

# **Géométrie (1er Semestre)**

Philippe Michel December 22, 2016



## 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. Groupe engendre par un ensemble	24
5. Le Theoreme de Lagrange	29
Chapitre 3. Isometries du plan	31
1. Plan vectoriel, affine, longueur et distance euclidienne	31
2. La structure du groupe des isometries	37
3. Classification des isometries lineaires	46
4. Conclusion	58
Chapitre 4. Isometries et nombres complexes	59
1. Construction des nombres complexes	59
2. Interpretation des isometries en termes de nombres complexes	61
Chapitre 5. Groupes finis d'isometries et polygones reguliers	69
1. Groupes dihedraux	69
2. Classification des sous-groupes finis d'isometries	70
Chapitre 6. Polygones reguliers	77
1. Polygones generalises et polygones reguliers	77
2. Existence des polygones (generalises) reguliers	79
3. Polygones constructibles a la regle et au compas	82



## 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 même forme signifie qu'elles sont obtenues l'une par rapport à l'autre par une isométrie: translation, rotation, symétrie axiale ou des compositions de ces dernières.

Le nombre de possibilités est infini; on va se restreindre au cas où 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'isométries du plan (indexé par un ensemble nécessairement infini  $I$ )

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

qui fournissent un ensemble de tuiles isométriques à la première

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

telles que cet ensemble de tuiles recouvre le plan

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

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

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

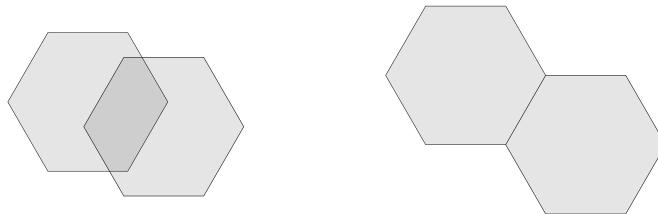


FIGURE 1. Tuiles qui s'intersectent suivant leurs bords ou non

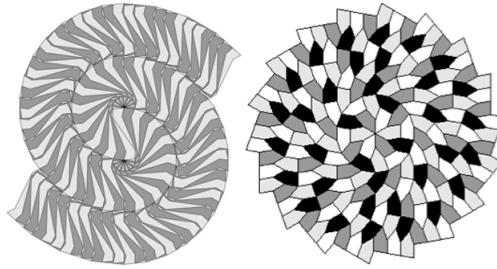


FIGURE 2. Pavages non-reguliers de Voderberg et de Hirschhorn-Hunt  
(source R. Coolman)

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 méthodes 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

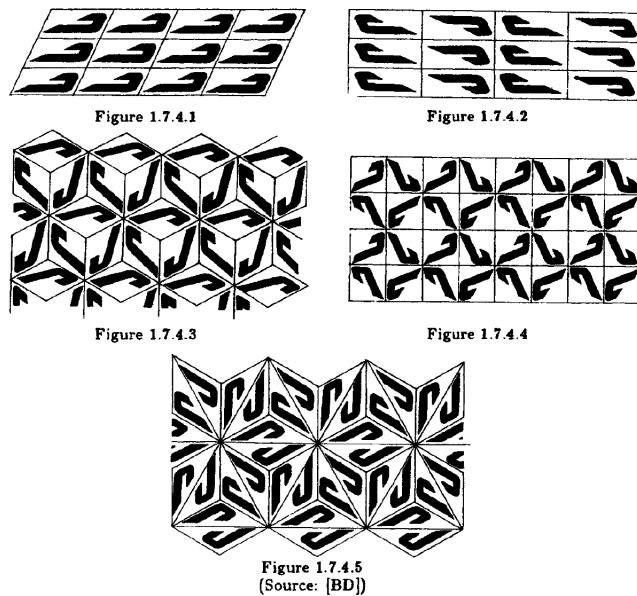


FIGURE 3. Pavages Reguliers sans symetries axiales (source Y. Brossard)

