier si $|z| = 1$,
$$z^{-1} = \overline{z}.$$
- Produit scalaire
$$\mathrm{Re}(z.\overline{z}') = xx' + yy' = \langle (x, y), (x', y') \rangle$$
- Caracterisation des nombres reels et nombres imaginaires:
$$\overline{z} = z \Leftrightarrow z = x,\ x \in \mathbb{R},\ \overline{z} = -z \Leftrightarrow z = iy,\ y \in \mathbb{R}.$$

On a

$$\overline{1} = 1,\ \overline{i} = -i$$

et donc la matrice de cette application lineaire dans la base $(1, i)$ est

$$M_{\overline{\cdot}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Cette application $z \mapsto \overline{z}$ correspond donc a la symetrie orthogonale $s_{\mathbf{e}_1}$ d'axe $\mathbb{R}\mathbf{e}_1$ (et de droite orthogonale $\mathbb{R}\mathbf{e}_2$): elle envoie le point $(x, y)$ sur le point $(x, -y)$ qui est le symetrique de $(x, y)$ par rapport a l'axe des $x$.

Plus generalement, on a vu que toute symetrie lineaire $s$ se decompose en la composee d'une rotation et d'une symetrie fixee (ou de maniere equivalente la matrice associee se decompose en produit d'une matrice de rotation et d'une matrice de symetrie). Prenant comme symetrie la symetrie $s_{\mathbf{e}_1}$ d'axe $\mathbb{R}\mathbf{e}_1$, on a

$$s = s_{\mathbf{e}_1} \circ r \text{ ( et } M_s = M_{s_{\mathbf{e}_1}} \times M_r).$$

On obtient ainsi que toute symetrie lineaire correspond a une unique transformation du corps des complexes de la forme

$$s_\rho : z \mapsto \overline{\rho z},\ \rho \in \mathbb{C}^1.$$

et si $\rho = \mathrm{c} + i\mathrm{s}$, la matrice de cette transformation dans la base $(1, i)$ est

$$\begin{pmatrix} \mathrm{c} & -\mathrm{s} \\ -\mathrm{s} & -\mathrm{c} \end{pmatrix}$$

en effet

$$s_\rho(1) = \overline{\rho} = \mathrm{c} - i\mathrm{s},\ s_\rho(i) = \overline{-\mathrm{s} + i\mathrm{c}} = --\mathrm{s} - i\mathrm{c}.$$

REMARQUE 2.1. Notons egalement que

$$\overline{\rho.z} = \overline{\rho}.\overline{z}$$

ainsi la symetrie

$$s_\rho = s_{\mathbf{e}_1} \circ r_\rho$$

s'ecrit egalement comme la composee

$$s_\rho = r_{\overline{\rho}} \circ s_{\mathbf{e}_1} = r_\rho^{-1} \circ s_{\mathbf{e}_1}.$$

On retrouve ainsi un cas particulier du fait que si $r$ est une rotation lineaire et $s$ une symetrie lineaire

$$r \circ s = s \circ r^{-1}.$$

*Homotheties.* Soit $\lambda \in \mathbb{R}^\times$, la multiplication

$$[\times\lambda] : \begin{array}{ccc} \mathbb{C} & \mapsto & \mathbb{C} \\ z & \mapsto & \lambda z \end{array}$$

correspond a l'application lineaire

$$h_{\lambda,0} : \mathbb{R}^2 \mapsto \mathbb{R}^2$$

qui consiste a multiplier par le facteur $\lambda$ les coordonnees d'un point $P$

$$h_{\lambda,0} : P = (x, y) \mapsto \lambda.P = (\lambda x, \lambda y).$$

DÉFINITION 4.3. *L'application $h_{\lambda,0}$ est appelee homothetie lineaire de rapport $\lambda$ et de centre $\mathbf{0}$.*

La matrice de cette application lineaire est la matrice scalaire

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda.\mathrm{Id}.$$

Soit $\gamma \in \mathbb{C}^\times$ un nombre complexe non-nul general; $\gamma$ peut s'ecrire

$$\gamma = \lambda.\rho \text{ avec } \lambda = |\gamma| \text{ le module et } \rho = \tfrac{\gamma}{|\gamma|}. \text{ la partie de module 1.}$$

Ainsi la multiplication par $\gamma$

$$[\times\gamma] : \begin{array}{ccc} \mathbb{C} & \mapsto & \mathbb{C} \\ z & \mapsto & \gamma.z \end{array}$$

est la composee

$$[\times\gamma] = [\times\lambda] \circ [\times\rho]$$

et correspond a la composee $h_{\lambda,\mathbf{0}} \circ r_\rho$ de la rotation lineaire $r_\rho$ et de l'homothetie $h_{\lambda,\mathbf{0}}$ de rapport $\lambda$ et de centre $\mathbf{0}$.

*Homotheties affines.*

DÉFINITION 4.4. *Etant donne $\vec{u} \in \mathbb{R}^2$, une application de la forme*

$$h_{\lambda,\vec{u}} := t_{\vec{u}} \circ h_{\lambda,0}$$

*est appelee homothetie affine de rapport $\lambda \in \mathbb{R}^\times$.*

REMARQUE 2.2. C'est une application affine, bijective et telle que $\mathrm{Fix}(h_{\lambda,\vec{u}})$ est reduit a un point sauf si $\lambda = 1$; dans ce dernier car $\mathrm{Fix}(h_{1,\vec{u}}) = \mathbb{R}^2$ ou $\emptyset$ suivant que $\vec{u} = \mathbf{0}$ ou non. Dans le premier cas, l'unique point fixe est appele le centre de l'homothetie $h_{\lambda,\vec{u}}$.

Une homothetie affine correspond a la transformation de $\mathbb{C}$ donnee par

$$z \mapsto \lambda z + \nu,\ \lambda \in \mathbb{R}^\times,\ \nu \in \mathbb{C}.$$

**Isometries generales.**

THÉORÈME 4.1. *Toute isometrie $\varphi$ de $\mathbb{R}^2$ s'identifie a une transformation complexe de la forme*

$$r_{\rho,\nu} :\ z \mapsto \nu + \rho.z,\ s_{\rho,\nu} :\ z \mapsto \nu + \overline{\rho.z}$$

*avec*

$$\nu \in \mathbb{C},\ \rho = \mathrm{c} + i\mathrm{s} \in \mathbb{C}^1\ (ie.\ \mathrm{c}^2 + \mathrm{s}^2 = 1)$$

*La partie lineaire $\varphi_0$ est donnee par*

$$r_\rho = r_{\rho,0} : z \mapsto \rho,\ s_\rho = s_{\rho,0} : z \mapsto \overline{\rho}$$

*et leur matrices sont donnees par*

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} c & -s \\ s & c \end{pmatrix} = \begin{pmatrix} c & -s \\ -s & -c \end{pmatrix}.$$

*Dans le premier cas $\varphi \in \mathrm{Isom}(\mathbb{R}^2)^+$ et dans le second $\varphi \in \mathrm{Isom}(\mathbb{R}^2)^-$. Les nombres complexes $(\rho, \nu)$ associes a $r_{\rho,\nu}$ et $s_{\rho,\nu}$ (ou bien seulement $\rho$ si on considere les isometries lineaires $r_\rho$ et $s_\rho$) sont appeles parametres complexes des ces isometries.*

## 2.1. Angle et nombre complexes.

**2.2. Mesure d'un angle.** Un angle correspond donc a une rotation et donc a un nombre complex de module 1, $\alpha$, ou encore un point sur le cercle unité. Pour des raisons pratiques, on preferera souvent representer un angle par un nombre reel: pour cela on mesure la *longueur* de l'arc du cercle unite $\mathbb{C}^1$ compris entre 1 et $\alpha$ (ou encore la longueur de l'arc de cercle unite determine par les deux vecteurs $\vec{u}, \vec{v}$: cela necessite de definir rigouresement ce qu'est la longueur d'un arc de cercle ce qui implique la notion d' integrale le long de courbe; cela sera defini rigoureusement au semestre de printemps.

Au lieu de cela, on admettra le resultat suivant de nature algebrique/analytique

THÉORÈME 4.2. *Il existe un morphisme de groupe non-trivial*

$$\phi_1 : (\mathbb{R}, +) \mapsto (\mathbb{C}^1, \times)$$

*qui est derivable (la fonction $t \mapsto \phi_1(t) = x_1(t) + iy_1(t)$ est derivable) et tel que $\phi_1'(0) = i$. Ce morphisme est surjectif et on a*

$$\ker \phi_1 = 2\pi\mathbb{Z} \subset \mathbb{R}$$

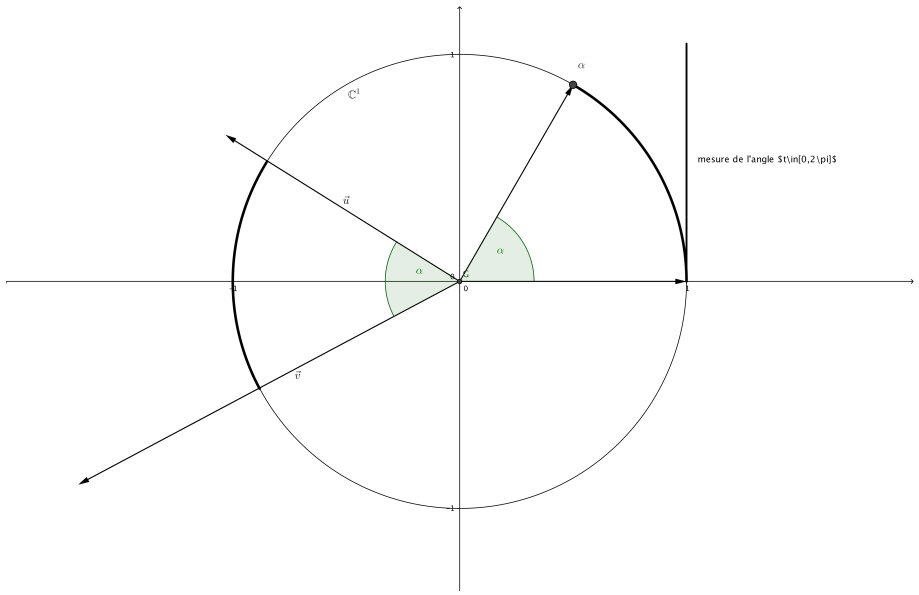


FIGURE 1. Deux paires de vecteurs representant le meme angle

*ou* $\pi = 3.14159\cdots$ *est une constante absolue. On a pour tout* $t$

$$|\phi_1'(t)| = 1.$$

*Tout autre morphisme de groupe derivable* $\phi : (\mathbb{R}, +) \mapsto \mathbb{C}^1$ *est de la forme*

$$\phi(t) = \phi_1(\lambda t)$$

*avec* $\lambda \in \mathbb{R}$. *On a* $\phi'(0) = \lambda i$, $|\phi'(t)| = |\lambda|$ *et*

$$\ker \phi = \frac{2\pi}{\lambda}\mathbb{Z}.$$

PREUVE. Admettons l'existence d'un morphisme de groupe non-constant $\phi$ qui soit derivable. On a $\phi(0) = 1$ et pour tout $s, t \in \mathbb{R}$

$$\phi(s)\phi(t) = \phi(s + t)$$

et en particulier

$$\phi(-s) = \phi(s)^{-1} = \overline{\phi(s)}.$$

Fixons $t \in \mathbb{R}$, la relation precedente est l'egalite de deux fonctions de la variable $s$:

$$s \mapsto \phi(s + t),\ s \mapsto \phi(s)\phi(t).$$

Les derivee en$s$ sont donc egales: on obtient alors $\forall s, t \in \mathbb{R}$

$$\phi'(s + t) = \phi'(s)\phi(t)$$

et

$$-\phi'(-s) = \overline{\phi'(s)}.$$

En $s = 0$ on obtient que

$$\phi'(t) = \phi'(0)\phi(t)$$

et

$$-\phi'(0) = \overline{\phi'(0)} \Rightarrow \phi'(0) = \lambda i \in i\mathbb{R}.$$

Notons que $\lambda \neq 0$ car sinon

$$\forall t,\ \phi'(t) = 0$$

et $\phi$ serait constant. On a

$$\phi'(t) = \phi'(0)\phi(t)$$

de sorte que

$$\forall t,\ |\phi'(t)| = |\lambda|.$$

Ce qui s'interprete en disant que $\phi(t)$ parcours le cercle $\mathbb{C}^1$ a vitesse constante.

Notons $\phi_1(t) := \phi(t/\lambda)$; c'est un morphisme de groupe non-constant qui verifie $\phi'(0) = i$.

Soit $\psi : (\mathbb{R}, +) \mapsto \mathbb{C}^1$ un autre morphisme derivable $\psi'(0) = i\mu$ alors

$$\varphi : t \mapsto \psi(t/\mu)\phi_1(t)^{-1} = \psi(t/\mu)\phi_1(-t)$$

est un morphisme de groupe derivable tel que

$$\varphi'(0) = \mu^{-1}\mu - 1 = 0.$$

Ce morphisme est donc constant egal a 1.

□

Ainsi tout nombre complexe de module 1, $z = x + iy$ tel que $x^2 + y^2 = 1$, est represente de maniere unique par un nombre reel $t \in [0, 2\pi[$: l'unique element $t$ dans cet intervalle tel que

$$z = e^{it} = \cos(t) + i\sin(t);$$

alternativement $z$ est represente de maniere unique par le sous-ensemble de $\mathbb{R}$ (l'ensemble des translates de $t$ par les elements du sous-groupe $(2\pi\mathbb{Z}, +)$)

$$t \,(\mathrm{mod}\, 2\pi) = t + 2\pi\mathbb{Z} \subset \mathbb{R}.$$

( si si $t' \in t \,(\mathrm{mod}\, 2\pi)$, $t' \,(\mathrm{mod}\, 2\pi) = t \,(\mathrm{mod}\, 2\pi)$. ) Ce nombre $t$ (ou cette classe de nombres) est appelle l'argument de $z$ et est note $\arg(z)$.

Si on considere l'angle forme par les deux vecteurs $(1, 0)$ sur $(x, y)$; le parametre complexe qui envoie le premier vecteur sur le second est precisement $z$ qu'on identifie avec $t$. On parlera "d'angle de mesure $t$" ou par abus de language "d'angle $t$".

Ainsi dans ce language on a le resultat tautologique suivant:

THÉORÈME 4.3. *Les isometries preservent les angles au sens suivant: soit $O, A, B$ trois points avec $A, B \neq O$ et $t \,(\mathrm{mod}\, 2\pi)$ la mesure de l'angle $\widehat{AOB}$; soit $\varphi \in \mathrm{Isom}(\mathbb{R}^2)$ et*

$$A' = \varphi(A),\ B' = \varphi(B),\ O' = \varphi(O);$$

- *si $\varphi \in \mathrm{Isom}(\mathbb{R}^2)^+$ alors la mesure de l'angle $\widehat{A'O'B'}$ vaut $t$;*
- *si $\varphi \in \mathrm{Isom}(\mathbb{R}^2)^-$ alors la mesure de l'angle $\widehat{A'O'B'}$ vaut $2\pi - t = -t \,(\mathrm{mod}\, 2\pi)$.*

Cette parametrisation est importante car elle permet d'ordonner les angles par l'ordre naturel de l'intervalle $[0, 2\pi[$: on dira qu'un angle est plus petit qu'un autre si son parametre reel dans $[0, 2\pi[$ est plus petit que celui de l'autre angle; on peut egalement parler de secteur angulaire par rapport a un segment oriente $[P, Q]$ associe a un intervalle $I \subset [0, 2\pi[$ comme etant l'ensemble des points $R$ du plan tel que le parametre reel associe a l'angle $\widehat{QPR}$ appartienne a l'intervalle I.

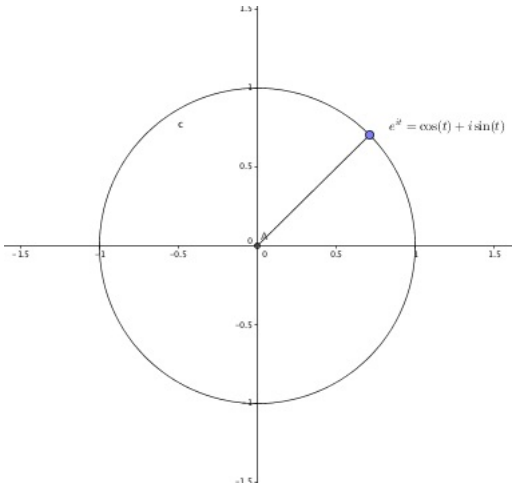


FIGURE 2. Le cercle trigonometrique

2.2.1. *Trigonometrie.* En peut egalement en deduire les proprietes bien connues mais admises des fonctions cosinus et sinus:

THÉORÈME 4.4. *Les fonctions* $t \mapsto \cos(t)$ *et* $t \mapsto \sin(t)$ *ont les proprietes suivantes*

(1) *Elles ont les expressions suivantes*

$$\cos(t) = \mathrm{Re}(e^{it}) = \frac{e^{it} + e^{-it}}{2},\ \sin(t) = \mathrm{Im}(e^{it}) = \frac{e^{it} - e^{-it}}{2};$$

(2) *elles sont periodiques de periode* $2\pi$*:*

$$\cos(t + 2\pi k) = \cos(t),\ \sin(t + 2\pi k) = \sin(t);$$

(3) $\cos(t)$ *est paire et* $\sin(t)$ *est impaire.*

(4) *elles sont derivables et verifient*

$$\cos'(t) = -\sin(t),\ \sin'(t) = \cos(t);$$

(5) *pour tout* $t, t' \in \mathbb{R}$

$$\cos(t + t') = \cos(t)\cos(t') - \sin(t)\sin(t');$$
$$\sin(t + t') = \sin(t)\cos(t') + \cos(t)\sin(t');$$

(6) *pour tout* $t$*,*

$$\cos(\pi - t) = -\cos(t),\ \sin(\pi - t) = \sin(t)$$

*de sorte que* $\cos(t)$ *et* $\sin(t)$ *sont determinees par leur restriction a l'intervalle* $[0, \pi/2]$*;*

(7) *on a la table de valeurs suivantes*

| $t =$ | $0$ | $\pi/6$ | $\pi/5$ | $\pi/4$ | $\pi/3$ | $\pi/2$ |
|---|---|---|---|---|---|---|
| $\cos(t) =$ | $1$ | $\frac{\sqrt{3}}{2}$ | $\frac{\sqrt{5}-1}{4}$ | $\frac{\sqrt{2}}{2}$ | $\frac{1}{2}$ | $0$ |
| $\sin(t) =$ | $0$ | $\frac{1}{2}$ | $\frac{\sqrt{10+2\sqrt{5}}}{4}$ | $\frac{\sqrt{2}}{2}$ | $\frac{\sqrt{3}}{2}$ | $1$ |

(8) *les fonctions* cos *et* sin *sont strictement positives sur l'intervalle* $]0, \pi/2[$*; la premiere est strictement decroissante et la seconde strictement croissante.*

CHAPITRE 5

# Groupes finis d'isometries

Dans ce chapitre, on va classifier tous les sous-groupes finis d'isometries du plan. On va voir qu'il sont de deux type: les groupes cycliques et les groupe dihedraux que l'on va discuter d'un point de vue abstrait.

On va commencer par montrer qu'il est facile de construire des groupes finis d'isometries.

## 1. Existence de groupes finis d'isometries

Soit $\mathcal{S} = \{P_1, \cdots, P_n\} \subset \mathbb{R}^2,\ n \geqslant 1$ un ensemble fini non-vide de points du plan.

THÉORÈME 5.1. *Si $\mathcal{S}$ possede au moins trois points non-alignes alors le groupe des isometries qui preservent l'ensemble $\mathcal{S}$*

$$\mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}} = \{\varphi \in \mathrm{Isom}(\mathbb{R}^2),\ \varphi(\mathcal{S}) = \mathcal{S}\}$$

*est un groupe fini.*

**Preuve**: Notons que si Le fait que $\mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}}$ soit un groupe provient du fait que la propriete de preserver un ensemble (globalement) est stable par composition et par inverse. On laisse au lecteur le soit de rediger cela.

Comme $\varphi$ est bijective sur $\mathbb{R}^2$ et qu'elle envoie $\mathcal{S}$ sur $\mathcal{S}$ elle induit une bijection sur cet ensemble, et donc un element $\sigma_\varphi$ du groupe des permutations de $\mathcal{S}$, $Bij(\mathcal{S})$ qui est fini de cardinal $n!$. Montrons que l'application

$$\varphi \mapsto \sigma_\varphi$$

est injective ce qui montrera que $\mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}}$ est fini de cardinal $\leqslant n!$. Supposons que pour $\varphi, \psi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}}$ on ait

$$\sigma_\varphi = \sigma_\psi$$

c'est a dire que pour tout $P \in \mathcal{S}$ on a

$$\varphi(P) = \psi(P)$$

alors l'isometrie composee $\phi := \psi^{-1} \circ \varphi$ laisse tout point de $\mathcal{S}$ fixe: pour tout $P \in \mathcal{S}$ on a

$$\phi(P) = \psi^{-1}(\varphi(P)) = \psi^{-1}(\psi(P)) = P$$

et $\phi$ est donc une isometrie dont l'ensemble des points fixes contient trois points non-aligne: la seule possibilite est que $\psi$ soit l'identite. □

REMARQUE 1.1. En fait on a que l'ordre de $\mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}}$ divise $n!$: l'application

$$\varphi \mapsto \sigma_\varphi$$

est un morphisme de groupe et donc realise $\mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}}$ comme un sous-groupe de $Bij(\mathcal{S})$ et on conclut par le theoreme de Lagrange.

REMARQUE 1.2. En fait le groupe $\mathrm{Isom}(\mathbb{R}^2)_{\mathcal{S}}$ est non-trivial seulement si l'ensemble $\mathcal{S}$ est d'une forme tres particuliere. On verra cette forme plus tard apres avoir classifier les groupes finis.

## 2. Groupes dihedraux

On rappelle qu'un groupe fini $G$ est cyclique si il est engendre par un element

$$G = \langle r \rangle = r^{\mathbb{Z}} = \{e_G, r, r^2, \cdots, r^{n-1}\}$$

ou

$$n = |G| = \mathrm{ord}(r) \geqslant 1$$

est l'ordre de $G$ (ou de son generateur $r$). On rappelle egalement que tous les groupes cyclique d'ordre $n$ sont tous isomorphes et isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. On designera par $\mathcal{C}_n$ un groupe cyclique d'ordre $n$ pris a isomorphisme pres.

DÉFINITION 5.1. *Un groupe $G$ fini est dit dihedral si il est engendre par deux elements $G = \langle r, s\rangle$ tel que $s$ est d'ordre 2, $s \notin \langle r\rangle$ ($s \neq e_G$, $s^2 = e_G$ et donc $s^{-1} = s$) et qui verifient la relation*

$$srs^{-1} = srs = r^{-1}.$$

*On notera*

$$G^+ = \langle r\rangle = r^{\mathbb{Z}}$$

*le sous-groupe (cyclique) engendre par $r$ et on pose $G^- = sG^+$.*

REMARQUE 2.1. Avec cette definition il y a un groupe qui est a la fois cyclique et dihedral: le groupe $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ (et tout groupe isomorphe): $\mathbb{Z}/2\mathbb{Z}$ est cyclique car engendre par 1 et dihedral en prenant $r = 0$ (l'element neutre) et $s = 1$. C'est le groupe possible.

THÉORÈME 5.2. *Soit $G$ un groupe dihedral, alors $G^+$ est un sous-groupe distingue et on a*

$$G = G^+ \sqcup G^- = r^{\mathbb{Z}} \sqcup sr^{\mathbb{Z}}.$$

*En particulier $|G| = |G^+| + |G^-| = 2|G^+|$.*

*Tout element $s'$ de $G^-$ est d'ordre 2 ($s' \neq e_G$, $s'^2 = e_G$) et on a pour tout $s' \in G^-$, et tout $r' \in G^+$*

$$s'r's'^{-1} = r'^{-1},\ G^- = s'G^+ = G^+.s',\ G^+ = s'G^- = G^-s'.$$

*Deux groupes dihedraux de meme ordre sont isomorphes.*

On designera par $\mathcal{D}_{2n}$ un groupe dihedral d'ordre $2n$ pris a isomorphisme pres.

PREUVE. On notera

$$\mathrm{Ad}(g) : \begin{array}{ccc} G & \mapsto & G \\ h & \mapsto & \mathrm{Ad}(g)(h) = g.h.g^{-1} \end{array}$$

l'application de conjugaison par $g$. Rappelons que

(1) Pour tout $g \in G$, $\mathrm{Ad}(g) : G \mapsto G$ est un isomorphisme de groupes,
(2) L'application

$$g \in G \mapsto \mathrm{Ad}(g) \in Bij(G)$$

est un morphisme de groupes de $G$ vers le groupe des bijections de $G$.

Soit

$$N(G^+) = \{g \in G,\ \mathrm{Ad}(g)(G^+) = G^+\} \subset G.$$

Nous allons montrer que $N(G^+) = G$ ce qui est equivalent a dire que $G^+$ est distingue. Pour cela nous notons que $N(G^+)$ est un sous-groupe de $G$ (appelle le *normalisateur* de $G^+$: en effet soit $g, g' \in N(G^+)$, on a

$$\mathrm{Ad}(g.g')(G^+) = \mathrm{Ad}(g)(\mathrm{Ad}(g')(G^+)) = \mathrm{Ad}(g)(G^+) = G^+.$$

Par ailleurs comme $g \mapsto \mathrm{Ad}(g)$ est un morphisme de groupes, l'application reciproque de $\mathrm{Ad}(g)$ est $\mathrm{Ad}(g)^{-1} = \mathrm{Ad}(g^{-1})$ et donc comme $\mathrm{Ad}(g)(G^+) = G^+$, on a

$$G^+ = \mathrm{Ad}(g)^{-1}(\mathrm{Ad}(g)(G^+)) = \mathrm{Ad}(g)^{-1}(G^+) = \mathrm{Ad}(g^{-1})(G^+)$$

donc $g^{-1} \in N(G^+)$.

On a pour tout $l \in \mathbb{Z}$, que

$$\mathrm{Ad}(r)(r^l) = r^l,\ \mathrm{Ad}(s)(r^l) = (r^{-1})^l = r^{-l}$$

donc $r, s \in N(G^+)$ et comme $r, s$ engendrent $G$ on a

$$G = \langle r, s\rangle \subset N(G^+).$$

Notons egalement que

$$G^- = s.G^+ = s.G^+.s^{-1}.s = G^+.s.$$

Montrons que $G^- = G - G^+$: comme $s \notin G^+$ pour tout $r' \in G^+$ on a $s.r' \notin G^+$ (sinon on aurait $s \in G^+ r'^{-1} = G^+$) donc $G^- \in G - G^+$. Reciproquement, considerons $g \in G$, on a

$$g = s^{k_1}.r^{l_1}.\cdots.s^{k_t}.r^{l_t},\ k_1, \cdots, l_t \in \mathbb{Z}.$$

Notons que comme $s^2 = e_G$ on peut oter toutes les puissances paires de $s$ dans cette ecriture et supposer que $k_1 \in \{0, 1\}$ et que $k_{t'} = 1$ pour $t' > 1$ (si un tel $t'$ existe):

$$g = s^{k_1}.r^{l_1}.s.r^{l_2}.s\cdots.s.r^{l_t},\ k_1, \cdots, l_t \in \mathbb{Z}.$$

Notons egalement que comme

$$s.r^l.s = s.r^l.s^{-1} = r^{-l},$$

on peut dans le mot representant $g$, remplacer les suites de la forme $s.r^{l'}.s$ par $r^{-l'}$ et donc ecrire $g$ sous la forme

$$g = s^{k_1} r^{l'} \text{ avec } k_1 \in \{0, 1\},\ l' \in \mathbb{Z}.$$

On a alors que

$$g \in G - G^+ \Longleftrightarrow k_1 = 1 \Longleftrightarrow g = s.r^{l'} \Longleftrightarrow g \in s.G^+ = G^-.$$

Soit $g \in G$, on a alors

$$\mathrm{Ad}(g)(r) = g.r.g^{-1} = s^{k_1}.r^{l'}.r.r^{-l'}s^{-k_1} = s^{k_1}.r.s^{-k_1} = \mathrm{Ad}(s^{k_1})(r) = \begin{cases} r & \text{si } k_1 = 0 \text{ cad } g \in G^+ \\ r^{-1} & \text{si } k_1 = 1 \text{ cad } g \in G^- \end{cases}.$$

On a donc

$$\mathrm{Ad}(g)(r) = r^{\varepsilon(g)} \text{ avec } \varepsilon(g) = \pm 1 \text{ si } g \in G^{\pm}$$

et plus generalement pour tout $r' = r^l \in G^+$, on a

$$\mathrm{Ad}(g)(r') = r'^{\varepsilon(g)} \text{ avec } \varepsilon(g) = \pm 1 \text{ si } g \in G^{\pm}.$$

En particulier pour $s' \in G^-$, on a

$$s'.r'.s'^{-1} = r'^{-1}.$$

De plus comme $s^2 = e_G$, on a

$$s'^2 = s.r^l.s.r^l = s.r^l.s^{-1}.r^l r^{-l}.r^l = e_G$$

donc $s'$ est d'ordre 2.

Soient $G = \langle r, s\rangle$ et $G' = \langle r', s'\rangle$ de groupes dihedraux de meme ordre ($|G| = |G'|$) alors $|G| = |G'| = 2|G^+| = 2|G'^+|$ donc $r$ et $r'$ sont de meme ordre, disons $n$. Tout element $g \in G$ s'ecrit de maniere unique sous la forme

$$g = s^k r^l,\ k \in \{0, 1\},\ 0 \leqslant l \leqslant n-1.$$

Posons

$$\phi : \begin{array}{ccc} G & \mapsto & G' \\ s^k r^l & \mapsto & s'^k r'^l \end{array}$$

alors $\phi$ est une bijection et on verifie que c'est un morphisme de groupes: il est clair que $\phi$ restreint a $G^+$ est un isomorphisme de groupes de $G^+$ vers $G'^+$, pour le reste on a que

$$\phi(sr^l) = \phi(s)\phi(r)^l$$

$$\phi(sr^l.sr^{l'}) = \phi(r^{-l}r^{l'}) = \phi(r^{-l+l'}) = \phi(r)^{-l+l'} = \phi(sr^l)\phi(sr^{l'})$$

$$\phi(r^{l'}sr^l) = \phi(ssr^{l'}sr^l) = \phi(sr^{l-l'}) = s'(r')^{l-l'} = \phi(r^{l'})\phi(sr^l).$$

□

Remarque 2.2. On defini l'application

$$\varepsilon : \begin{array}{ccc} G & \mapsto & \{\pm 1\} \\ g & \mapsto & \varepsilon(g) \end{array}$$

ou $\varepsilon(g) = \pm 1$ suivant que $g \in G^{\pm}$. Alors $\varepsilon$ est un morphisme de groupes dont le noyau est $G^+$.

## 3. Classification des sous-groupes finis d'isometries

Dans cette section, on classifie les sous-groupes finis d'isometries du plan. On va montrer qu'un groupe fini d'isometries est soit un groupe cyclique, soit un groupe dihedral.

Théorème 5.3. *Soit $G \subset \mathrm{Isom}(\mathbb{R}^2)$ un sous-groupe fini d'isometries. Alors*

- *$G$ est soit cyclique soit dihedral.*
- *Si on note $G^+ = G \cap \mathrm{Isom}(\mathbb{R}^2)^+$ (le sous-groupe des rotations de $G$) alors $G^+$ est cyclique et distingue dans $G$. $G$ est cyclique si et seulement si $G = G^+$.*
- *$G$ (resp. $G^+$) est conjugue a un sous groupe fini du groupe des isometries lineaires $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ (resp. $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$).*

On commence par montrer la

Proposition 5.1. *Soit $G \subset \mathrm{Isom}(\mathbb{R}^2)$ un sous-groupe fini alors il existe un point $P = P_G \in \mathbb{R}^2$ qui est fixe pour tous les elements de $G$:*

$$\forall \psi \in G,\ \psi(P) = P$$

PREUVE. Soit $Q \in \mathbb{R}^2$ un point quelconque et

$$P = P_{G,Q} = \frac{1}{|G|} \sum_{\varphi \in G} \varphi(Q)$$

le barycentre des differentes images de $Q$ par les elements de $G$ pour les poids uniformes $|G|^{-1}$. Soit $\psi \in G$ alors $\psi$ est affine et donc preserve le barycentre: $\psi(P)$ est le barycentre des points $\{\psi(\varphi(Q)),\ \varphi \in G\}$:

$$\psi(P) = \frac{1}{|G|} \sum_{\varphi \in G} \psi(\varphi(Q)).$$

Rapelons la preuve de ce fait decomposons $\psi$ en translation et prtie lineaire, $\psi = t_{\psi(\mathbf{0})} \circ \psi_0$, alors comme $\psi_0$ est lineaire

$$\psi(P) = \psi(\mathbf{0}) + \psi_0(\frac{1}{|G|} \sum_{\varphi \in G} \varphi(Q)) = \psi(\mathbf{0}) + \frac{1}{|G|} \sum_{\varphi \in G} \psi_0(\varphi(Q))$$

$$\frac{1}{|G|} \sum_{\varphi \in G} (\psi(\mathbf{0}) + \psi_0(\varphi(Q)) == \frac{1}{|G|} \sum_{\varphi \in G} \psi(\varphi(Q))$$

car

$$\psi(\mathbf{0}) = \frac{1}{|G|} \sum_{\varphi \in G} \psi_0(\mathbf{0}).$$

Comme $G$ est un groupe on a

$$\psi(P) = \frac{1}{|G|} \sum_{\varphi \in G} \psi(\varphi(Q)) = \frac{1}{|G|} \sum_{\varphi' \in G} \varphi'(Q) = P.$$

□

Soit

$$G_0 = \mathrm{Ad}(t_{-P})(G) = t_{-P} \circ G \circ t_P$$

le groupe conjugue de $G$ par la translation $t_P$; pour tout $\varphi_0 \in G_0$, il existe $\varphi \in G$ de la forme $t_{-P} \circ \varphi \circ t_P$ et on a

$$\varphi_0(\mathbf{0}) = t_{-P} \circ \varphi \circ t_P(\mathbf{0}) = t_{-P} \circ \varphi(P) = t_{-P}(P) = \mathbf{0}.$$

Donc $G_0 \subset \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$.

Quitte a remplacer $G$ par le groupe isomorphe $G_0$, on peut donc supposer que

$$G \subset \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}.$$

Soit

$$G^+ = G \cap \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}};$$

c'est de sous-groupe des rotations lineaires de $G$; soit $n$ son ordre. Interpretes en terme de nombres complexes, $G^+$ correspond a un sous-groupe fini du groupe $\mathbb{C}^1$ des nombres complexes de module 1

$$(\{\alpha_1, \cdots, \alpha_n\}, \times) \subset (\mathbb{C}^1, \times).$$

THÉORÈME 5.4. *Soit $G$ un sous-groupe fini de $(\mathbb{C}^\times, \times)$ et $n = |G|$ son ordre alors $G$ est cyclique, contenu dans $\mathbb{C}^1$ et egal a l'ensemble*

$$\mu_n = \{\alpha \in \mathbb{C},\ \alpha^n = 1\}$$

*des racines $n$-iemes de l'unite: les racines complexes du polynome $X^n - 1$. En particulier le groupe $\mu_n$ est l'unique sous-groupe de $\mathbb{C}^\times$ d'ordre $n$.*

Avant de montrer ce resultat, on rappelle le

THÉORÈME 5.5 (Theoreme de Lagrange). *Soit $(G,.)$ un groupe fini d'ordre $|G|$ alors pour tout sous-groupe $H \subset G$ l'ordre de $H$, $|H|$ divise l'ordre de $G$, $|G|$. En particulier, pour tout $g \in G$, l'ordre de $g$ divise l'ordre de $G$.*

On aura egalement besoin du lemme suivant

LEMME 5.1. *Soit $G$ un groupe commutatif et $g, h \in G$ des elements d'ordre $m$ et $n$, alors le sous-groupe $\langle g, h\rangle$ contient un element $k$ d'ordre exactement $[m, n]$.*

PREUVE. Supposons que $(m, n) = 1$ alors $[m, n] = mn$ et prenons $k = g.h$; on a

$$(g.h)^{mn} = (g^m)^n.(h^n)^m = e_G$$

donc $\mathrm{ord}(g.h)|mn$. Soit $d$ l'ordre de $g.h$, on a $(g.h)^d = e_G$ avec $d|mn$ et $d \neq mn$. On a

$$g^d = h^{-d}$$

et donc

$$g' = g^d = h^{-d} \in \langle g\rangle \cap \langle h\rangle.$$

Soit $e$ l'ordre de $g'$ alors $e|m = |\langle g\rangle|$ et $e|n = |\langle h\rangle|$ par le Theoreme de Lagrange, et donc $e|(m, n) = 1$. Ainsi

$$g^d = g' = e_G$$

donc $m|d$; de meme $n|d$ donc $mn|d$ car $(m, n) = 1$. Ainsi $mn|d$ et $gh$ est d'ordre $mn$.