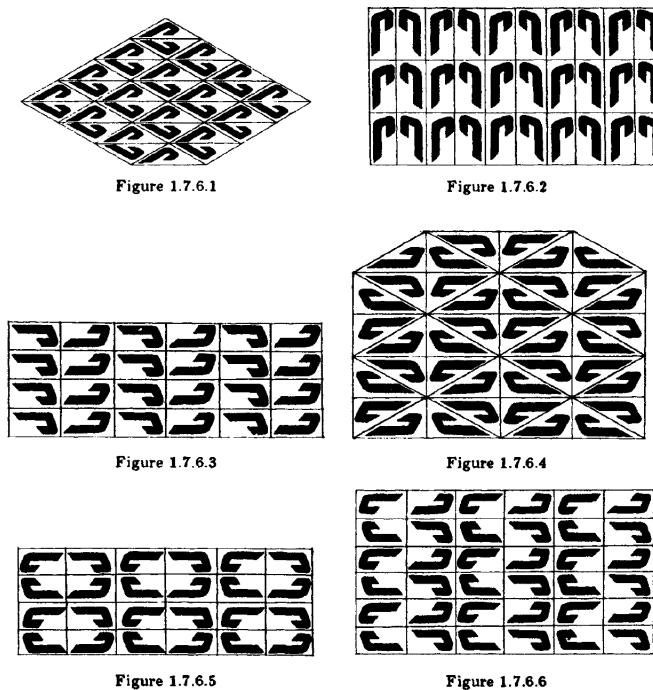


FIGURE 4. Pavages Reguliers avec symetries axiales (source Y. Brossard)

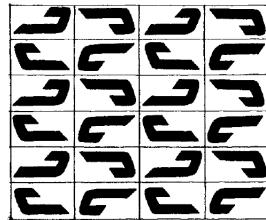


Figure 1.7.6.7

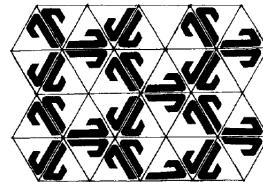


Figure 1.7.6.8

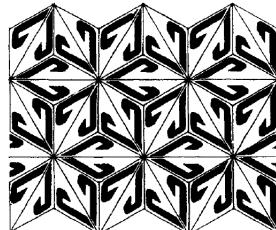


Figure 1.7.6.9

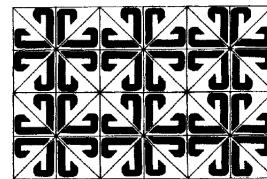


Figure 1.7.6.10

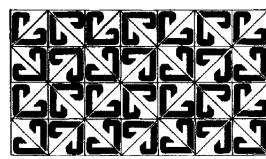


Figure 1.7.6.11

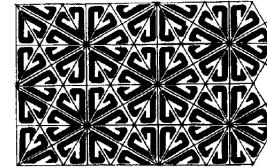


Figure 1.7.6.12

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

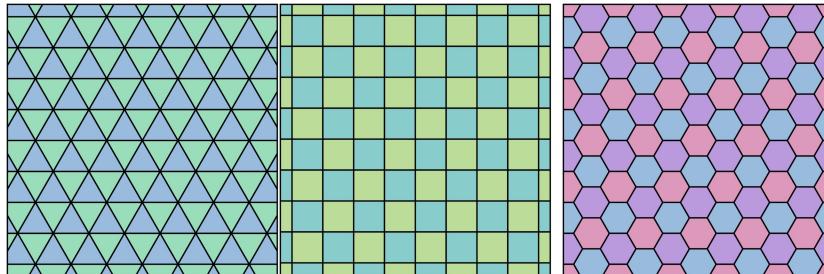


FIGURE 6. Polygones Reguliers paveurs (source wikimedia)

- (1) Si deux isometries laissent un pavage invariant leur composée laisse également le pavage invariant.
- (2) Si une isometrie 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 coordonnees 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:

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

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  $E$ ,  $\text{Id}_E : E \rightarrow E$  est l'application definie par

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

Le graphe de  $\text{Id}_E$  s'appelle 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

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

Question: quels sont les graphes de ces applications ?

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

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

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

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

Reciproquement a une application  $\phi$  on associe

$$\vec{f}_\phi = (\phi(e_1), \dots, \phi(e_n))$$

En particulier si  $E$  et  $F$  sont finis

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

### 1.1. Composition d'applications.

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

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

La composition defini donc une application du produit  $F^E \times G^F$  vers l'ensemble d'applications  $G^E$  notee  $\circ$

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

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

DÉFINITION 2.4 (Image/Pre-image d'un sous-ensemble). Soit  $\phi : E \rightarrow F$  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  $\phi : E \rightarrow F$  est

- Injective: si pour tout  $f \in F$ , l'ensemble  $\phi^{-1}(\{f\})$  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  $\phi^{-1} : F \rightarrow E$  comme etant l'application qui a  $f \in F$  associe l'unique element de l'ensemble  $\phi^{-1}(\{f\}) \subset E$ . L'application  $\phi^{-1} : F \rightarrow E$  est egalement une bijection.
- 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  $\text{Inj}(E, F)$ ,  $\text{Surj}(E, F)$  et  $\text{Bij}(E, F)$  l'ensemble des applications injectives, surjectives et bijectives de  $E$  vers  $F$ :

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

DÉFINITION 2.6. Si  $E = F$ , l'ensemble des bijections de  $E$  vers lui-même,  $\text{Bij}(E, E)$  sera également note

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

et sera appellé l'ensemble des permutations de  $E$  ou l'ensemble des transformations de  $E$  ou encore le groupe symétrique de  $E$ .

### 1.3. Cardinal d'un ensemble.

DÉFINITION 2.7. Soient  $E$  et  $F$  deux ensembles; si il existe un bijection  $\varphi : E \rightarrow F$  entre  $E$  et  $F$  on dit qu'ils ont le même cardinal.

REMARQUE 1.2. Notons que si  $\phi : E \rightarrow F$  est une bijection alors l'application réciproque  $\phi^{-1} : F \rightarrow E$  en est également une, donc la relation "avoir le même cardinal" est une relation symétrique.

DÉFINITION 2.8. Soit  $n \geq 1$  un entier non-nul. Si un ensemble  $E$  a même cardinal que l'ensemble

$$\{1, \dots, n\}$$

on dit que  $E$  est de cardinal  $n$  et on écrit (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  $n \geq 0$ .

EXEMPLE 1.3 (Denombrement). Soient  $E$  et  $F$  des ensembles finis alors  $F^E$  est fini et  $|F^E| = |F|^{|E|}$ . On a également

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

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

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

DÉFINITION 2.9 (Ensembles dénombrables). Un ensemble infini qui a même cardinal que  $\mathbb{N}$  est dit dénombrable.

EXEMPLE 1.4. Les ensembles  $\mathbb{Z}, \mathbb{N}^2, \mathbb{Q}, \mathbb{N}^3, \mathbb{N}^4, \dots$  sont tous dénombrables.

EXEMPLE 1.5 (Cantor). L'intervalle  $[0, 1]$  n'est pas dénombrable. Ce résultat est obtenu par le célèbre argument diagonal de cantor.

**1.4. Critères numériques d'injectivité ou de surjectivité pour les ensembles finis.** Si les ensembles de départ ou d'arrivée sont finis on a les implications suivantes

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

Par contraposée on a

- Si  $|E| > |F|$  alors  $\phi$  n'est pas injective (il existe deux éléments  $e, e' \in E$  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 également les critères suivants qui sont utiles:

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

**1.5. Morphismes de structures.** Dans la suite on va rencontrer des ensemble munis d'une structure additionnelle  $Str$  (par exemple les espaces vectoriels, les groupes ou les  $G$ -ensembles). Ces ensembles munis d'une telle structure additionnelles sont regroupes dans une *catégorie*: la catégorie  $\mathcal{EV}_{\mathbb{R}}$  des espaces vectoriels sur  $\mathbb{R}$ , la catégorie  $\mathcal{G}$  des groupes, etc...

Etant donnees  $E, F$  des ensembles appartenant a une telle catégorie, c'est a dire possedant une structure  $Str$  supplementaire donnee, on dira qu'une application  $\phi : E \rightarrow F$  compatible avec  $Str$  est *morphism*e ou *homomorphisme* (de la catégorie concerne).

- Si le morphisme a pour ensemble d'arrivee  $E$ , on parlera d'*endomorphisme*.
- Si le morphisme est bijectif on parlera d'*isomorphisme* ou d'homeomorphismes (de structure),
- pour un endomorphisme bijectif

et on parlera d'*automorphisme* (de structure) si la bijection va d'un ensemble sur lui-même.

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

Si la structure est evidente (d'apres le contexte) on pourra omettre de la mentionner.

**EXEMPLE 1.6.** Dans la catégorie des  $\mathbb{R}$ -espaces vectoriels les morphismes sont les applications  $\mathbb{R}$ -lineaires.

## 2. Groupes

**DÉFINITION 2.10.** Un groupe  $(G, \star, \cdot^{-1}, e_G)$  est un ensemble  $G$  muni

- 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 2.1.** 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

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

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

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

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

**DÉFINITION 2.11** (Groupe commutatif). *Un groupe  $(G, \star)$  est dit commutatif ou abélien si de plus la loi de composition  $\star$  vérifie:*

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

**DÉFINITION 2.12** (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 élément neutre sont des groupes et même des groupes abéliens. En revanche  $\mathbb{N}$  n'est pas un groupe car il manque l'inversion.

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

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

munis de la multiplication  $\times$ , de l'inversion  $x \mapsto 1/x$  et de 1 comme élément 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  $n \geq 1$ ,  $\mathbb{R}^n$  et  $\mathbb{C}^n$  munis de l'addition des vecteurs, de la multiplication par  $-1$ , et de l'élément neutre  $\vec{0} = (0, \dots, 0)$  sont des groupes.