En general, il existe $m'|m$ et $n'|n$ tel que $m'n' = [m, n]$ et $(m', n') = 1$. Rappelons que si on decompose $m$ et $n$ en produit de nombres premiers on a

$$m = \prod_p p^{\alpha_p},\ n = \prod_p p^{\beta_p},\ [m, n] = \prod_p p^{\max(\alpha_p,\beta_p)},\ (m, n) = \prod_p p^{\min(\alpha_p,\beta_p)}.$$

On defini alors

$$m' = \prod_{\substack{p\\ \alpha_p \geqslant \beta_p}} p^{\alpha_p},\ n' = \prod_{\substack{p\\ \beta_p > \alpha_p}} p^{\beta_p}.$$

Ces entiers sont premiers entre eux car les conditions $\alpha_p \geqslant \beta_p$ et $\alpha_p < \beta_p$ sont mutuellement exclusives. D'autre part on a $m'|m$ et $n'|n$ puisque les exposants pour tous les nombres premiers de ces decomposition sont inferieurs ou egaux a ceux des decompositions de $m$ et $n$ et enfin on a

$$[m, n] = \prod_p p^{\max(\alpha_p,\beta_p)} = \prod_{\substack{p\\ \alpha_p \geqslant \beta_p}} p^{\alpha_p} \prod_{\substack{p\\ \alpha_p < \beta_p}} p^{\beta_p} = m'n'.$$

Soient

$$g' = g^{m/m'} \text{ et } h' = h^{n/n'};$$

alors $g'$ et $h'$ sont d'ordre $m'$ et $n'$ respectivement: en effet on a

$$(g')^{m'} = g^{mm'/m'} = g^m = e_G$$

et si $0 < m'' < m'$ on a $(g')^{m''} = g^{mm''/m'} \neq e_G$ car $mm''/m' < m$ et $m$ est l'ordre de $g$.

Commme $(m', n') = 1$ le produit $g'.h'$ est d'ordre $m'n'$. □

3.0.1. *Preuve du Theoreme 5.6.* Soit $G \subset \mathbb{C}^\times$ un groupe fini d'ordre $n$. Par le theoreme de Lagrange pour tout $\alpha \in G$, on a $\alpha^n = 1$ et donc

$$|\alpha|^n = |\alpha^n| = 1 \Rightarrow |\alpha| = 1$$

et on a

$$G \subset \mu_n \subset \mathbb{C}^1$$

et donc $n \leqslant |\mu_n|$. Comme $|\mu_n| \leqslant n$ on a $n = |\mu_n|$ et

$$G = \mu_n.$$

Montrons que $G$ est cyclique: soit $\alpha \in G$ un element d'ordre maximal $n_\alpha$. Il suffit de montrer que $n_\alpha = n$ car alors on aura

$$\langle \alpha \rangle = \alpha^{\mathbb{Z}} = G$$

et $G$ sera cyclique de generateur $\alpha$.

Comme $n_\alpha \leqslant n$ (Lagrange) il suffit de montrer que $n_\alpha \geqslant n$. Soit $\beta$ un autre element de $G$ d'ordre $n_\beta$, alors, par le lemme 5.1, il existe dans $G$ un element $\gamma$ d'ordre $[n_\alpha, n_\beta]$; mais si $n_\beta \not| n_\alpha$, alors $[n_\alpha, n_\beta]$ est $> n_\alpha$ ce qui contredit par maximalite de $n_\alpha$, on en deduit que

$$\forall \beta \in G,\ n_\beta | n_\alpha.$$

Ainsi tout element de $G$ est d'ordre divisible par $n_\alpha$: en particulier

$$\forall \beta \in G \subset \mathbb{C}^\times,\ \beta^{n_\alpha} - 1 = 0.$$

Comme $\mathbb{C}$ est un corps, le nombre de racines distinctes du polynome $X^{n_\alpha} - 1$ est $\leqslant \deg(X^{n_\alpha} - 1) = n_\alpha$ donc $n = |G| \leqslant n_\alpha$ et donc

$$|G| = n = n_\alpha \text{ et } G = \alpha^{\mathbb{Z}} = \mu_n$$

est cyclique d'ordre $n$. □

Remarque 3.1. En fait la preuve precedente utilise seulement le fait que $\mathbb{C}$ est un corps et donc que si $P(X) \in \mathbb{C}[X]$ est un polynome de degre $n$ alors le nombre des racine de $P$ dans $K$ est $\leqslant n$. On a en fait le resultat plus general suivant:

Théorème 5.6. *Soit $(K, +, \times)$ un corps et $G$ un sous-groupe fini du groupe multiplicatif $(K^\times, \times)$ et $n = |G|$ son ordre alors $G$ est un groupe cyclique egal au groupe des racine $n$-iemes de l'unite contenue dans $K$*

$$\mu_n(K) = \{\alpha \in K^\times,\ \alpha^n = 1_k\}.$$

3.0.2. *Fin de la preuve du Theoreme 5.3.* Soit $G \subset \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ un groupe fini d'isometries lineaires et

$$G^+ = G \cap \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}},\ G^- = G \cap \mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}$$

et soit $n$ l'ordre de $G^+$; on vient de montrer que $G^+ = \langle r_\alpha \rangle$ est un groupe cyclique engendre par une rotation $r = r_\alpha$ de parametre complexe $\alpha$, un generateur de $\mu_n$. Ainsi si $G^+ = G$, $G$ est cyclique comme annonce.

Sinon, soit $s \in G^- = G \cap \mathrm{Isom}(\mathbb{R}^2)^-_{\mathbf{0}}$ alors $s$ est une symetrie lineaire et donc d'ordre 2; calculons $s \circ r_\alpha \circ s^{-1}$ a l'aide des complexes: en posant $s = s_\beta$, on trouve que

$$s_\beta \circ r_\alpha \circ s_\beta^{-1} = s_\beta \circ r_\alpha \circ s_\beta = r_{\overline{\beta}.\overline{\alpha}.\beta} = r_{\overline{\alpha}\overline{\beta}.\beta} = r_{\alpha^{-1}} = r^{-1}$$

car

$$\alpha^{-1} = \overline{\alpha} \text{ et } \beta^{-1} = \overline{\beta}.$$

Ainsi on obtient que $G$ est dihedral d'ordre $2n$. □

Notons que si $G$ est dihedral d' ordre $2n$, le groupe $G^+$ est uniquement defini (c'est le groupe de rotations de parametres contenus dans $\mu_n$); en revanche, le groupe total $G$, si il est dihedral n'est pas unique: on peut choisir la symetrie lineaire $s$ de maniere arbitraire et obtenir des groupes finis d'isometries isomorphes mais distincts. Notons cependant que pour $\alpha, \beta, \gamma \in \mathbb{C}^1$

$$r_\gamma \circ r_\alpha \circ r_\gamma^{-1} = r_\alpha,\ r_\gamma \circ s_\beta \circ r_\gamma^{-1} = s_{\overline{\gamma}^2\beta};$$

ainsi choisissant $\gamma \in \mathbb{C}^1$ tel que $\gamma^2 = \beta$ (on a vu qu'un tel $\beta$ existe) on voit que le conjugue de $G_0$ par $r_\gamma$ est le groupe dihedral

$$\langle r_\alpha, s_1 \rangle, \quad \text{ou } \alpha \text{ est un generateur de } \mu_n.$$

On a donc montre (en conjuguant $G$ par la rotation affine $r_\gamma \circ t_{-P}$ que

PROPOSITION 5.2. *Tout sous-groupe fini de* $\mathrm{Isom}(\mathbb{R}^2)$ *est conjugue (par une rotation affine) a un sous-groupe d'un groupe dihedral de la forme*

$$\{r_\alpha,\ s_1 \circ r_\alpha,\ \alpha \in \mu_n\}.$$

### 3.1. Existence de sous-groupes cycliques.

THÉORÈME 5.7. *Pour tout* $n \geqslant 1$*, il existe dans* $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{0}}$ *un et un seul sous-groupe cyclique d'ordre* $n$ *, qui correspond aux rotations associes au groupe* $\mu_n$*; par contre il existe une infinite de sous-groupe dihedraux d'ordre* $2n$*.*

PREUVE. Montrons que pour tout $n \geqslant 1$

$$\mu_n = \{\alpha \in \mathbb{C},\ \alpha^n = 1\},$$

est d'ordre $n$ exactement. Comme c'est l'ensemble des racines du polynome $X^n - 1$ et egalement le noyau du morphisme de groupe

$$z \in \mathbb{C}^\times \mapsto z^n \in \mathbb{C}^\times$$

c'est donc un sous-groupe de $\mathbb{C}^\times$ d'ordre $\leqslant n$ et cyclique en vertu des resultats precedents. On a par le theoreme fondamental de l'algebre

$$X^n - 1 = \prod_{\alpha \in \mu_n} (X - \alpha)^{\mu(\alpha)},\ \textit{avec } \mu(\alpha) \geqslant 1.$$

On a $\sum_\alpha \mu(\alpha) = 1$. Supposons que $\mu(\alpha_0)$ soit $\geqslant 2$ pour un certain $\alpha_0 \in \mu_n$ alors par la regle de derivation de Leibniz on a

$$(X^n - 1)' = nX^{n-1} = \sum_\alpha \mu(\alpha)(X - \alpha)^{\mu(\alpha)-1} \prod_{\alpha' \neq \alpha} (X - \alpha')^{\mu(\alpha')}$$

et donc

$$n\alpha_0^{n-1} = \sum_\alpha \mu(\alpha)(\alpha_0 - \alpha)^{\mu(\alpha)-1} \prod_{\alpha' \neq \alpha} (\alpha_0 - \alpha')^{\mu(\alpha')} = 0$$

ce qui est absurde car $n\alpha_0^{n-1} \neq 0$; ainsi $\mu(\alpha) = 1$ pour tout $\alpha$ et $|\mu_n| = n$. Ainsi $\mu_n$ est le groupe cyclique recherche.

Soit $\alpha$ un generateur de $\mu_n$ et $s_1$ la symetrie par rapport a l'axe reel:

$$s_1 : z \mapsto \overline{\beta z}.$$

On a $s_1^2 = \mathrm{Id}_{\mathbb{C}}$ et

$$s_1 r_\alpha s_1 : z \mapsto \overline{\alpha\overline{z}} = \overline{\alpha} z = \alpha^{-1} z = r_\alpha^{-1}(z).$$

Ainsi le groupe endrendre par $r_\alpha$ et $s_1$ est dihedral d'ordre $2n$.

Soit $r$ un rotation qui n'appartient par au groupe $\langle r_\alpha \rangle$ alors $s' = s_1 \circ r$ est une symetrie qui n'appartient pas au groupe $\langle r_\alpha, s_1 \rangle$ et le groupe $\langle r_\alpha, s' \rangle$ est different de $\langle r_\alpha, s_1 \rangle$. Une variation de cet argument montre qu'en variant $r$, on peut construire une infinite de tels groupes distincts. □

DÉFINITION 5.2. *Un generateur $\alpha$ du groupe cyclique $\mu_n$ (en d'autre termes une racine n-ieme de l'unite d'ordre n exactement) sera appellee racine primitive n-ieme de l'unite.*

REMARQUE 3.2. Le fait que $\mu_n$ soit d'ordre $n$ bien que cela paraisse evident (au moins si on admet l'existence de l'exponentielle complexe, cf. Exercies) n'est pas evident du point de vue algebrique: pour tout $p$ premier, soit $\mathbb{F}_p$ le corps fini a $p$ elements. Considerons le polynome $X^p - 1_{\mathbb{F}_p}$: on a (binome de Newton)

$$(X - 1_{\mathbb{F}_p})^p = X^p - 1_{\mathbb{F}_p} + \sum_{k=1}^{p-1} C_p^k (-1_{\mathbb{F}_p})^{p-k} X^k$$

mais pour $0 < k < p$, l'entier $C_p^k$ est divisible par $p$ de sorte que

$$C_p^k (-1_{\mathbb{F}_p})^{p-k} = q \times p.1_{\mathbb{F}_p} (-1_{\mathbb{F}_p})^{p-k} = 0_{\mathbb{F}_p}$$

de sorte que

$$X^p - 1_{\mathbb{F}_p} = (X - 1_{\mathbb{F}_p})^p$$

et donc $1_{\mathbb{F}_p}$ est la seule racine du polynome $X^p - 1_{\mathbb{F}_p}$ et donc la rseule racine $p$-ieme de l'unite !

CHAPITRE 6

# Polygones reguliers

Dans ce chapitre, on va utiliser la classification des groupes finis d'isometries pour etudier les polygones reguliers du plan. Commencons par definir un polygone.

## 1. Polygones generalises et poygones reguliers

DÉFINITION 6.1. *Soit $n \geqslant 3$ un entier, un polygone generalise a n cotes $\mathbf{P} \subset \mathbb{R}^2$ est une reunion de segments (appeles cotes du polygone) de la forme*

$$\mathbf{P} = \bigcup_{i=1\cdots n} [P_i P_{i+1}]$$

*avec*

$$P_1, \cdots, P_n,\ P_{n+1} = P_1$$

*un ensemble de n points* **distincts** *du plan (qu'on appelle sommets du polygone et on notera $\Sigma$ l'ensemble des sommets), tels que*

(1) *les sommets de deux cotes consecutifs ne sont pas alignes,*
(2) *deux segments quelconques n'ont pas plus d'un point d'intersection.*

*On notera*

$$\mathbf{P} = [P_1 \cdots P_n].$$

On a une notion de polygone un peu plus restrictive qu'on ne discutera pas plus avant

DÉFINITION 6.2. *Un polygone (tout court) a n cotes est un polygone generalise*

$$\mathbf{P} = \bigcup_{i=1\cdots n} [P_i P_{i+1}]$$

*avec $P_{n+1} = P_1$ tel que deux cotes ne se coupent que s'ils sont consecutifs; ils se coupent alors en un seul point (le sommet bordant les deux cotes). Un polygone a 3 cotes est un triangle, a 4 un quadrilatere etc... Un triangle rectangle est un triangle dont deux cotes sont perpendiculaires. Un parallelogramme est un quadrilatere $[PQRS]$ tel que les paires $([PQ], [RS])$ et $([QR], [SP])$ sont paralleles, etc...*

Si un polygone generalise n'est pas un polygone on dit qu'il est "croise" autrement si on veut preciser on dira qu'il est non-croise.

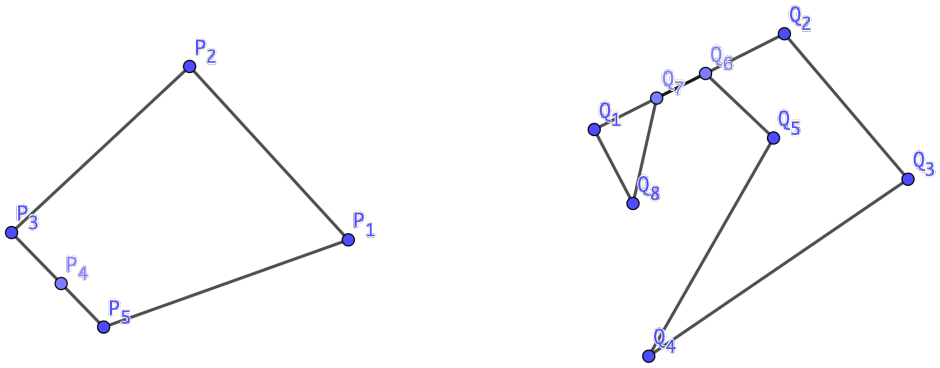


FIGURE 1. Lignes polygonales qui ne sont pas des polygones generalises.

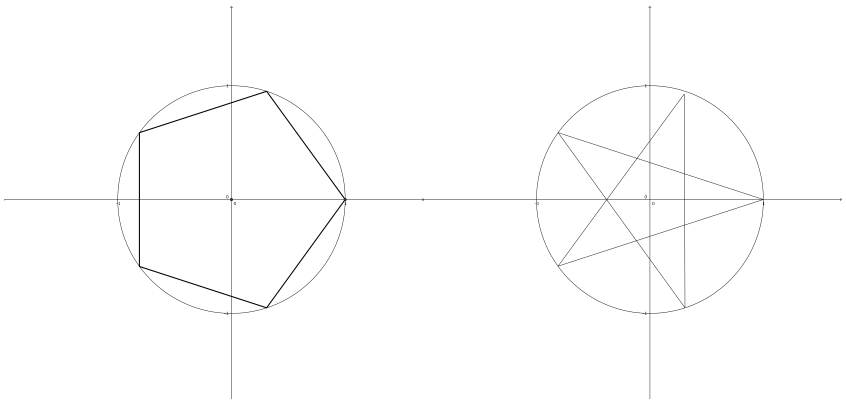

FIGURE 2. Pentagone regulier et pentagone regulier generalise.

DÉFINITION 6.3. *Un polygone generalise (croise ou pas)* $\mathbf{P}$ *a* $n$ *cotes est regulier si ses cotes sont de meme longueur et si les angles formes par deux cotes consecutifs orientes* $\overrightarrow{P_iP_{i+1}}$ *et* $\overrightarrow{P_{i+1}P_{i+2}}$ *sont egaux (pour* $i = n-1$*, on pose* $P_n = P_0,\ P_{n+1} = P_1$*).*

PROPOSITION 6.1. *Soit* $\phi \in \mathrm{Isom}(\mathbb{R}^2)$ *une isometrie et* $\mathbf{P} = [P_1, \cdots, P_n]$ *un polygone generalise (resp. regulier) alors* $\phi(\mathbf{P}) = [\phi(P_1), \cdots, \phi(P_n)]$ *est un polygone generalise (resp. regulier).*

PREUVE. Rappelons (cf. Exercice) que pour tout segment $[P, Q]$ on a

$$\phi([P, Q]) = [\phi(P), \phi(Q)].$$

En effet

$$[P,Q] = \{\lambda P + (1-\lambda)Q,\ \lambda \in [0,1]\}$$

et comme

$$\phi = t_{\phi(0)} \circ \phi_0$$

avec $\phi_0$ lineaire on a

$$\phi(\lambda P + (1-\lambda)Q) = \phi(0) + \phi_0(\lambda P + (1-\lambda)Q) = \phi(0) + \lambda\phi_0(P) + (1-\lambda)\phi_0(Q)$$
$$= \lambda(\phi(0) + \phi_0(P)) + (1-\lambda)(\phi(0) + \phi_0(Q)) = \lambda\phi(P) + (1-\lambda)\phi(Q).$$

(car $1.\phi(0) = \lambda\phi(0) + (1-\lambda)\phi(0)$).

On a donc

$$\phi(\mathbf{P}) = \bigcup_{i=1\cdots n} [\phi(P_i)\phi(P_{i+1})]$$

et il reste a verifier que les segments $[\phi(P_i)\phi(P_{i+1})]$ verifent bien les proprietes d'intersection demandees. Mais etant donnes deux segments $[\phi(P_i)\phi(P_{i+1})]$ et $[\phi(P_j)\phi(P_{j+1})]$ on a pour leur intersection

$$[\phi(P_i)\phi(P_{i+1})] \cap [\phi(P_j)\phi(P_{j+1})] = \phi([P_iP_{i+1}] \cap [P_jP_{j+1}])$$

et comme $\phi$ est un isometrie (bijective) $\phi([P_iP_{i+1}] \cap [P_jP_{j+1}])$ est vide, reduit a un point, ou est un segment si et seulement si $[P_iP_{i+1}] \cap [P_jP_{j+1}]$ est vide, reduit a un point, ou est un segment et donc les proprietes d'intersection des segments image par $\phi$ sont les meme que pour $\mathbf{P}$. En particulier cela montrer que $\phi$ envoie les cote de $\mathbf{P}$ sur ceux de $\phi(\mathbf{P})$ et les sommets sur les sommets. □

REMARQUE 1.1. Cette proposition est valide plus generalement si $\phi$ est une seulement application affine (la composee d'une translation et d'une application lineaire inversible): en effet, on a seulement utilise ici le fait que l'image par $\phi$ d'un segment est le segment d' extremites les images des extremites du segment d'origine et ce fait reste vrai pour les applications affines (la preuve donnee ci-dessus utilise seulement que l'isometrie est une application affine) et le fait qu'une application affine est bijective et donc preserve les intersection (ou l'absence d'intersection) entre les cotes.

Rappelons egalement

DÉFINITION 6.4. *Soit $\mathbf{P} \subset \mathbb{R}^2$ un sous-ensemble de $\mathbb{R}^2$, le groupe d'isometries de $\mathbf{P}$ est l'ensemble*

$$\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}} = \{\varphi \in \mathrm{Isom}(\mathbb{R}^2),\ \varphi(\mathbf{P}) = \mathbf{P}\}.$$

*C'est un sous-groupe de* $\mathrm{Isom}(\mathbb{R}^2)$.

Rappelons le resultat suivant vu en exercice

PROPOSITION 6.2. *Soit $\mathbf{P} \subset \mathbb{R}^2$ un ensemble quelconque et $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}$ son groupe d'isometries et soit $\psi \in \mathrm{Isom}(\mathbb{R}^2)$ une autre isometrie et $\psi(\mathbf{P})$ l'image de $\mathbf{P}$ par $\psi$ alors*

$$\mathrm{Isom}(\mathbb{R}^2)_{\psi(\mathbf{P})} = \mathrm{Ad}(\psi)(\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}) = \psi \circ \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}} \circ \psi^{-1}.$$

PREUVE. Soit $\phi' \in \psi \circ \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}} \circ \psi^{-1}$ alors $\phi' = \psi \circ \phi \circ \psi^{-1}$ avec $\phi \in \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}$ et

$$\phi'(\psi(\mathbf{P})) = \psi \circ \phi \circ \psi^{-1}(\psi(\mathbf{P})) = \psi \circ \phi(\mathbf{P}) = \psi(\mathbf{P})$$

car $\phi(\mathbf{P}) = \mathbf{P}$. On a donc

$$\mathrm{Isom}(\mathbb{R}^2)_{\psi(\mathbf{P})} \supset \psi \circ \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}} \circ \psi^{-1}.$$

Pour montrer l'inclusion inverse il suffit de montrer que

$$\psi^{-1}\circ \mathrm{Isom}(\mathbb{R}^2)_{\psi(\mathbf{P})}\circ\psi \subset \psi^{-1}\circ\psi\circ \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}\circ\psi^{-1}\circ\psi = \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}$$

car la conjugaison est une bijection. Applicant le resultat precedant a $\mathbf{P'} = \psi(\mathbf{P})$ et $\psi' = \psi^{-1}$ on a

$$\psi'\circ \mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}'}\circ {\psi'}^{-1} \subset \mathrm{Isom}(\mathbb{R}^2)_{\psi'(\mathbf{P}')}$$

ce qui est precisement cequ'on veut montrer. □

Si $\mathbf{P}$ est un polygone on a

THÉORÈME 6.1. *Soit $\mathbf{P}$ un polygone generalise alors son groupe d'isometries est fini; il est donc cyclique ou bien dihedral. Le centre de $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}$ est le barycentre des sommets de $\mathbf{P}$.*

PREUVE. On a vu qu'une isometrie transforme un polygone en un autre polygone envoyant les cotes sur les cotes et les sommets sur les sommets. Ainsi chaque element du groupe des isometries de $\mathbf{P}$ preserve les sommets de $\mathbf{P}$ et comme l'ensemble des sommets contient trois points non alignes le groupe des isometries est fini. □

## 2. Existence des polygones (generalises) reguliers

THÉORÈME 6.2. *Soit $G^+ \subset \mathrm{Isom}(\mathbb{R}^2)^+$ un groupe fini de rotations d'ordre $n \geqslant 3$ et $r$ un generateur de $G^+$ (rappelons que $G^+$ est cyclique). Soit $P \in \mathbb{R}^2$ qui n'est pas le centre $P_r$ de $r$. Alors le polygone generalise de sommets*

$$P_0 = P,\ P_1 = r(P),\ P_2 = r^2(P) = r(P_1), \cdots, P_{n-1} = r^{n-1}(P),\ P_n = r^n(P) = P$$

*est regulier; ses sommets sont situes sur le cercle centre en $P_r$ et de rayon $d(P_r, P)$ et le barycentre des sommets est $r$. Par ailleurs son groupe d'isometries est le groupe dihedral d'ordre $2n$*

$$G = \langle r, s\rangle$$

*engendre par $r$ et $s$ ou ou $s$ est la symetrie axiale d'axe la droite $(P_r, P)$.*

PREUVE. On a pour tout $k$,

$$r([P_k, P_{k+1}]) = [r(P_k), r(P_{k+1})] = [P_{k+1}, P_{k+2}]$$

donc la rotation $r$ envoie un cote sur le cote suivant (car $P_{n+1} = P$ et $P_{n+2} = P_1$), donc $r$ preserve $\mathbf{P}$; et donc $\mathbf{P}$ est preserve par n'importe quelle puissance $r^n$ et donc preserve par le groupe tout entier $G^+ = r^{\mathbb{Z}}$.

Soit $s$ la symetrie d'axe $(P_r, P)$. Montrons qu'elle preserve $\mathbf{P}$.

Pour cela on commence par montrer que

$$\mathrm{Ad}(s)(r)s\circ r\circ s^{-1} = r^{-1}.$$

Puisque cette symetrie preserve $P_r$, $\mathrm{Ad}(s)(r)$ a egalement $P_r$ comme point fixe et si $r_\alpha$ et $s_\beta$ designent les parties lineaires de $r$ et $s$ ($\alpha, \beta \in \mathbb{C}^1$), la partie lineaire de $\mathrm{Ad}(s)(r)$ est egale a

$$s_\beta r_\alpha s_\beta^{-1} : z \mapsto \overline{\beta(\alpha\overline{\beta z})} = \overline{\alpha} z = \alpha^{-1} z = r_\alpha^{-1}(z).$$

Ainsi comme le centre et les parties lineaires coincident, on a

$$srs^{-1} = r^{-1} \text{ et donc } sr^k s^{-1} = r^{-k}$$

On a ainsi (car $s(P) = P$)

$$s(P_k) = s(r^k(P)) = s\circ r^k\circ s^{-1}\circ s(P) = r^{-k}(s(P)) = r^{-k}(P) = P_{n-k}$$

et donc le segment $[P_k, P_{k+1}]$ est envoye sur le segment

$$[P_{n-k-1}, P_{n-k}]$$

et $s$ preserve donc $\mathbf{P}$. Ainsi le groupe $\langle r, s\rangle$ engendre par $r$ et $s$ preserve $\mathbf{P}$ et c'est un groupe dihedral d'ordre $2n$.

On sait que $\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}}$ est fini et on a vu qu'il contient le groupe dihedral $\langle r, s\rangle$. Il suffit donc de montrer que

$$\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{P}} = G^+.$$

Soit $r' \in \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{P}}$ alors $r'$ a le meme centre que $r$ et on a $r'(P) = P^k = r^k(P)$ ainsi la rotation $r'.r^{-k}$ a deux points fixes ($P_r$ et $P$) c'est donc l'identite et $r' = r^k$. On a donc montrer que

$$\mathrm{Isom}(\mathbb{R}^2)_{\mathbf{P}} = \langle r, s\rangle = G.$$

Montrons que $\mathbf{P}$ est regulier. Pour cela on va translater ce polygome.

Soit

$$r' = t_{-P_r} \circ r \circ t_{P_r}$$

le conjugue de $r$ par la translation $t_{P_r}$.

La rotation $r'$ est lineaire (car 0 est un point fixe) et engendre le groupe de rotations lineaire $G'^+ = \mathrm{Ad}(t_{-P_r})(G^+)$.

Soit $P' = t_{-P_r}(P) = P - P_r$ le translate de $P$ alors le polygone $\mathbf{P'}$ de sommets

$$P'_0 = P',\ P'_1 = r'(P'),\ P'_2 = r'^2(P') = r'(P'_1), \cdots, P'_{n-1} = r'^{n-1}(P'),\ P'_n = r'^n(P') = P'$$

est le translate

$$\mathbf{P'} = -P_r + \mathbf{P}.$$

Ainsi, quitte a remplacer $\mathbf{P}$ par $\mathbf{P'}$ on peut supposer que $G^+$ est un groupe de rotations lineaires et que $r = r_\alpha$ est lineaire de parametre complexe $\alpha \in \mathbb{C}^1$. Alors $\alpha$ est un generateur du groupe des racines $n$-iemes de l'unite $\mu_n$.

Soit $z \in \mathbb{C}$ correspondant a $P$ alors $z \neq 0$ et les complexes correspondant aux sommets de $\mathbf{P}$ sont

$$P_0 = z,\ P_1 = \alpha z, \cdots, P_{n-1} = \alpha^{n-1} z$$

et les cotes consecutifs $\overrightarrow{P_k P_{k+1}},\ k \geqslant 0$ sont donnes par les differences

$$\alpha^{k+1} z - \alpha^k z = \alpha^k(\alpha - 1)z,\ k \geqslant 0.$$

En particulier pour tout $k$, on a

$$d(\mathbf{0}, P_k) = |\alpha^k z| = |z|$$

est constant et

$$d(P_k, P_{k+1}) = |\alpha^{k+1} z - \alpha^k z| = |\alpha - 1||z|$$

est constant.

Par ailleurs

$$\vec{P_{k+1}P_k} = \alpha^k(1-\alpha)z,\ \vec{P_{k+1}P_{k+2}} = \alpha^{k+1}(\alpha - 1)z = -\alpha.\alpha^k(1-\alpha)z$$

et l'angle entre ces deux vecteurs (de meme longueur) est le quotient de ces deux nombres complexes

$$\widehat{P_k P_{k+1} P_{k+2}} = \frac{-\alpha.\alpha^k(1-\alpha)z}{\alpha^k(1-\alpha)z} = -\alpha$$

qui est constant. □

THÉORÈME 6.3. *Reciproquement tout polygone generalise regulier est obtenu de cette maniere.*

On deduit de ce resultat et du Theoreme precedent

COROLLAIRE 6.1. *Le groupe d'isometries d'un polygone generalise regulier* $\mathbf{P}$ *a* $n$ *cotes est dihedral d'ordre* $2n$*, engendre par* $r$ *une rotation d'ordre* $n$ *centree au barycentre des sommets de* $\mathbf{P}$ *et par la symmetrie axiale passant par un somment de* $\mathbf{P}$ *et le barycentre.*

**Preuve**: Soit

$$\mathbf{P} = [P_0, \cdots, P_{n-1}, P_n = P_0] \subset \mathbb{C}$$

un polygone generalise regulier, $\{z_0, \cdots, z_{n-1}\}$ les $n$ nombres complexes distincts correspondants aux sommets de $\mathbf{P}$ et (posant $z_n = z_0,\ z_{n+1} = z_1$) soient

$$\{\omega_k = z_{k+1} - z_k, k = 0 \cdots n-1\}$$

les nombres complexes correspondant aux cotes

$$\{\overrightarrow{P_k P_{k+1}}, k = 0, \cdots, n-1\};$$

par definition, l'angle $P_k\widehat{P_{k+1}P_{k+2}}$ est constant: notons le parametre complexe de cet angle par $-\alpha \in \mathbb{C}^1$. Ainsi, pour tout $k$, on a

$$\alpha\omega_k = \omega_{k+1} \text{ et donc } \omega_k = \alpha^k\omega_0.$$

Comme $\omega_n = \omega_0 = \alpha^n\omega_0$ on a $\alpha^n = 1$ et donc $\alpha \in \mu_n$; de plus

$$z_k = \omega_k + \cdots + \omega_0 + z_0 = z_0 + \omega_0(1 + \alpha + \cdots + \alpha^{k-1}) = z_0 + \omega_0\frac{\alpha^k - 1}{\alpha - 1}.$$

Supposons alors que $\alpha^d = 1$ pour $0 < d < n$, on aurait $z_d = z_0$ ce qui est absurde (car les $z_k$ sont distincts) et donc $\alpha$ est un generateur de $\mu_n$.

Calculons le barycentre $b$ de $\mathbf{P}$:

$$b = \frac{1}{n}\sum_{k=0}^{n-1} z_k = z_0 - \frac{\omega_0}{\alpha - 1} + \frac{\omega_0}{\alpha - 1}\sum_{k=0}^{n-1}\alpha_k = \frac{\alpha z_0 - z_1}{\alpha - 1} + \frac{\omega_0}{\alpha - 1}\frac{\alpha^n - 1}{\alpha - 1} = \frac{\alpha z_0 - z_1}{\alpha - 1}$$

et on a donc

$$z_k - b = \alpha^k\frac{z_1 - z_0}{\alpha - 1} \text{ et en particulier } z_0 - b = \frac{z_1 - z_0}{\alpha - 1}$$

de sorte que pour tout $k$

$$z_k = b + (z_0 - b)\alpha^k.$$

Posant

$$z'_k = z_k - b,\ k = 0 \cdots n$$

on voit que

$$z'_k = \alpha^k z'_0 = r_{\alpha,0}(z'_0)$$

est obtenu en applicant a $z'_0$ la rotation centree en 0 d'angle $\alpha$ $k$-fois; ainsi le polygone $\mathbf{P}' = [z'_0, \cdots, z'_{n-1}]$ est de la forme requise et $\mathbf{P}$ est son translate par $b$ et ses sommets sont obtenu en applicant les rotations centrees en $b$ et d'angles $\alpha^k$.

□

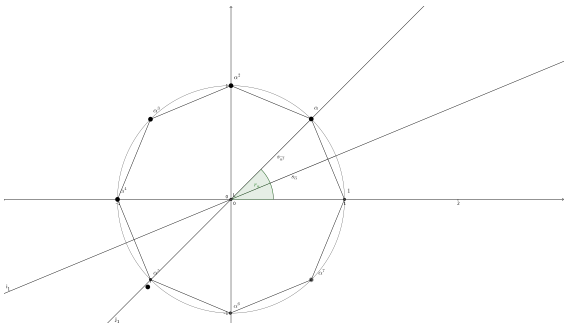

FIGURE 3. La rotation $r_\alpha$ et les symetries $s_{\overline{\alpha}}$ et $s_{\overline{\alpha}^2}$.

REMARQUE 2.1. Supposons (quitte a faire une translation et une rotation) que $\mathbf{P}$ a pour barycentre l'origine et que $P$ correspond a $x$ un nombre reel $> 0$. Avec les notation precedentes $r = r_\alpha$ avec $\alpha \in \mu_n$ un generateur et $s = s_1$ la symetrie par rapport a l'axe des $x$.