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

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

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 2.5** (Le groupe des permutations d'un ensemble). Soit  $E$  un ensemble, alors l'ensemble  $(\text{Bij}(E), \circ)$  muni de la composition d'applications,

$$\circ : (\phi, \psi) \mapsto \phi \circ \psi : e \in E \mapsto \phi(\psi(e)) \in E,$$

a une structure de groupe.

L'élément neutre est l'application identité

$$\text{Id}_E : e \in E \mapsto e.$$

L'inverse d'une bijection  $\phi$  est la bijection réciproque  $\phi^{-1}$ .

On l'appelle  $\text{Bij}(E) = \mathfrak{S}_E = S_E$  le groupe des permutations, ou des transformations de  $E$  ou encore le groupe symétrique de  $E$ .

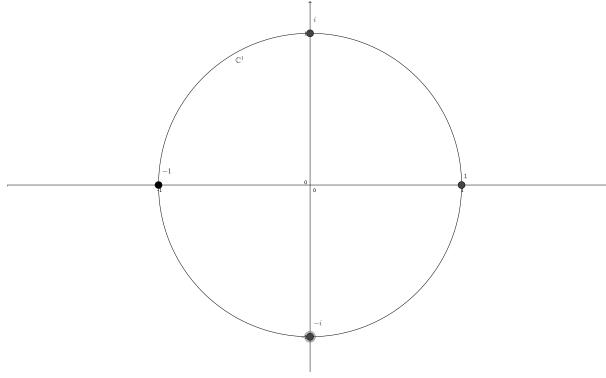


FIGURE 1. Le cercle unite

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

Si  $|E| \leq 3$  ce groupe est commutatif; il ne l'est plus dès que  $n \geq 4$ . Par exemple si  $E = \{1, 2, 3, 4\}$ ,  $\sigma = (1234)$  et  $\tau = (123)$  on a

$$(1234) \circ (123) = (1324), \quad (123) \circ (1234) = (1342) \neq (1324).$$

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

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

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

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

car

- (1) La multiplication des matrices est associative.
- (2)  $\det(M \cdot M') = \det(M) \cdot \det(M')$  est non-nul si (et seulement si)  $\det(M)$  et  $\det(M')$  le sont et  $M \cdot M' \in \mathrm{GL}_2(k)$ .
- (3)  $M \cdot \mathrm{Id} = \mathrm{Id} \cdot M = M$
- (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

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

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

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

Ainsi l'ensemble  $\mathbb{N}_{<12}$  forme un groupe commutatif d'élément neutre 0.

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

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

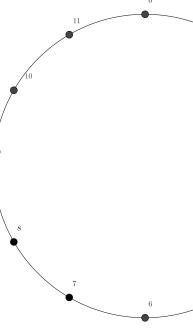


FIGURE 2. Le groupe de l'horloge

Ainsi équipe,  $\mathbb{N}_{< N}$  forme un groupe commutatif d'élément neutre 0; l'inverse de 0 est 0 et de  $n \geq 1$  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 entiers  $< 12$  et premiers à 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'élément neutre 1.

Plus généralement pour  $N \geq 1$ , soit

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

; 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'élément neutre 1. L'existence d'un inverse est une conséquence de l'identité de Bezout pour  $a$  et  $N$  qui sont premiers entre eux.

**EXEMPLE 2.10.** Soit  $N \geq 1$  et

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

l'ensemble des racines  $N$ -ièmes de l'unité muni de la multiplication est un groupe d'élément neutre 1.

**EXEMPLE 2.11.** Notons  $d(PQ) = \sqrt{(x_P - x_Q)^2 + (y_P - y_Q)^2}$  la distance Euclidienne dans le plan  $\mathbb{R}^2$ . On note

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

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

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

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

L'élément neutre est l'élément

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

et l'inversion est donnée par

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

## 2.2. Sous-groupe.

DÉFINITION 2.13. *Un sous-groupe  $H \subset G$  d'un groupe  $(G, *)$  est un sous-ensemble vérifiant*

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

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

EXEMPLE 2.12. – L'élément neutre  $\{e_G\}$  forme un sous-groupe à lui tout seul:

Le sous-groupe trivial.