Notons que les isometries preservant $\mathbf{P}$ sont les rotations

$$r_1 = \mathrm{Id}_{\mathbb{R}^2},\ r_\alpha, \cdots, r_{\alpha^{n-1}}$$

et les symetries

$$s_1,\ r_\alpha s_1, \cdots, r_{\alpha^{n-1}} s_1.$$

On a

$$r_{\alpha^k} s_1 = s_{\alpha^{-k}}$$

(rappelons que $s_{\alpha^{-k}} : z \mapsto \overline{\alpha^{-k} z}$) et la symetrie $s_{\alpha^{-k}}$ est la symetrie par rapport a la droite $\mathbb{R}\beta^k$ avec $\beta$ verifiant

$$\beta^2 = \alpha.$$

il s'agit donc de la droite passant par l'origine et

- par le sommet $\alpha^{k/2}$ si $k$ est pair,
- par le milieu du segment $[\alpha^{\frac{k-1}{2}}, \alpha^{\frac{k+1}{2}}]$ si $k$ est impair.

## 3. Polygones constructibles a la regle et au compas

On sait depuis la petite enfance construire sur une feuille, plusieurs polygones reguliers comme le triangle equilateral, le carre, l 'hexagone voire, (si on a ete assidu) le pentagone, l' octogone (8 cotes), le decagone (10 cotes) et meme le dodecagone (12 cotes). En revanche, meme les enfants tres assidus n'ont jamais appris construire un heptagone (7 cotes), ni un enneagone (9 cotes) ou un triskaidecagone (13 cotes). On va expliquer pourquoi.

Cette question est egalement intimement liee au fait qu'en trigonometrie on apprend les cosinus et sinus des angles

$$0, \pi/6, \pi/4, \pi/3, \pi/2, \pi$$

mais pas celui de $\pi/7$ ou $\pi/9$ (notons cependant que l'on pourrait eventuellement apprendre le cosinus et sinus des angles $\pi/5$ ou $2\pi/5$, cf. les exercices...).

La notion fondamentale pour expliquer cela est celle de

DÉFINITION 6.1 (Constructibilite a la regle et au compas). *Soit $P_0 = (0,0)$ et $P_1 = (1,0)$. Un point $P$ du plan est constructible à la regle et au compas a partir d'un ensemble fini de points $\mathcal{P}_n = \{P_0, P_1, \cdots, P_n\}$ contenant $P_0$ et $P_1$ si $P$ est obtenu soit*

- *comme l'intersection de deux droites passant chacune par deux points distincts de $\{P_0, P_1, \cdots, P_n\}$*
- *de l'intersection d'une droite passant par deux points distincts de $\{P_0, \cdots, P_n\}$ et d'un cercle dont le centre est contenu dans $\{P_0, P_1, \cdots, P_n\}$ et le rayon est egal a la distance $|P_iP_j|$ pour $0 \leqslant i, j \leqslant n$.*
- *de l'intersection de deux cercles centres en des elements de $\mathcal{P}_n$ et de rayons $|P_iP_j|$ et $|P_kP_l|$.*

*– Un point $P$ est constructible a la regle et au compas si il existe un ensemble de points $\{P_0, P_1, \cdots, P_n, P_{n+1}\}$ avec $P_{n+1} = P$ tel que pour tout $i \geqslant 2$, $P_i$ soit constructible à la regle et au compas a partir de $\{P_0, P_1, \cdots, P_{i-1}\}$.*

Identifiant le plan $\mathbb{R}^2$ a $\mathbb{C}$, on a

DÉFINITION 6.5. *Un nombre complexe $z = x + iy$ est constructible a la regle et au compas si et seulement si le point $P = (x, y)$ l'est.*

Notons que

- Tout entier relatif est constructible,
- tout nombre rationel est constructible (Theoreme de Thales -cf. ci-dessous)
- $\sqrt{2}$ et plus generalement toute racine carree d'un nombre rationel est constructible.

Une serie de problemes fameux qui remontent a l'antiquite se reduisent a determiner si tel ou tel nombre est constructible:

(1) Doublement du cube: peut on construire avec regle et compas un cube dont le volume est le double de celui du cube unite ?
(2) Trisection de l'angle: est-il possible en general de couper un angle en trois angles egaux a la regle et au compas?
(3) Peut on construire les polygones reguliers a la regle et au compas ?
(4) Quadrature du cercle: peut on construire avec regle et compas un carre dont l'aire est celle du cercle de rayon unite?

THÉORÈME 6.4. *L'ensemble des nombres complexes constructibles a la regle et au compas forme un corps.*

PREUVE. Notons que puisque les projections d'un point sur l'axe des abscisses et l'axe des ordonnees peuvent etre construites a la regle et au compas on voit que

$$z = x + iy \in \mathbb{C} \text{ est contructible si et seulement si } x \text{ et } y \text{ le sont.}$$

Il suffit alors de montrer que si les reels $x$ et $y$ (correspondant aux points $(x,0)$ et $(y,0)$) sont constructibles et $y \neq 0$ alors

$$-x,\ x+y,\ xy,\ x/y$$

sont constructibles. Les deux premiers sont evidents; les deux suivants relevent du theoreme de Thales: □

Par des methodes de geometrie, d'algebre (theorie de Galois) et d'arithmetique (theorie algbrique des nombres et theorie de la transcendance) on montre que les problemes ci-dessous admettent les reponses suivantes

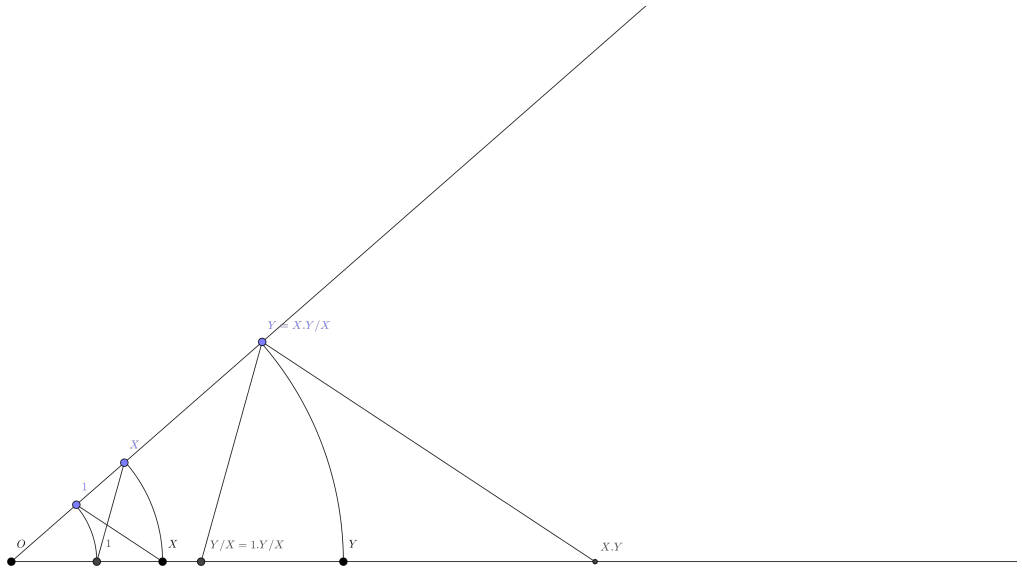


FIGURE 4. Par Thales $XY$ et $X/Y$ sont constructibles si $X$ et $Y$ le sont.

(1) Doublement du cube: c'est impossible.
(2) Trisection de l'angle: c'est impossible en general.
(3) Construction de polygones reguliers: il n'est pas possible de les construire tous; voir ci-dessous.
(4) Quadrature du cercle: c'est impossible.

La troisieme probleme revient a determiner si $\alpha_n \in \mu_n$ est constructible. En utilisant des methodes d'arithmetique et de theorie de Galois Gauss et Wantzel on montre

THÉORÈME 6.5 (Gauss-Wantzel). *Un polygone regulier a $n$ cotes est constructible a la regle et au compas si et seulement si $n$ est de la forme*

$$n = 2^k \text{ ou bien } n = 2^k \prod_i p_i$$

*ou $\prod_i p_i$ est un produit (non-vide) de nombres premiers tous distincts et "de Fermat": on dit que $p_i$ est de Fermat si $p_i = 2^{2^{k_i}} + 1$ avec $k_i \geqslant 0$ un entier.*

REMARQUE 3.1. Gauss est devenu celebre quand a 19 ans il a montre que la condition etait suffisante et a effectivement construit le polygone regulier a 17 cotes (voir la figure ci-dessous qui donne les 64 etapes de la construction) et un peu plus tard Wantzel a montre qu'elle etait necessaire.

On peut donc construire:

- Le triangle equilateral: $3 = 2^1 + 1$.
- Le carre: $4 = 2^2$
- Le pentagone regulier : $5 = 2^2 + 1$.
- L' hexagone regulier: $6 = 2 \times 3$.

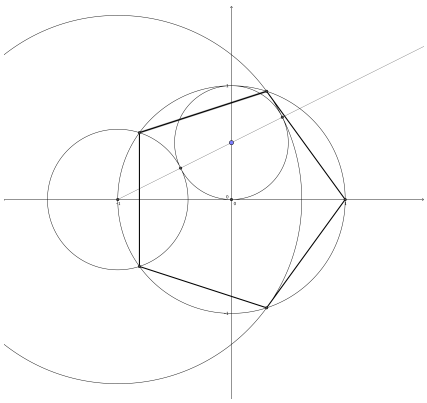

FIGURE 5. Construction de Duerer du pentagone regulier.

- Le decagone regulier: $10 = 2 \times 5$
- le polygone regulier a 15 cotes: $15 = 3 * 5$
- le polygone regulier a 17 cotes: $17 = 2^4 + 1$.
- En fait si on sait construire un polygone regulier a $n$ cotes on sait construire celui a $2n$ cotes en construisant par bisection des angles.

REMARQUE 3.2. Les seuls nombres premiers de Fermat connus a ce jour sont

$$2 = 1 + 2^0,\ 3 = 1 + 2^1,\ 5 = 1 + 2^2,\ 17 = 1 + 2^4,\ 257 = 1 + 2^8, 65537 = 1 + 2^{16}.$$

Notons que pour que $2^l + 1$ soit premier il est necessaire que $l$ soit ou bien nul ou bien une puissance de 2 (Fermat).

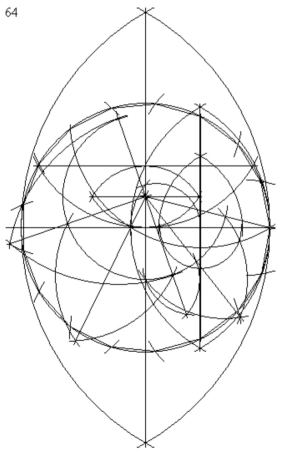


FIGURE 6. Construction de Gauss du polygone regulier a 17 cotes (source Wikipedia)

CHAPITRE 7

# Action d'un groupe sur un ensemble

Dans ce chapitre on definit et on etudie la notion d'action d'un groupe sur un ensemble; on appliquera cette notion dans le chapitre suivant a l'action d'un sous-groupe d'isometrie preservant un pavage.

## 1. Action a gauche, a droite

Soit $(G,.)$ un groupe et $X$ un ensemble. Une action de $G$ sur $X$ est la donnee pour chaque element de $G$ d'une bijection de $X$ sur lui-meme de sorte que la famille de ces bijections soient compatible avec les lois de groupes sur $G$ et sur $\mathrm{Bij}(X)$.

DÉFINITION 7.1. *Une action a gauche d'un groupe $G$ sur un ensemble $X$ est la donnee d'un morphisme de groupe*

$$\mathrm{a}_l : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(X) \\ g & \mapsto & \mathrm{a}_l(g) : X \mapsto X \end{array}.$$

*En d'autre termes c'est une application verifiant*

(1) $\mathrm{a}_l(e_G) = \mathrm{Id}_X$,
(2) $\mathrm{a}_l(g^{-1}) = \mathrm{a}_l(g)^{-1}$,
(3) $\mathrm{a}_l(g.g') = \mathrm{a}_l(g) \circ \mathrm{a}_l(g')$.

*On notera $G \curvearrowright X$ le fait qu'un groupe agisse sur un ensemble a gauche. Un ensemble $X$ muni d'une action à gauche d'un groupe $G$ sera appelé un $G$-ensemble à gauche.*

NOTATION. Soit $\mathrm{a}_l : G \to \mathrm{Bij}(X)$ une action alors pour tout $g$, $\mathrm{a}_l(g)$ est une bijection de $X$ sur $X$. Pour designer l'image d'un element $x \in X$ par cette bijection la notation

$$\mathrm{a}_l(g)(x)$$

est un peu lourde. On l'omettra ou on la remplacera avec un autre symbole par exemple on pourra ecrire

$$\mathrm{a}_l(g) = (x)g.x \text{ ou } g \odot x \text{ a la place de } \mathrm{a}_l(g)(x).$$

Comme $\mathrm{a}_l$ est un morphisme de groupes on a

$$\mathrm{a}_l(g) \circ \mathrm{a}_l(g') = \mathrm{a}_l(g.g').$$

En d'autres termes, pour tout $x \in X$ et tout $g, g' \in G$ on a

$$\mathrm{a}_l(g)(\mathrm{a}_l(g')(x)) = \mathrm{a}_l(g.g')(x).$$

Avec la notation introduite ci-dessus cela nous donne

$$g \odot (g' \odot x) = g \odot g' \odot x = (g.g') \odot x.$$

Cela conduit a la definition alternative mais equivalente d'une action de groupes:

DÉFINITION 7.2. *Une action à gauche d'un groupe $G$ sur un ensemble $X$ est la donnee d'une application*

$$\odot : \begin{array}{ccc} G \times X & \mapsto & X \\ (g,x) & \mapsto & g \odot x \end{array}$$

*vérifiant*

$$\forall x \in X,\ e_G \odot x = x$$

$$\forall g, g' \in G, x \in X,\ g \odot (g' \odot x) = (g.g') \odot x;$$

*(en particulier si $g' = g^{-1}$ on aura pour tout $x \in X$*

$$g \odot (g^{-1} \odot x) = (g.g^{-1}) \odot x = e_G \odot x = x.)$$

1.0.1. *Action a droite.* Quelque fois on tombe naturellement sur la structure suivante

DÉFINITION 7.3. *Une action a droite d'un groupe $G$ sur un ensemble $X$ est la donnee d'une application*

$$\mathrm{a}_r : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(X) \\ g & \mapsto & \mathrm{a}_r(g) : X \mapsto X \end{array}$$

*verifiant*

(1) $\mathrm{a}_r(e_G) = \mathrm{Id}_X$,
(2) $\mathrm{a}_r(g^{-1}) = \mathrm{a}_r(g)^{-1}$,
(3) $\mathrm{a}_r(g.g') = \mathrm{a}_r(g') \circ \mathrm{a}_r(g)$.

*On notera $X \curvearrowleft G$ le fait qu'un groupe agisse sur un ensemble a droite. Un ensemble $X$ muni d'une action à gauche d'un groupe $G$ sera appelé un $G$-ensemble à gauche.*

On a donc par exactement un morphisme de groupe mais presque:

EXERCICE 7.1. Soit $\mathrm{a}_r : G \to \mathrm{Bij}(X)$ une action a droite alors l'application

$$g \in G \mapsto \mathrm{a}_r(g^{-1}) \in \mathrm{Bij}(X)$$

est un morphisme de groupe (donc definit une action a gauche).

On a la formulation equivalente

DÉFINITION 7.4. *Une action à droite d'un groupe $G$ sur un ensemble $X$ est la donnee d'une application*

$$\odot : \begin{array}{ccc} X \times G & \mapsto & X \\ (x,g) & \mapsto & x \odot g \end{array}$$

*vérifiant*

$$\forall x \in X,\ x \odot e_G = x$$

$$\forall g, g' \in G, x \in X,\ (x \odot g) \odot g' = x \odot (g.g');$$

REMARQUE 1.1. Si $\odot$ est une action à gauche, l'application

$$\tilde{\odot} : \begin{array}{ccc} X \times G & \mapsto & X \\ (x,g) & \mapsto & x \tilde{\odot} g = g^{-1} \odot x \end{array}$$

défini une action à droite. Il est donc facile de passer d'une action à gauche à une action à droite et vice-versa.

### 1.1. Exemples.

1.1.1. *Action tautologique du groupe symetrique.* Le groupe $\mathfrak{S}_X = \mathrm{Bij}(X)$ des permutations de $X$ sur $X$ munis de $\mathrm{Id}_X$ comme element neutre et de la composition $\circ$ comme loi de groupe agit a gauche sur l'ensemble $X$, le morphisme $\mathrm{a}_l$ etant l'application identite

$$\mathrm{Id}_{\mathrm{Bij}(X)} : \sigma \in \mathrm{Bij}(X) \to \sigma \in \mathrm{Bij}(X).$$

C'est l'action *tautologique*: cette action est donnee pour $\sigma \in \mathfrak{S}_X$ et $x \in X$ par

$$\sigma \odot x = \sigma(x).$$

On a pour tout $x \in X$

$$\mathrm{Id}_X \odot x = \mathrm{Id}_X(x) = x$$

et

$$\sigma \odot (\sigma' \odot x) = \sigma(\sigma'(x)) = \sigma \circ \sigma'(x) = \sigma \circ \sigma' \odot x.$$

l'identite

$$\sigma(\sigma'(x)) = \sigma \circ \sigma'(x)$$

est precisement la definition de la composee de deux applications.

1.1.2. *Action triviale.* C'est l'action qui correspond au morphisme constant

$$g \in G \to \mathrm{Id}_X \in \mathrm{Bij}(X).$$

En d'autres termes

$$\forall x \in X,\ g \in G,\ g.x = x.$$

1.1.3. *Action restreinte a un sous-groupe.* Si un groupe $G$ agit sur un ensemble $X$ alors tout sous-groupe $H \subset G$ agit egalement sur $X$: le morphisme est le morphisme $\mathrm{a}_{l\,H}$ par restriction de $\mathrm{a}_l$ au sous-groupe $H \subset G$. On parle "d'action par restriction a $H$ de l'action de $G$ sur $X$".

1.1.4. *Action du groupe des isometrétries sur* $\mathbb{R}^2$. Considerons le cas $X = \mathbb{R}^2$ et $G = \mathrm{Isom}(\mathbb{R}^2)$ le groupe des isometrie de $\mathbb{R}^2$. On a montrer que l'ensemble des isometrie de $\mathbb{R}^2$ est un sous-groupe de $\mathrm{Bij}(\mathbb{R}^2)$ et donc agit sur $\mathbb{R}^2$ par restriction de l'action tautologique de $\mathrm{Bij}(\mathbb{R}^2)$.

1.1.5. *Iteration d'une permutation.* Soit $X$ un ensemble et $\sigma \in \mathrm{Bij}(X)$ une bijection de $X$, le sous groupe $\sigma^{\mathbb{Z}} \subset \mathrm{Bij}(X)$ agit donc sur $X$ par restriction. On rappelle qu'on dispose d'un morphisme de groupes

$$\exp_\sigma : n \in \mathbb{Z} \to \sigma^n \in \sigma^{\mathbb{Z}} \subset \mathrm{Bij}(X)$$

obtenu en posant

$$\sigma^0 = \mathrm{Id}_X$$

pour $n \in \mathbb{N}_{\geqslant 1}$

$$\sigma^n = \sigma \circ \sigma \cdots \circ \sigma,\ n - fois$$

et pour $n < 0$

$$\sigma^n = \sigma^{-1} \circ \sigma^{-1} \cdots \circ \sigma^{-1},\ |n| - fois$$

de sorte que

$$\exp_\sigma(m+n) = \sigma^{m+n} = \sigma^m \circ \sigma^n = \exp_\sigma(m) \circ \exp_\sigma(n).$$

Ainsi le morphisme

$$\exp_\sigma : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathrm{Bij}(X) \\ n & \mapsto & \sigma^n \end{array}$$

defini une action de $\mathbb{Z}$ sur $X$:

$$n \odot x := \sigma^n(x).$$

1.1.6. *Action d'un groupe sur lui-même par translation.* Soit $G$ un groupe, alors $G$ agit sur lui-même (à gauche) par multiplication à gauche et (à droite) par multiplication à droite:

$$g \odot h = g.h.$$

On dit que $G$ agit sur lui-même par translations: le morphisme est le morphisme "translation a gauche"

$$\mathrm{tl} : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{tl}_g : h \in G \to \mathrm{tl}_g(h) = g.h \end{array}$$

ou le morphisme "translation a droite"

$$\mathrm{tr} : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{tr}_g : h \in G \to \mathrm{tr}_g(h) = h.g \end{array}$$

Exemple 1.1. Un cas important pour ce cours est l'action par translation d'un espace vectoriel $V$ sur lui-même: pour tout $\vec{v} \in V$ on note $T_{\vec{v}}$ la translation de vecteur $\vec{v}$

$$T_{\vec{v}} : \vec{x} \mapsto T_{\vec{v}}(\vec{x}) = \vec{x} + \vec{v}.$$

1.1.7. *Action d'un groupe sur lui-même par conjugaison.* Une deuxième action importante d'un groupe sur lui-même est l'action par conjugaison: etant donné $g \in G$ soit $\mathrm{Ad}(g)$ l'application

$$\mathrm{Ad}(g) : \begin{array}{ccc} G & \mapsto & G \\ h & \mapsto & g.h.g^{-1} \end{array}$$

alors $\mathrm{Ad}(g) \in \mathrm{Bij}(G)$ est une bijection (et egalement un morphisme de groupes) d'inverse $\mathrm{Ad}(g^{-1})$ et l'application

$$\mathrm{Ad} : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{Ad}(g) : h \in G \to ghg^{-1} \end{array}$$

est un morphisme de groupes. Cela definit donc une action de $G$ sur $G$ qu'on appelle action *adjointe* ou par *conjugaison.*

1.1.8. *Action induite sur les sous-ensembles et les fonctions.* L'action (a gauche) d'un groupe $G$ sur un ensemble $X$, induit une action (a gauche) de $G$ sur l'ensemble $\mathcal{P}(X)$ des sous-ensembles de $X$: etant donne $Y \subset X$ et $g \in G$, on pose

$$g \odot Y = \{g \odot y,\ y \in Y\} \subset X.$$

Notons que $\mathcal{P}(X)$ est en bijection avec $\{0,1\}^X = \{\phi : X \to \{0,1\}\}$ l'ensemble des fonctions de $X$ a valeurs dans $\{0,1\}$ (a un sous-ensemble $Y \subset X$ on associe la fonction indicatrice

$$1_Y : \begin{array}{ccc} X & \mapsto & \{0,1\} \\ x & \mapsto & \begin{cases} 1 & \text{si } x \in Y \\ 0 & \text{sinon.} \end{cases} \end{array}$$

qui vaut un ou zero suivant que l'on se trouve dans l'ensemble ou pas. L'action de $G$ sur $\mathcal{P}(X)$ defini donc une action de $G$ sur $\mathcal{F}(X, \{0,1\})$.

Cette action se generalise a tout espace de fonctions: etant donne

$$\mathcal{F}(X; \mathbb{R}) = \{f : x \mapsto f(x) \in \mathbb{R}\},$$

l'espace des fonctions sur $X$ a valeurs dans $\mathbb{R}$, l'action (a gauche) d'un groupe $G$ sur $X$, induit une action (a droite) de $G$ sur l'ensemble $\mathcal{F}(X; \mathbb{R})$: etant donne $f : X \mapsto \mathbb{R}$ et $g \in G$, on definit la fonction $f_{|g}$ par la formule

$$f_{|g} : x \mapsto f(g \odot x).$$

Notons que pour obtenir une action a gauche il suffit de poser

$$g.f : x \mapsto f_{|g^{-1}}(x) = f(g^{-1} \odot x).$$

EXERCICE 7.2. Verifier que $(f, g) \mapsto f_{|g}$ est bien une action a droite et que $(g, f) \mapsto g.f$ est une action a gauche.

## 2. Noyau, Image d'une action

DÉFINITION 7.5. *Soit $G \curvearrowright X$ une action a gauche d'une groupe sur un ensemble defini par un morphisme*

$$\mathrm{a}_l : G \to \mathrm{Bij}(X).$$

*Le noyau et l'image de cette action sont definis respectivement de noyau* $\ker \mathrm{a}_l \in G$ *et l'image* $\mathrm{Im}\, \mathrm{a}_l \in \mathrm{Bij}(X)$ *de ce morphisme.*

*Si on dispose d'une action a droite* $\mathrm{a}_r : G \to \mathrm{Bij}(X)$ *le noyau et l'image de l'action sont les noyau et image de l'action a gauche correspondante:*

$$\mathrm{a}_l : g \mapsto \mathrm{a}_r(g^{-1}).$$

EXEMPLE 2.1. Un groupe $G$ agit trivialement sur un ensemble $X$ ssi le noyau de l'action est $G$ tout entier.

DÉFINITION 7.6. *Etant donne $G \curvearrowright X$ un $G$-ensemble (a gauche). Si* $\ker(\mathrm{a}_l) = \{e_G\}$ *c'est a dire si le morphisme*

$$\mathrm{a}_l : G \mapsto \mathrm{Bij}(X)$$

*est injectif, on dira que l'action est fidele ou que $G$ agit fidelement sur $X$. De maniere equivalente, $G$ agit fidelement sur $X$*

$$\forall x \in X,\ g \odot x = x \Longrightarrow g = e_G.$$

EXERCICE 7.3. Montrer que l'action d'un groupe $G$ sur lui-meme par translations est fidele.

EXERCICE 7.4. Montrer que le noyau de l'action de $G$ sur lui-meme par conjugaison est le sous-groupe appele le centre de $G$

$$Z(G) = \{h \in G,\ \text{ pour tout } g \in G\ g.h = h.g\}.$$

**2.1. Action par automorphismes relatifs a une structure.** Soit $X$ un $G$-ensemble muni d'une structure supplementaire $Str$ (par exemple $X$ est un groupe, un espace vectoriel etc...); on dira que $G$ agit sur $X$ par automorphismes pour cette structure si l'image de cette action $\mathrm{Im}\, \mathrm{a}_l$ est contenue dans le sous-groupe $\mathrm{Aut}_{Str}(X) \subset \mathrm{Bij}(X)$ des bijections preservant la structure additionelle de $X$, ie.

$$\forall g \in G,\ \mathrm{a}_l(g) \in \mathrm{Aut}_{Str}(X).$$

EXEMPLE 2.2. Si $X$ est un $\mathbb{R}$-espace vectoriel et que pour tout $g$

$$\mathrm{a}_l(g) : X \mapsto X$$

est une application lineaire. On dira alors que $G$ agit lieairement sur $X$.

REMARQUE 2.1. Pour montrer que $G$ agit sur $X$ par automorphismes relativement a une structure $Str$, il suffit de montrer que pour tout $g$ $\mathrm{a}_l(g) : x \mapsto g \odot x$ est un morphisme pour cette structure: en effet $\mathrm{a}_l(g^{-1})$ sera egalement un morphisme pour cette structure et $\mathrm{a}_l(g)$ et $\mathrm{a}_l(g^{-1})$ sont des morphisme et des applications reciproques l'une de l'autre, ce sont donc des isomorphismes.

EXEMPLE 2.3. L'action de $\mathrm{Isom}(\mathbb{R}^2)$ sur $\mathbb{R}^2$ est par isometries: elle preserve la structure donnee par la distance euclidienne sur $\mathbb{R}^2$.

EXEMPLE 2.4. L'action de $G$ sur lui-meme par conjugaison est une action par automorphismes relativement a la structure de groupe (Exercice: le verifier).

EXEMPLE 2.5. L'action de $G$ sur lui-meme par translations a gauche n'est PAS une action par automorphismes relativement a la structure de groupe sauf si le groupe est trivial (Exercice: le verifier).

EXEMPLE 2.6. Soit $G$ agissant a gauche sur un ensemble $X$, et $\mathcal{F}(X;\mathbb{R}) \curvearrowleft G$ l'action a droite de $G$ sur l'espace vectoriel des fonctions sur $X$ induite par cette action. Le groupe $G$ agit (a droite) sur $\mathcal{F}(X;\mathbb{R})$ par automorphismes lineaire, ie. relativement a la structure d'espace vectoriel: pour tout $g$, l'application

$$\mathrm{a}_r(g) : f \mapsto f_{|g}$$

est une application lineaire inversible (Exercice: le verifier).

### 2.2. Morphisme de $G$-ensembles.

DÉFINITION 7.7. *Un morphisme de $G$-ensembles (a gauche) – encore appele "application d'entrelacement"– est une application*

$$\phi : X \mapsto Y$$

*qui est compatible avec les structures de $G$-ensemble de $X$ et $Y$: elle satisfait*

$$\forall g \in G,\ \forall x \in X,\ \phi(g \odot x) = g \otimes \phi(x).$$

*De maniere equivalente on a pour tout $g \in G$*

$$\varphi \circ \mathrm{a}_{l,X}(g) = \mathrm{a}_{l,Y} \circ \varphi(g)$$

*ou $\mathrm{a}_{l,X}$ et $\mathrm{a}_{l,Y}$ designent respectivement les applications de $G$ dans $\mathrm{Bij}(X)$ et $\mathrm{Bij}(Y)$ qui definissent ces actions.*

*On notera $\mathrm{Hom}_{G-ens}(X,Y)$ l'ensemble des morphismes de $G$-ensembles de $X$ vers $Y$. Si $\phi$ est bijectif on dira que $\phi$ est un isomorphisme (ou un homeomorphisme) de $G$-ensembles. Si $Y = X$ on parlera d'endomorphisme ou d'automorphisme de $G$-ensembles...*

EXERCICE 7.5. Montrer que si un morphisme $\varphi : X \to Y$ de $G$-ensembles est bijectif alors l'application reciproque $\varphi^{-1}$ est encore un morphisme de $G$-ensembles.

## 3. Points fixes et Stabilisateurs

DÉFINITION 7.1. *Soit $G \curvearrowright X$ un $G$-ensemble. Un element $x \in X$ est un point fixe d'un element $g \in G$ si*

$$g.x = x.$$

*On notera l'ensemble des points fixes d'un element $g \in G$ par*

$$X^g = \mathrm{Fix}_X(g) = \{x \in X,\ g.x = x\}.$$

*Dualement etant donne $x \in X$ le stabilisateur de $x$ est l'ensemble des $g \in G$ dont $x$ est un point fixe, on le note*

$$G_x = \{g \in G, g.x = x\} \subset G.$$

PROPOSITION 7.1. *Le stabilisateur $G_x$ est un sous-groupe de $G$.*

PREUVE. Clairement $e_G \in G_x$. Il suffit de montrer que

$$\forall g, g' \in G_x,\ g.g'^{-1} \in G_x.$$

□

EXEMPLE 3.1. Soit un sous-groupe $H$ agissant sur $G$ par multiplication a gauche et soit $g \in G$, on a

$$H_g = \{h \in H, h.g = g\} = \{e_G\}.$$

## 4. Orbites

DÉFINITION 7.8. *Etant donné une action de groupe $G \curvearrowright X$ et $x \in X$, l'orbite de $x$ sous l'action de $G$ (la $G$-orbite de $x$) est le sous-ensemble*

$$G.x = \{g.x,\ g \in G\} \subset X.$$

*Soient $x' \in X$, on notera la relation "$x'$ appartient a la $G$-orbite de $x$" sous la forme*

$$x' \sim_G x \iff x' \in G.x$$

THÉORÈME 7.1. *La relation $x' \sim_G x$ est une relation d'equivalence et dont les differentes classes d'equivalences sont les orbites $G.x$ pour $x \in X$.*

PREUVE. Cette relation est

- Reflexive: soit $x \in X$, on a $x = e_G.x \in G.x$ donc $x \sim_G x$.
- Symetrique: soient $x, x' \in X$ si $x' \sim_G x$ alors $x' \in G.x$ alors $x' = g.x$ pour $g \in G$ et $g^{-1}.x' = g^{-1}.g.x = x$ donc $x \in G.x'$ et $x \sim_G x'$.
- Transitive: soient $x, x', x'' \in X$, si $x' \sim_G x$ et $x'' \sim_G x'$ alors $x' = g.x$ et $x'' = g'.x'$ pour $g, g' \in g$ et donc $x'' = g'.g'.x = (g'g).x \in G.x$ et $x'' \sim_G x$.

□

Il sera utile d'introduire une notation pour l'espace de toutes les orbites.

DÉFINITION 7.9. *On note*

$$G\backslash X = \{G.x,\ x \in X\} \subset \mathcal{P}(X)$$

*l'ensemble des $G$-orbites de $X$ (c'est un sous-ensemble de l'ensemble des parties de $X$); on appelle cet ensemble le quotient de $X$ sous l'action de $G$.*

*On note $\pi_G$ ou encore* $\mathrm{red}_G$*, l'application surjective*

$$\mathrm{red}_G = \pi_G : \begin{array}{ccc} X & \mapsto & G\backslash X \\ x & \mapsto & G.x \end{array}$$

*qui a un element de $x$ associe son orbite; on l'appelle cette application "projection sur $G\backslash X$" ou encore "reduction modulo $G$" et on note egalement l'image de $x$, $G.x$, "$x$ modulo $G$" qu'on note encore*

$$G.x = x \,(\mathrm{mod}\, G).$$

*Si $X \curvearrowleft G$ agit a droite, l'orbite de $x$ sera notee $x.G$ et l'espace des orbites $X/G$.*

EXEMPLE 4.1. Soit $G = \mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ le groupe des rotations centrees en $\mathbf{0}$ agissant sur $X = \mathbb{R}^2$. Ses orbites sont les cercle centres en $\mathbf{0}$. L'ensemble des orbites $G\backslash X$ s'identifie avec la demi-droite $\mathbb{R}_{\geqslant 0}(1, 0)$ (ou avec n'importe quelle demi-droite partant de $(0, 0)$).

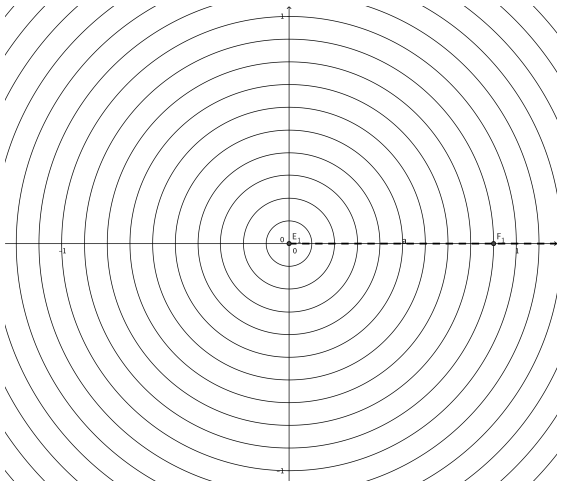

FIGURE 1. Orbites de $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}} \curvearrowright \mathbb{R}^2$.

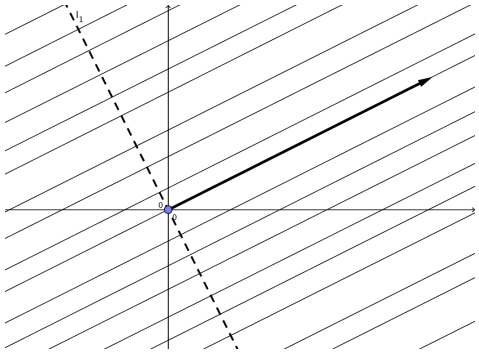

FIGURE 2. Orbites de $\mathbb{R}.(2,1) \curvearrowright \mathbb{R}^2$.

EXEMPLE 4.2. Soit $G = \mathbb{R}.(2,1)$ le groupe des multiples du vecteur $(2,1)$; ce groupe agit sur $X = \mathbb{R}^2$ par translations; ses orbites sont les droites de direction le vecteur $(2,1)$. L'ensemble des orbites $G\backslash X$ s'identifie avec la droite $\mathbb{R}(1,-2)$ (ou avec n'importe quelle droite non-paralelle a $(2,1)$.

NOTATION.