- L'ensemble  $\text{Isom}(\mathbb{R}^2)$  est un sous-groupe de  $\text{Bij}(\mathbb{R}^2)$ .
- L'ensemble des rotations de centre 0 et d'angle  $2\pi/N$  est un sous-groupe de l'ensemble des isométries du plan.
- L'ensemble  $T(\mathbb{R}^2)$  des translations du plan est un sous-groupe de l'ensemble des isométries  $\text{Isom}(\mathbb{R}^2)$ .
- L'ensemble  $\{0, 2, 4\}$  est un sous-groupe de  $\mathbb{Z}/6\mathbb{Z}$ .
- L'ensemble  $\{\text{Id}_{\{1,2,3\}}, (123), (132)\}$  est un sous-groupe de  $\mathfrak{S}_3$ .

PROPOSITION 2.1 (Critère de sous-groupe). *Un sous-ensemble non-vide  $H$  d'un groupe  $G$  est un sous-groupe (pour  $\star$  et d'élément neutre  $e_G$ ) ssi*

$$(2.2) \quad \forall h, h' \in H, h * h'^{-1} \in H.$$

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

Réiproquement, étant donné  $H \subset G$  vérifiant (2.2) et  $h, h' \in H$

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

□

EXEMPLE 2.13. Soit  $E$  un ensemble,  $F \subset E$  un sous-ensemble et  $(G, \circ) \subset (\text{Bij}(E), \circ)$  un sous-groupe de  $(\text{Bij}(E), \circ)$  (le groupe des bijections de  $E$  sur lui-même, muni de la composition, de l'identité de  $E$  comme élément neutre et de l'application réciproque pour l'inverse). On considère

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

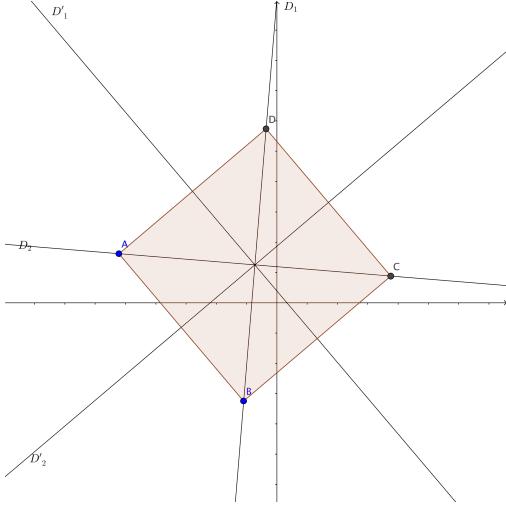


FIGURE 3.

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

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

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  $G = \text{Isom}(\mathbb{R}^2)$  l'ensemble des isometries de  $\mathbb{R}^2$  (vu au gymnasie et qu'on etudiera un peu plus tard).  $\text{Isom}(\mathbb{R}^2)$  est un sous-groupe de  $\text{Bij}(\mathbb{R}^2)$ . Considerons un carre dans  $\mathbb{R}^2$  de centre  $P$  de diagonales sont notes  $D_1, D_2$  et dont les droites joignant les milieux des cotes opposées sont notes  $D'_1, D'_2$  alors

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

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

**EXERCICE 2.3.** Soit  $N \geq 1$  et  $M|N$  alors l'ensemble des multiples de  $M$  dans  $\{0, \dots, N-1\}$  forme un sous-groupe de  $\mathbb{Z}/N\mathbb{Z}$  de cardinal  $N/M$  et reciproquement tout sous-groupe est de cette forme.

**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	$a \oplus b$	(0,0)	(0,1)	(1,0)	(1,1)
1	1	5	7	11	(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
5	5	1	11	7	(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
7	7	11	1	5	(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
11	11	7	5	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 2.14. *Etant donnees 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)  $\phi(g \cdot g') = \phi(g) \star \phi(g')$
- (3)  $\phi(g^{-1}) = \phi(g)^{-1}$

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

DÉFINITION 2.15. *Soit  $G$  et  $H$  deux groupes, on note*

- $\text{Hom}_{Gr}(G, H)$  l'ensemble des morphismes de groupes de  $G$  vers  $H$ .
- $\text{End}_{Gr}(G) = \text{Hom}_{Gr}(G, G)$  l'ensemble des endomorphismes (de  $G$  vers lui-même).
- $\text{Iso}_{Gr}(G, H)$  l'ensemble des morphismes de groupes de  $G$  vers  $H$  qui sont bijectifs et dont l'inverse est également un morphisme de groupe: c'est l'ensembles des isomorphismes de  $G$  vers  $H$ .
- $\text{Aut}_{Gr}(G) = \text{Iso}_{Gr}(G, G)$  l'ensemble des isomorphismes de  $G$  vers  $G$ : les automorphismes de  $G$ .

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

PROPOSITION 2.2 (Critere de morphisme). *Pour verifier qu'une application*

$$\phi : G \rightarrow H$$

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

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

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:

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

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

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

de sorte que

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

□

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

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

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  $t_g(g') = e_g \cdot g' = g'$  et  $t_{e_G} = \text{Id}_G$ . Sinon on a

$$t_g(e_G) \circ g \cdot e_G = g \neq e_G$$

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

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

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

EXERCICE 2.4. Montrer que l'application tramslation a gauche

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

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

**3.2. Exemple: isomorphismes de groupes.** On a defini un isomorphisme de groupes  $\phi : G \rightarrow H$  comme etant une application bijective entre  $G$  et  $H$  qui est morphisme de groupe et dont la reciproque  $\phi^{-1}$  est egalement un morphisme de groupe; la proposition suivante montre que cette derniere condition est en fait automatique:

PROPOSITION 2.3. *Soit  $\phi : G \rightarrow H$  un morphisme de groupe qui en tant qu'application est bijectif alors l'application reciproque  $\phi^{-1} : H \rightarrow G$  est un morphisme de groupes.*

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

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

Pour cela il suffit de montrer que

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

On a

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

et comme  $\phi$  est un morphisme

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

□

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

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

Cette application est un morphisme de groupe: par le critere de morphisme, il suffit de montrer que

$$\forall g', g'' \in G, \text{Ad}_g(g'.g'') = \text{Ad}_g(g').\text{Ad}_g(g'').$$

On a (car  $g^{-1}.g = e_G$ )

$$\text{Ad}_g(g'.g'') = g.g'.g''.g^{-1} = g.g'.g^{-1}.g.g''.g^{-1} = \text{Ad}_g(g').\text{Ad}_g(g'').$$

Par ailleurs  $\text{Ad}_g$  est un isomorphisme de groupes. En effet,  $\text{Ad}_g$  admet  $\text{Ad}_{g^{-1}}$  comme application reciproque qui est egalement un morphisme de groupes:

$$\forall g' \in G, \text{Ad}_{g^{-1}} \circ \text{Ad}_g(g') = g^{-1}.g.g'.g^{-1}.g = e_G.g'.e_G = g'$$

donc

$$\text{Ad}_{g^{-1}} \circ \text{Ad}_g = \text{Id}_G$$

et de meme

$$\text{Ad}_g \circ \text{Ad}_{g^{-1}} = \text{Id}_G.$$

EXERCICE 2.5. Montrer que l'application conjugaison

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

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

### 3.4. Noyau, Image.

DÉFINITION 2.16. Soient  $(G, \cdot)$  et  $(H, \star)$  deux groupes et  $\phi : G \rightarrow H$  un morphisme de groupes,

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

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

- Le noyau de  $\phi$  est la pre-image (l'ensemble des antécédents) de l'élément neutre  $e_H$

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

PROPOSITION 2.4. Soit  $\phi : G \rightarrow H$  un morphisme de groupes,  $\ker(\phi)$  et  $\text{Im}(\phi)$  sont des sous-groupes de  $G$  et  $H$  respectivement.

PREUVE. D'après la Proposition 2.1 il suffit de vérifier que

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

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

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

c'est à 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

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

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

L'importance du noyau tient au fait qu'il permet de résoudre des équations linéaires dans des groupes:

THÉORÈME 2.1. Soit  $\phi : G \rightarrow H$  un morphisme de groupes. Soit  $h \in H$  alors l'ensemble des solutions de l'équation (d'inconnue  $g \in G$ )

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

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

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

Dans le second cas,  $g_0$  désigne n'importe quelle solution de l'équation  $E(\phi, h)$ , i.e.  $\phi(g_0) = h$ .

**Preuve:** Dans le premier cas, si  $h \notin \text{Im}(\phi)$  alors il n'a pas d'antécédent et l'équation  $E(\phi, h)$  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

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

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

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

alors

$$g = k \star g_0, \quad g = g_0 \cdot k'$$

et

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

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 à dire l'image de  $\ker(\phi)$  par l'application  $t_{g_0}$  de translation à gauche par  $g_0$ .  $\square$

**REMARQUE 3.1.** Ce résultat très général recouvre plusieurs cas particuliers rencontrés au gymnase: considérons par exemple le cas où  $G = \mathbb{R}^m$  et  $H = \mathbb{R}^n$  sont les groupes abéliens associés à des espaces vectoriels de dimension finie et  $\phi : \mathbb{R}^m \rightarrow \mathbb{R}^n$  est une application linéaire donnée par une matrice  $\mathbf{a} = (a_{ij})_{i \leq m, j \leq n}$  et  $h = \mathbf{y} = (y_1, \dots, y_n)$ : dans ce cas, notant  $g = \mathbf{x} = (x_1, \dots, x_m)$  l'équation devient  $\phi(x_1, \dots, x_m) = (y_1, \dots, y_n)$  ou encore le système de  $n$  équations linéaires à  $m$  inconnues