Comme la relation $x \sim_G x'$ est une relation d'equivalence dont les classes d'equivalences sont les differentes $G$-orbites on a

THÉORÈME 7.2 (Disjonction et partition des orbites). *Soit $G \curvearrowright X$ un $G$ ensemble et $x, x' \in X$.*

*Si $G.x$ et $G.x'$ sont deux $G$-orbites alors*

$$G.x \cap G.x' \neq \emptyset \Leftrightarrow G.x = G.x'$$

*(ou de maniere equivalente*

$$G.x \cap G.x' = \emptyset \Leftrightarrow G.x \neq G.x'.$$

*En particulier*

$$x' \in G.x \Leftrightarrow G.x' = G.x.$$

*En d'autre termes deux $G$-orbites distinctes sont disjointes et comme tout element $x \in X$ est contenu dans au moins une $G$-orbite (la sienne $G.x$), l'ensemble des $G$-orbites de $X$ forme une partition de $X$:*

$$X = \bigsqcup_{\mathcal{O} \in G\backslash X} \mathcal{O}.$$

C'est un consequence d'un resultat general sur les relations d'equivalences sur un ensemble mais on peut retrouver cela directement a partir des definitions de l'action d'un groupe:

PREUVE. Si $G.x = G.x'$ alors evidemment $G.x \cap G.x' = G.x \neq \emptyset$. Reciproquement supposons que $G.x \cap G.x' \neq \emptyset$ et soit $y$ dans l'intersection:

$$y = g.x = g'.x' \Rightarrow g^{-1}.y = g^{-1}(g.x) = g^{-1}(g'.x') \Rightarrow x = (g^{-1}.g').x' \in G.x'$$

de sorte que

$$G.x \subset G.(G.x') = (G.G).x' = G.x'$$

et de meme $G.x' \subset G.x$.

Tout element de $x$ est contenu dans une orbite (la sienne, $G.x$ car $e_G.x = x$ ! ) de sorte que

$$X = \bigcup_{\mathcal{O} \in G\backslash X} \mathcal{O}$$

mais les orbites distinctes sont disjointes donc cette reunion est une partition. □

COROLLAIRE 7.1 (Formule des classes). *Si $X$ est un ensemble fini*

$$|X| = \sum_{\mathcal{O} \in G\backslash X} |\mathcal{O}|.$$

**4.1. Exemple: le Theoreme de Lagrange.** Le theoreme de Lagrange est un application de la notion d'action de groupe pour l'action d'un groupe sur lui meme par translations a gauche ou a droite.

Soit $H \subset G$ un sous-groupe de $(G, .)$, alors $H$ agit sur $G$ par translations à gauche (resp. à droite):

$$h \in H \mapsto \mathrm{a}_l(h) : g \mapsto h.g \text{ (resp. } \mathrm{a}_r(h) : g \mapsto g.h).$$

DÉFINITION 7.2. *L'espace des orbites de $G$ sous l'action de $H$ par translations a gauche (resp. a droite) est noté $H\backslash G$ (resp. $G/H$) et est appelle quotient a gauche (resp. a droite) de $G$ par la sous-groupe $H$.*

*– Une orbite pour l'action a gauche $H.g$ s'appelle egalement une classe a gauche (de $g$).*

*– Une orbite pour l'action a droite $g.H$ s'appelle egalement classe a droite (de $g$).*

*Le cardinal $|H\backslash G|$ s'appelle l'indice de $H$ dans $G$ et se note $[G : H]$.*

THÉORÈME 7.3 (Theoreme de Lagrange). *Supposons que $H$ soit fini, alors toutes les orbites de $H\backslash G$ (ou des $G/H$) ont meme cardinal egal a $|H|$. Si de plus $G$ est fini alors on a*

$$|G| = |H||H\backslash G| = |H||G/H|.$$

*En particulier l'ordre de $H$ divise l'ordre de $G$ et*

$$|G/H| = |H\backslash G| = |G|/|H|.$$

PREUVE. Supposons $H$ fini. Soit $\mathcal{O} = H.g$ une orbite. Comme L'application de translation a a droite par $g$

$$g' \in G \mapsto g'.g \in G$$

est injective et que l'image de $H$ par cette application est $H.g$, on a $|H.g| = |H|$ et donc toutes les orbites sont de la meme taille.

Par la formule des classes on a alors

$$|G| = \sum_{\mathcal{O} \in H\backslash G} |\mathcal{O}| = \sum_{\mathcal{O} \in H\backslash G} |H| = |H\backslash G|.|H|$$

(cette formule est valable pour $|G|$ fini ou infini). □

**4.2. Domaine fondamental.** Pour comprendre la structure d'un espace des orbites, il est souvent utile d'avoir recourt a un sous-ensemble de $X$ en bijection avec $G\backslash X$

DÉFINITION 7.10. *Soit $G \curvearrowright X$ un $G$-ensemble; un domaine fondamental pour l'action de $G$ est un sous-ensemble*

$$\mathcal{D}_G \subset X$$

*tel que l'application*

$$x \in \mathcal{D}_G \mapsto G.x \in G\backslash X$$

*est bijective: pour tout $\mathcal{O}$ il existe un unique $x \in \mathcal{D}_G$ tel que $\mathcal{O} = G.x$.*

*Un domaine fondamental s'appelle egalement "systeme de representants des differentes orbites".*

REMARQUE 4.1. Un domaine fondamental n'est pas uniquement definit.

EXEMPLE 4.3. Toute demi-droite d'extremite $(0,0)$, par exemple $\mathbb{R}_{\geqslant 0}(1,0)$, est domaine fondamental de $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}} \curvearrowright \mathbb{R}^2$.

EXEMPLE 4.4. toute droite non-parallele au vacteur $(2,1)$ est un domaine fondamental pour $\mathbb{R}(2,1) \curvearrowright \mathbb{R}^2$.

EXERCICE 7.6. Soit $\mathbb{Z}$ agissant sur $\mathbb{R}$ par translations: montrer que $[0,1[$ et un domaine fondamental.

EXERCICE 7.7. Soit $\mathbb{Z}^2$ agissant sur $\mathbb{R}^2$ par translations: montrer que $[0,1[^2$ et un domaine fondamental.

EXERCICE 7.8. Soit $q \geqslant 1$ et le sous-groupe $q\mathbb{Z}$ agissant sur $\mathbb{Z}$ par translations: montrer que $\{0, 1, \cdots, q-1\}$ et un domaine fondamental.

## 5. Espace quotient et quotient de groupes

On va maintenant donner un résultat important concernant la structure des orbites d'une action de groupe:

THÉORÈME 7.4 (Theoreme Orbite/stabilisateur). *Soit $X$ un $G$ ensemble et $x \in X$ un element. On note son orbite $\mathcal{O} = G.x \in G\backslash X$ et on note $G_x$ le stabilisateur de $x$ dans $G$.*

*L'application*

$$g.G_x \in G/G_x \mapsto g.x \in \mathcal{O} \tag{5.1}$$

*définit une bijection entre l'ensemble (des $G_x$-orbites de $G$ pour la multiplication à droite)*

$$G/G_x = \{g.G_x,\ g \in G\}$$

*et la $G$-orbite*

$$\mathcal{O} = G.x.$$

*De plus si $x' \in \mathcal{O}$ est dans l'orbite de $x$ alors son stabilisateur $G_{x'}$ est conjugué à celui de $x$ et lui est donc isomorphe; ainsi $G_x$ et $G_{x'}$ ont le meme même cardinal.*

*En particulier si $X$ et $G$ sont finis on a*

$$|G.x| = |G/G_x| = |G|/|G_x|.$$

PREUVE. Notons qu'une orbite $g.G_x$ peut-etre representee de multiples manieres: si $g'$ appartiennent a $g.G_x$, on a

$$g.G_x = g'.G_x;$$

hors, l'application 5.1 semble dependre du choix de $g$: montrons que ce n'est pas le cas. soit $g' \in g.G_x$, on a par definition $g' = g.g_x$ avec $g_x \in G_x$ et donc

$$g'.x = (g.g_x).x = g.(g_x.x) = g.x.$$

cette application est surjective: prenons $x' \in \mathcal{O} = G.x$ alors $x' = g.x$ et est l'image par 5.1 de l'orbite a droite $g.G_x$.

Montrons qu'elle est injective: supposons que

$$g.x = g'.x$$

on a

$$x = g^{-1}.g'.x \text{ et donc } g^{-1}.g' \in G_x \text{ et donc } g' \in g.G_x.$$

En d'autre termes $g'.G_x = g.G_x$.

Soit $x' \in \mathcal{O}$, on a $x' = g.x$: soit $g' \in G_{x'}$, on a

$$g'.x' = x' \Leftrightarrow g'.g.x = g.x \Leftrightarrow g^{-1}.g'.g.x = x \Leftrightarrow g^{-1}.g'.g \in G_x.$$

Ainsi

$$G_{x'} = g.G_x.g^{-1}.$$

□

**5.1. Transitivite d'une action.** soit $G \curvearrowright X$, on discute des deux cas extremes possibles pour une orbite $G.x$:

$$G.x = \{x\}, \quad G.x = X.$$

dans

DÉFINITION 7.11. *Soit $G \curvearrowright X$ un $G$-ensemble. Un element $x \in X$ est un point fixe sous l'action de $G$ si l'orbite de $x$ est reduite a $\{x\}$:*

$$G.x = \{x\}.$$

DÉFINITION 7.12. *Si $G \curvearrowright X$ n'a qu'une seule orbite (il existe $x \in G$ tel que $X = G.x$ et donc pour tout $x'$, $X = G.x'$) on dit que $G$ agit transitivement sur $X$. On dit que $X$ est un espace homogene sous l'action de $G$.*

EXEMPLE 5.1. Soit $X$ un $G$ ensemble et $x \in X$ alors $G$ agit transitivement sur la $G$-orbite $G.x$:

$$g.(g'.x) = (g.g').x \in G.x.$$

Si $G$ agit transtivement sur $X$, on a (par le Theoreme Orbite/Stabilisateur) pour tout $x \in X$

$$X = G.x \simeq G/G_x$$

et tous les stabilisateurs $G_x,\ x \in X$ sont conjugues.

**5.2. 2-transitivité.** Un renforcement de la notion de transitivite est la notion de 2-transitivite: si $G$ agit sur $X$ alors $G$ agit sur le produit $X^2 = X \times X$ par

$$\begin{array}{ccc} G \times X^2 & \mapsto & x^2 \\ (g,(x,x')) & \mapsto & (g.x, g.x')^{\cdot} \end{array}$$

La diagonale de $X \times X$ est definie comme le sous-ensemble

$$\Delta_X = \{(x,x),\ x \in X\} \subset X \times X.$$

est est stable sous cette action

$$g.(x,x) = (g.x, g.x) \in \Delta_X.$$

En fait $X$ et $\Delta_X$ sont en bijection ($\delta : x \mapsto (x,x)$) et cette bijection est compatible avec l'action de $G$:

$$g.\delta(x) = g.(x,x) = (g.x, g.x) = \delta(g.x).$$

Ainsi comme $G$ laisse stable $\Delta_X$, il laisse stable le complement de la diagonale

$$X \times X - \Delta_X = \{(x,x'),\ x,x' \in X,\ x \neq x'\}.$$

En effet si $x \neq x'$ alors $g.x \neq g.x'$ (puisque l'action par $g$ est une bijection donc injective)

Définition 7.13. *On dit que l'action de $G$ sur $X$ est 2-transitive si l'action induite de $G$ sur $X \times X - \Delta_X$ est transitive. Autrement dit si*

$$\forall x,x',y,y' \in X,\ x \neq x',\ y \neq y',\ \textit{il existe } g \in G \textit{ tel que } g.x = y,\ g.x' = y'.$$

En fait la notion de 2-transitivité est plus forte que la transitivité

Proposition 7.2. *Si $G$ agit 2-transitivement sur $X$ alors $G$ agit transitivement sur $X$.*

Preuve. Si $X$ ne contient qu'un seul element ($X \times X - \Delta_X = \emptyset$) il n'y a rien a dire l'action est transitive. Soit $x,x' \in X$, si $x = x'$ alors $e_G.x = x$. Supposons donc que $x \neq x'$ alors $(x,x')$ et $(x',x)$ appartiennent a $X \times X - \Delta_X$ et par 2-transitivité il existe $g \in G$ tel que

$$g(x,x') = (g.x, g.x') = (x',x)$$

et en particulier $g.x = x'$. □

Remarque 5.1. Ainsi si un groupe $G$ agit 2-transitivement sur $X$ son action induite sur $X \times X$ possède 2 orbites

$$\Delta_X \text{ et } X \times X - \Delta_X.$$

Remarque 5.2. La notion de 2-transitivité est beaucoup plus forte que la simple transitivité: comme on l'a vu dans la preuve elle montre que si $x,x'$ sont distincts il existe $g \in G$ qui "echange" $x$ et $x'$:

$$g.x = x',\ g.x' = x.$$

On pourrait de même définir la 3, 4, et $n$-transitivité...

Exemple 5.2. Le groupe $\mathrm{Isom}(\mathbb{R}^2)$ agit transitivement sur $\mathbb{R}^2$ mais pas 2-transitivement: en effet deux points distincts sont envoyes par toute isometrie sur deux points distincts mais les images doient etre a meme distance que la distance entre les deux points originaux. En fait c'est la seule obstruction:

EXERCICE 7.9. Montrer que le groupe $\mathrm{Isom}(\mathbb{R}^2)$ agit transitivement sur l'ensemble des paires de points de $\mathbb{R}^2$ a distance 1 l'un de l'autre.

$$(P,Q) \in \mathbb{R}^2,\ d(P,Q) = 1.$$

Est ce que le sous-groupe $\mathrm{Isom}(\mathbb{R}^2)^+$ agit 2-transitivement ?

## 6. La formule des points fixes (de Burnside)

THÉORÈME 7.5 (Formule de Burnside). *Soit $G$ un groupe fini et $G \curvearrowright X$ un $G$-ensemble fini. Soit*

$$X^g = \{x \in X,\ g.x = x\}$$

*l'ensemble des points fixes de $G$, on a*

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G} |X^g| :$$

*le nombre d'orbites de $G$ dans $X$ est la valeur moyenne du nombre de points fixes des element de $G$.*

PREUVE. Soit

$$S = \{(g,x) \in G \times X,\ g.x = x\}.$$

On a

$$|S| = \sum_{g\in G} |X^g| = \sum_{x\in X} |G_x| = \sum_{\mathcal{O}} \sum_{x\in\mathcal{O}} |G_x|$$

car les orbites forment une partition de $X$. On a vu dans le theoreme 7.4 que etant donne une orbite $\mathcal{O}$, l'application $x \in \mathcal{O} \mapsto |G_x|$ est constante egale a

$$|G_x| = |G|/|\mathcal{O}|$$

et donc

$$\sum_{x\in\mathcal{O}} |G_x| = \sum_{x\in\mathcal{O}} |G|/|\mathcal{O}| = |G||\mathcal{O}|/|\mathcal{O}| = |G|.$$

Ainsi

$$\sum_{\mathcal{O}} \sum_{x\in\mathcal{O}} |G_x| = |G| \sum_{\mathcal{O}} 1 = |G||G\backslash X|$$

et donc

$$\frac{1}{|G|}\sum_{g\in G} |X^g| = |G\backslash X|.$$

□

REMARQUE 6.1. Cette formule (ou encore Lemme de Burnside) n'est pas vraiment due a Burnside; c'est une manifestation du phenomene qui veut que l'on ne prete qu'aux riche. Cette formule est mentionnee dans son livre (un grand classique) de 1897 sur la theorie des groupes finis il l'attribue a Frobenius (1887) mais elle etait deja connue (sous une forme plus obscure) de Cauchy au moins des 1845. On l'appelle egalement le *"Lemme qui n'est pas de Burnside !"*

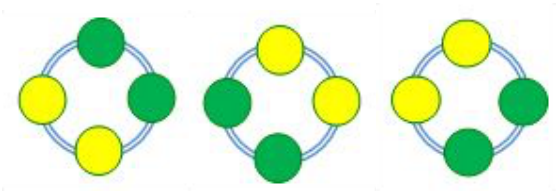

FIGURE 3. Un modele de collier a deux perles vertes et deux perles jaunes

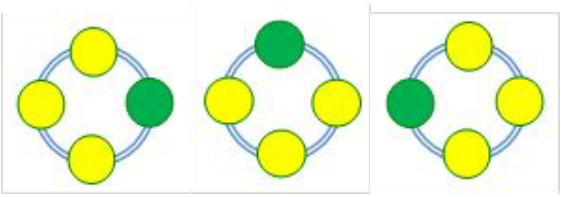

FIGURE 4. Un modele de collier a une perle verte et trois perles jaunes

**6.1. Application au secteur de la haute joaillerie.** Nous utiliserons cette formule pour classifier sous-groupes finis de $\mathrm{Isom}(\mathbb{R}^3)$ ainsi que les solides platoniciens.

Nous allons voir maintenant comment cette formule permet de resoudre des problemes de combinatoire, notamment le comptage de colliers: nous sommes dans une usine fabriquant des colliers de perles colorees; pour des questions de marketing on veut savoir combien de modeles de colliers differents on peut presenter.

Supposons qu'on veuille fabriquer des colliers de 4 perles de couleurs jaunes et vertes. Pour cela on considere les quatre sommes d'un carre (qu'on appelle par exemple $1, i, -1, -i$) que l'on va colorer soit en vert soit en jaune.

Dans le processus, il est clair qu'on obtiendra des modeles de colliers identiques meme si les sommets colories sont differents: par exemple dans les deux figures ci-dessous (colliers avec 2 perles vertes et 2 jaunes ou bien 1 perle verte et 3 jaunes) les trois coloriages fournissent le meme modele de collier.

Pour formaliser cela on defini un coloriage (des sommets d'un carre par les deux couleurs jaune et vert) comme etant une fonction

$$c : \{1, i, -1, -i\} \mapsto \{J, V\}$$

qui assigne au sommet $s \in \{1, i, -1, -i\}$ la couleur $c(s) \in \{J, V\}$.