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

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

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

ou  $\mathbf{x}_0$  est une solution particulière de  $Eq(\mathbf{a}, \mathbf{y})$  et  $\mathbf{x}$  est une solution quelconque de l'équation linéaire homogène (i.e. sans second membre)

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

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

Un autre cas est celui des équations différentielles linéaires: si on cherche les solutions de l'équation différentielle (d'ordre 1)

$$a \cdot f'(x) + b \cdot f(x) = h(x)$$

ou  $a, b \in \mathbb{R}$ ,  $a \neq 0$ ,  $f : x \mapsto f(x)$  est une fonction de classe  $C^1$  (derivable de dérivée 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  $f(x) = f_0(x) + k(x)$  où  $f_0$  est une solution particulier de cette équation (qu'il faut trouver) et  $k$  est une solution de l'équation sans second membre

$$a \cdot f'(x) + b \cdot f(x) = 0$$

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

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

Le théorème admet les corollaires suivants:

**THÉORÈME 2.2** (Critère d'injectivité de morphismes). *Un morphisme de groupes  $\phi : G \mapsto H$  est injectif si et seulement si*

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

**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

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

mais

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

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

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  $\phi : G \rightarrow H$  un morphisme alors  $\phi(G) = \text{Im}(\phi)$  est un groupe fini et one a*

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

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

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

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

**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,  $\text{Im} \phi = \phi(G)$  est fini. Quand  $h$  varie dans  $\text{Im} \phi$  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  $\text{Im} \phi$ . On note cela

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

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

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

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

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

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

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

$\square$

### 3.4.1. Notion de sous-groupe distingué.

DÉFINITION 2.17. Soit  $G$  une groupe et  $K$  un sous-groupe. On dit que  $K$  est distingué dans  $G$  (ou est normal dans  $G$ ) et on le note

$$K \triangleleft G$$

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

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

En d'autre termes si  $K$  est invariant par conjugaison par n'importe quel élément de  $G$ .

EXEMPLE 3.1. Les sous-groupes  $\{e_G\}$  et  $G$  sont distingués mais ce sont des sous-groupes distingués évidents.

REMARQUE 3.5. Cette notion est importante pour étudier la structure des groupes car elle permet de la décomposer en structure plus simple: si  $K \triangleleft G$  est un sous-groupe distingué, on peut associer à  $G$  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 décomposition au groupes  $K$  et  $G/K$  jusqu'à ce que ce soit impossible: un groupe qui ne possède aucun sous-groupe distingué non-trivial est dit *simple*. Les groupes simples sont en quelque sorte les briques de base des groupes quelconques.

THÉORÈME 2.4. soit  $\phi : G \rightarrow H$  un morphisme de groupes alors  $K = \ker \phi$  est distingué.

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

$$g_0 \cdot \ker \phi = \ker \phi \cdot g_0$$

Multippliant cette égalité à droite par  $g_0^{-1}$  on obtient

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

□

## 4. Groupe engendré 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 propriété, c'est à dire que tout sous-groupe  $H \subset G$  contenant  $A$  contient également ce sous-groupe. On note ce sous-groupe  $\langle A \rangle$  et on l'appelle le sous-groupe engendré par l'ensemble  $A$ .

Si  $\langle A \rangle = G$ , on dit que  $A$  engendre  $G$  ou que  $A$  est un ensemble de générateur 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 le plus 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)  $g \cdot g'^{-1} \in H$  donc  $g \cdot g'^{-1} \in \langle A \rangle$ . □

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

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

$$g^0 := e_G$$

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

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

et on pose

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

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

$$(4.1) \quad g^{-n} = (g^n)^{-1}, \quad g^m \star g^n = g^{m+n}.$$

Un élément de la forme  $g^n$  sera appellé 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'identité (4.1) montrer que

**PROPOSITION 2.5.** *L'application (exponentielle de base  $g$ ) définie par*

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

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

**PROPOSITION 2.6.** *On a l'égalité*

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

*le groupe  $g^{\mathbb{Z}}$  est le sous-groupe engendré 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  $g^{\mathbb{Z}}$ .  $\square$

**4.2. Groupe engendré par un ensemble, bis.** La proposition précédente se généralise comme suit:

**THÉORÈME 2.5.** *Soit  $(G, \star)$  un groupe et  $A \subset G$  un sous-ensemble de  $G$ . Le sous-groupe engendré par  $A$  est l'ensemble des éléments de  $G$  de la forme*

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

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

On laisse la preuve de ce théorème en exercice.