On note $\mathcal{F}(\{1, i, -1, -i\}, \{J, V\})$ l'ensemble de toutes ces fonctions. C'est un ensemble fini de cardinal

$$|\mathcal{F}(\{1, i, -1, -i\}, \{J, V\})| = |\{J, V\}|^{|\{1,i,-1,-i\}|} = 2^4.$$

Considerons $\mathrm{Isom}(\mathbb{R}^2)_{C_4}$ le groupe des isometries du carre

$$C_4 = [1, i, -1, -i].$$

Ce groupe agit (a droite) sur l'espace des coloriages par permutation: si $\varphi$ est une telle isometrie elle induit une permutation des sommets du carre et on defini un nouveau coloriage en posant pour $x \in \{1, i, -1, -i\}$

$$c_{|\sigma}(s) = c(\sigma(s)).$$

Comme on permute les sommets du carre a l'aide d' isometries preservant les sommets (une rotation qui "fait tourner" le collier autour de l'axe perpendiculaire a son plan ou bien une symetrie axiale qui "retourne" le collier dans l'espace) le nouveau coloriage obtenu correspondra au meme modele de collier.

En d'autre termes *deux coloriages c correspondent au meme collier si ils sont dans la meme orbite sous l'action de* $\mathrm{Isom}(\mathbb{R}^2)_{C_4}$.

Le nombre de colliers possibles (a 4 perles et 2 couleurs)$C(4,2)$ est donc egal au nombres d'orbites de cette action. Pour compter le nombre d'orbites on utilise la formule de Burnside:

$$C(4,2) = \frac{1}{8} \sum_{\varphi \in \mathrm{Isom}(\mathbb{R}^2)_{C_4}} |\mathcal{F}(\{1,i,-1,-i\},\{J,V\})^{\varphi}|.$$

Rappelons que ce groupe est diedral d'ordre 8 compose de 4 rotations (d'ordre $1,2,4$ et 4) et 4 symetries axiales (2 d'axes passant par les diagonales et 2 d'axes passant par les milieux des cotes opposes).

(1) Si $\varphi = \mathrm{Id}$, on a
$$|\mathcal{F}(\{1,i,-1,-i\},\{J,V\})^{\varphi}| = 2^4$$
car tout les coloriages sont fixes par l'identite.

(2) Si $\varphi = r_4$ est une des deux rotations d'ordre 4, on a
$$|\mathcal{F}(\{1,i,-1,-i\},\{J,V\})^{r_4}| = 2$$
car si on choisit une couleur pour le sommet 1 et que le coloriage est fixe, tous les sommet seront de cette couleur.

(3) Si $\varphi = r_2$ est la rotation d'ordre 2, on a
$$|\mathcal{F}(\{1,i,-1,-i\},\{J,V\})^{r_2}| = 2^2$$
car si on choisit une couleur parmi 2 pour le sommet 1 et une pour le sommet $i$ et que le coloriage est fixe par $r_2$, alors $-1$ sera de la couleur de 1 et $-i$ de celle de $i$.

(4) Si $\varphi = \sigma_D$ est une des deux symetries d'axe une des diagonales, on a
$$|\mathcal{F}(\{1,i,-1,-i\},\{J,V\})^{\sigma_D}| = 2^3$$
car on peut choisir un couleur par sommet de la diagonale et une couleur commune pour les deux sommets de part et d'autre de la diagonale.

(5) Si $\varphi = \sigma_M$ est une des deux symetries d'axe passant par les milieux des cotes opposes, on a
$$|\mathcal{F}(\{1,i,-1,-i\},\{J,V\})^{\sigma_M}| = 2^2$$
car on peut choisir pour chaque sommet d'un cote de l'axe une couleur parmi 2 et le sommet symetrique sera de la meme couleur.

On obtient donc

$$C(4,2) = \frac{1}{8}(2^4 + 2\times 2 + 1\times 2^2 + 2\times 2^3 + 2\times 2^2) = \frac{1}{8}(16+4+4+16+8) = 6.$$

Voici les 6 modeles possibles

$$(V,V,V,V),\ (J,J,J,J),\ (V,V,V,J),\ (J,J,J,V),\ (V,V,J,J),(V,J,V,J).$$

Bien sur on aurait pu faire le decompte a la main mais l'avantage de cette methode est qu'elle peut mecaniquement donner une formule pour des configurations plus compliquees

de colliers et de couleurs. Par exemple une formule generale pour

$$C(4, c)$$

pour tout entier $c \geqslant 1$.

EXERCICE 7.10. Calculer $C(5, 12)$ ou $C(6, 5)$ de la meme maniere.

Nous verrons en exercice d'autres exemples similaires ainsi que des applications (plus scientifiques) pour calculer le nombre de molecules isomeres (chirales ou pas) d'une molecule donnee.

## 7. Groupe quotient

Soit $G$ un groupe et $H \subset G$ un sous-groupe. Sous certaines conditions sur $H$ on peut donner a l'espace des orbites (a droite pour fixer les idees) $G/H$ une structure de groupe compatible avec celle de $G$: ie. de sorte que la surjection naturelle

$$\mathrm{red}_H : \begin{array}{ccc} G & \mapsto & G/H \\ g & \mapsto & g.H = g \,(\mathrm{mod}\, H) \end{array}$$

qui a un element $G$ associe son orbite soit un morphisme de groupe. Si c'est le cas l'element neutre de $G/H$ pour cette loi devrait etre

$$\mathrm{red}_H(e_G) = H.$$

Definissons maintenant un candidat naturel pour cette loi. L'ensemble

$$G/H = \{g.H,\ g \in G\}$$

est un sous-ensemble de l'ensemble des parties de $G$, $\mathcal{P}(G)$ et ce dernier ensemble admet une loi de composition naturelle donnee par la multiplication dans le groupe: a deux sous-ensembles $A, B \subset G$, on associe le produit $A.B$ forme de l'ensemble de tous les produits d'elements de $A$ et d'elements de $B$,

$$A.B := \{a.b,\ a \in A,\ b \in B\} \subset \mathcal{P}(G).$$

Un "inverse" naturel serait donne par

$$A^{-1} = \{a^{-1},\ a \in A\}.$$

Cette loi est associative

$$(A.B).C = A.(B.C).$$

Notons que l'ensemble

$$A.A^{-1} = \{a.a'^{-1},\ a, a' \in A\}$$

peu varier avec l'ensemble $A$ et donc on ne peut esperer disposer d'un element neutre (voir le Lemme ci-dessous) Ainsi cette "loi" n'a pas beaucoup de chance d'etre une loi de groupes de l'ensemble complet $\mathcal{P}(G)$.

Considerons cette loi mais restreinte au sous-ensemble $G/H$: on

LEMME 7.1. *Soit $H \subset G$ un sous-groupe alors*

$$H^{-1} = H,\ H.H = H.$$

**Preuve**: La premiere egalite est evidente car un groupe est invariant par inversion. Pour la second egalite on a

$$\forall h, h' \in H,\ h.h' \in H$$

donc

$$H.H \subset H$$

et

$$H = \{e_G\}.H \subset H.H.$$

□

Ainsi pour $H$ un sous-groupe, $H = e_G.H \in G/H$ a une bonne chance d'etre l'element neutre du quotient $G/H$ pour cette loi de composition.

Pour l'inversion on a pour tout $g \in G$

$$(g.H)^{-1} = H^{-1}.g^{-1} = H.g^{-1}.$$

Pour avoir une loi de groupe, il est necessaire que cet ensemble $H.g^{-1}$ soit de la forme $g'.H$; supposons que ce soit le cas, on doit alors avoir

$$g.H.H.g^{-1} = e_{G/H} = H \Longrightarrow gHg^{-1} = H \Longleftrightarrow H \text{ est distingue}$$

car $H.H = H$. Notons alors que dans ce cas on a

$$H.g^{-1} = g^{-1}.g.H.g^{-1} = g^{-1}.H. \tag{7.1}$$

Ains on a trouve une condition necessaire pour ce le produit d'ensemble soit une loi de groupe sur $G/H$: $H$ est distingue. Le Theoreme suivant dit que cette condition est suffisante.

THÉORÈME 7.6 (Existence du groupe quotient). *Soit $H \lhd G$ un sous-groupe distingue de $G$ alors le quotient $G/H$ munis de la loi de multiplication des ensemble*

$$gH.g'H = \{a.b,\ a \in g.H,\ b \in g'.H\}$$

*a une structure de groupe telle que $\mathrm{red}_H : G \mapsto G/H$ est un morphisme surjectif de groupe et dont le noyau est $H$:*

$$\ker(\mathrm{red}_H) = H.$$

*En particulier l'element neutre de $G/H$ est $H$, l'inverse de $gH$ est $g^{-1}H$ et on a*

$$g.H.g'.H = g.g'.H.$$

*Le groupe $G/H$ ainsi obtenu s'appelle le groupe quotient de $G$ par $H$.*

REMARQUE 7.1. On a vue qu'un noyau $\ker\phi$ d'un morphisme de groupes $\phi : G \to G'$ est un sous-groupe distingue.

Reciproquement tout groupe distingue $H \lhd G$ est le noyau d'un morphisme: c'est le noyau du morphisme $\mathrm{red}_H : G \mapsto G/H$.

**Preuve**: Supposons que $H$ est distingue dans $G$. Nous devons verifier les quatre conditions qui font de $(G/H, .)$ un groupe

(1) On a bien une loi de composition dans $G/H$: si $g, g' \in G$ alors l'ensemble produit $g.H.g'.H$ est de la forme $g''.H$: en effet

$$g.H.g'.H = g.g'.g'^{-1}.H.g'.H = g.g'.H.H = g.g'.H \text{ car } g'^{-1}.H.g' = H,$$

(2) On a vu que cette loi est associative.
(3) $H$ est l'element neutre:

$$\forall g \in G,\ g.H.H = g.H,\ H.g.H = g.g^{-1}.H.g.H = g.H.H = g.H\ (\text{ car } g^{-1}.H.g = H).$$

(4) Existence d'un inverse: pour tout $g \in G$, l'inverse de $g.H$ est donne par (7.1),

$$(g.H)^{-1} = g^{-1}.H$$

qui appartient bien a $G/H$ car on a (a nouveau le calcul precedent)

$$g.H(g.H)^{-1} = g.H.g^{-1}.H = g.g^{-1}.H = H.$$

Le fait que $\mathrm{red}_H$ soit un morphisme de groupe resulte des formules precedentes:

$$\forall g, g' \in G,\ \mathrm{red}_H(g).\mathrm{red}_H(g') = g.H.g'.H = g.g'.H = \mathrm{red}_H(g.g').$$

Cette application est surjective et comme $H$ est un groupe

$$g.H = H \Longleftrightarrow g = g.e_G \in H \text{ et } g.H = H.$$

donc son noyau est $H$.

□

Remarque 7.2. Si $G$ est un groupe abelien tout sous-groupe $H \subset G$ est distingue et le groupe quotient $G/H$ a toujours une structure de groupe donnee par

$$g.H.g'.H = gg'.H.$$

Exemple 7.1. Un exemple important de groupe quotient d'un groupe abelien est le groupe de l'horloge note au depart $\mathbb{Z}/N\mathbb{Z}$ qu'on a definit comme l'ensemble des entiers

$$\{0, 1, \cdots, N-1\}$$

munis de l'addition

$$m \oplus m' = \text{reste de la division euclidienne de } m + m' \text{ par } N.$$

On a la

Proposition 7.3. *L'application*

$$m \in \{0, 1, \cdots, N-1\} \mapsto m + N\mathbb{Z} \in \mathbb{Z}/N\mathbb{Z}$$

*est un isomorphisme entre le groupe de l'horloge et le groupe quotient de $\mathbb{Z}$ par le sous-groupe $N\mathbb{Z}$ justifiant ainsi la notation $\mathbb{Z}/N\mathbb{Z}$ pour le grouep de l'horloge.*

### 7.1. Le Theoreme Noyau-Image.

Théorème 7.7 (Theoreme Noyau-Image). *Soit $\phi : G \mapsto G'$ un morphisme de groupes de noyau $H = \ker(\phi) \subset G$ et d'image $H' = \mathrm{Im}(\phi) \subset G'$. Alors $\phi$ induit un isomorphisme de groupes*

$$\phi_H : G/H \simeq H'$$

*defini par*

$$\phi_H(g.H) = \phi(g).$$

*En particulier si $G'$ est fini, $G/H$ est fini ($H$ est d'indice fini dans $G$) et on a*

$$|G/H| = |H'|.$$

*En particulier si $G$ est fini on a (par le Theoreme de Lagrange)*

$$|G|/|H| = |G/H| = |H'|.$$

PREUVE. Soit $\phi_H$ l'application donnee par la regle

$$\phi_H : \begin{array}{ccc} G/H & \mapsto & H' \\ gH & \mapsto & \phi(g) \end{array}$$

est bien definie: si $gH = g'H$, on a $g' = gh$ pour $h \in H$ et

$$\phi_H(g'H) = \phi(gh) = \phi(g)\phi(h) = \phi(g).$$

Elle est d'image $H'$: pour tout $h \in H'$, alors il existe $g \in G$ tel que $\phi(g) = h$ et donc

$$\phi_H(g.H) = \phi(g) = h.$$

Enfin c'est un morphisme de groupe car

$$\forall g, g' \in G,\ \phi_H(g.H.g'.H) = \phi_H(g.g'.H) = \phi(g).\phi(g') = \phi_H(g.H)\phi_H(g'.H).$$

Montrons que $\phi_H$ est injectif: on a

$$\phi_H(gH) = e_{G'} \Leftrightarrow \phi(g) = e_{G'} \ \Leftrightarrow g \in \ker\phi = H \Leftrightarrow gH = H = e_{G/H}.$$

□

### 7.2. Groupes quotients et morphismes de groupes.

THÉORÈME 7.8. *Soit $G$ une groupe et $H \subset G$ un sous-groupe distingue et $G'$ un autre groupe. Il existe une bijection entre les ensembles suivants*

1. *L'ensemble des morphismes $\phi : G \to G'$ tels que $H \subset \ker(\phi)$.*
2. *L'ensemble des morphismes $\phi_H : G/H \to G'$.*

*Cette bijection est donnee par*

$$\phi_H \mapsto \phi := \phi_H \circ \mathrm{red}_H.$$

*en d'autre termes etant donne $\phi_H \in \mathrm{Hom}_{Gr}(G/H, G')$ on a*

$$\phi(g) = \phi_H(g.H).$$

**Preuve**: Soit $\phi_H \in \mathrm{Hom}_{Gr}(G/H, G')$ et $\phi$ definit par

$$\phi(g) = \phi_H(\mathrm{red}_H(g)) = \phi_H(gH).$$

Comme $\phi$ est le compose de deux morphismes de groupes c'est un morphisme de groupes de plus

$$\forall h \in H,\ \phi(h) = \phi_H(H) = \phi_H(e_{G/H}) = e_{G'}$$

donc

$$H \subset \ker(\phi).$$

On montrera en exercice que cette application est une bijection entre les deux ensembles mentiones. □

## 8. Complement: Produit semi-direct

On a vu que etant donne deux groupes $(H,.)$ et $(K,.)$ on pouvait construire un nouveau groupe, le produit direct $(H\times K,(.,.))$ dont les elements sont les paires $(h,k),\ k\in H, k\in K$ et dont la loi de groupe est

$$(h,k)\times(h',k')=(hh',kk').$$

On va generaliser cet constructions dans le cas ou $K$ agit sur $H$:

THÉORÈME 7.9 (Produit semi-direct externe). *Soit $H$ et $K$ deux groupes tel que $K$ agit (a gauche) sur $H$ par automorphismes de groupes (pour tout $k\in K$, $h\in H\mapsto k\odot h\in H$ est un morphisme de groupes); notons cette action par $k\odot h$. L'ensemble produit $H\times K$ muni de la loi*

$$\star:\ ((h,k),(h',k'))\mapsto(h,k)\star(h',k')=(h.k\odot h',k.k')$$

*est un groupe d'element neutre $(e_H,e_K)$ et dont l'inversion est donnee par*

$$(h,k)^{\star(-1)}=(k^{-1}\odot h^{-1},k^{-1}).$$

*On note ce groupe $H\rtimes_\odot K$ et on l'appelle produit semi-direct externe de $H$ par $K$. Les injections de $H$ et $K$*

$$i:\begin{array}{ccc}H&\hookrightarrow&H\rtimes K\\ h&\mapsto&(h,e_H)\end{array},\quad j:\begin{array}{ccc}K&\hookrightarrow&H\rtimes K\\ k&\mapsto&(e_H,k)\end{array}$$

*sont des morphismes de groupes injectif ce qui permet d'identifier $H$ et $K$ aux sous-groupes images $i(H)$ et $j(K)$. Avec ces identifications le groupe $H$ est distingue dans $H\rtimes K$ et $K$ agit sur $H$ par conjugaison. De plus le quotient $H\rtimes K/H$ est isomorphe a $K$.*

Reciproquement

THÉORÈME 7.10. *Soit $(G,.)$ un groupe; $H,K\subset G$ des sous-groupes avec $H\triangleleft G$ ($H$ est distingue dans $G$). On suppose que*

1. *$H.K=G$,*
2. *$H\cap K=\{e_G\}$.*

*Soit $H\rtimes K$ le produit semi-direct externe obtenu en faisant agir $K$ sur $H$ par conjugaison dans $G$ (on rappelle que $H$ est distingue dans $G$); alors l'application*

$$\begin{array}{ccc}H\rtimes K&\mapsto&G\\ (h,k)&\mapsto&h.k\end{array}$$

*est un isomorphisme de groupes; en particulier tout element $g\in G$ se decompose de maniere unique en un produit $g=h.k$ avec $h\in H$ et $k\in K$.*

REMARQUE 8.1. Le produit direct est un cas particulier du produit semi-direct quand $H$ agit sur $G$ trivialement:

$$\forall h\in H,\ k\in K,\ k\odot h=h.$$

EXEMPLE 8.1 (Le groupe dihedral). Soit $R=\langle r\rangle=r^{\mathbb{Z}}$ un groupe fini cyclique d'ordre $n$ et $S=\{1,s\}$ un groupe d'ordre 2 qui agit sur $R$ par inversion: par

$$r\odot s=r^{-1}.$$

Le groupe

$$R\rtimes S$$

est un *groupe dihedral* $\mathcal{D}_{2n}$.