**EXEMPLE 4.1.**  $\mathbb{Z}$  et  $\mathbb{Z}/N\mathbb{Z}$  sont engendrés par 1.

**EXEMPLE 4.2.** Considerons le groupe symétrique à  $n$  éléments

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

Pour  $a, b \in \{1, 2, \dots, n\}$  on note  $(a, b)$  la permutation qui envoie  $a$  sur  $b$ ,  $b$  sur  $a$  et qui laisse fixe tous les autres éléments de  $\{1, 2, \dots, n\}$ : si  $a = b$ ,  $(a, a)$  est l'identité 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

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

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

**EXEMPLE 4.3.** 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 4.4.** 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 gymnasie mais on va le redemontrer en cours.

**4.3. 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  $n \geq 1$  un entier,

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

et on pose

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

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  $g$ .

#### 4.4. Ordre d'un element.

**DÉFINITION 2.18.** 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  $\langle g \rangle$

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

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

**PROPOSITION 2.7.** Si  $\text{ord}(g) < \infty$  est d'ordre fini  $\text{ord}(g)$  est le plus petit entier  $n > 0$  solution de l'équation

$$g^n = e_G$$

et tout entier (relatif) solution de cette équation est un multiple de  $\text{ord}(g)$ .

Pour la preuve rappelons le resultat suivant vu en exercice:

LEMME 2.1. *Tout sous-groupe  $H$  de  $\mathbb{Z}$  est de la forme  $H = N\mathbb{Z}$  pour  $N > 0$ . En particulier, si  $H \neq \{0\}$ ,  $N$  est le plus petit entier positif contenu dans  $H$ .*

PREUVE. Soit  $H \subset \mathbb{Z}$  un sous-groupe et que  $H \neq \{0\}$ , il existe un  $N > 0$  contenu dans  $\mathbb{Z}$  et minimal pour cette propriété (il existe  $N \neq 0$  et quitte à remplacer  $N$  par  $-N$  on peut supposer  $N > 0$ ). Comme  $N \in H$  tous ses multiples  $m.N$ ,  $m \in \mathbb{Z}$  sont dans  $H$  ( $m.N$  est la somme  $|m|$  fois de  $N$  ou  $-N$ ), on a donc  $N\mathbb{Z} \subset H$ . Montrons l'inclusion inverse.

Soit  $M \in H$ , considérons la division euclidienne de  $M$  par  $N$ , on a

$$M = Q.N + R$$

avec  $Q \in \mathbb{Z}$  et  $0 \leq R \leq N - 1$  et  $R = M - Q.N \in H$  mais comme  $0 \leq R < N$  la minimale de  $N$  est contredite sauf si  $R = 0$  et  $M$  est un multiple de  $N$ .  $\square$

PREUVE. L'ensemble des entiers  $n$  solutions de l'équation précédente est précisément le noyau  $\ker \exp_g$ , c'est donc un sous-groupe de  $\mathbb{Z}$  et on a vu que tout sous-groupe  $H$  de  $\mathbb{Z}$  est de la forme  $N\mathbb{Z}$  pour  $N \geq 0$ . Si  $N = 0$  alors  $\exp_g$  est injective et  $\mathbb{Z} \simeq \text{Im } \exp_g = g^{\mathbb{Z}}$ . Si  $N > 0$  alors  $N$  est par définition la plus petite solution non-nulle de l'équation

$$g^n = e_G.$$

$\square$

#### 4.5. Groupes cycliques.

DÉFINITION 2.19. *Un groupe  $G$  engendre par un seul élément  $g \in G$ , autrement dit,*

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

*est dit cyclique.*

PROPOSITION 2.8. *Soit  $G$  un groupe cyclique alors ou bien  $G$  est infini et il est isomorphe à  $\mathbb{Z}$ , ou bien  $G$  est fini et il est isomorphe à  $\mathbb{Z}/N\mathbb{Z}$  où  $N = |G| = \text{ord}(g)$ .*

PREUVE. Considérons le morphisme

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

comme on l'a vu,  $\ker \exp_g = N\mathbb{Z}$  pour  $N \geq 0$ .

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

Si  $N > 0$  alors  $N = \text{ord}(g) = |G|$  est la plus petite solution strictement positive de l'équation

$$g^n = e_G.$$

Considérons l'application

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

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

$$g^r \cdot g^{r'} = g^{r+r'} = g^{kN+r''} = g^{kN} \cdot g^{r''} = g^{r''}$$

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'équation  $g^n = e_G$ , on a  $g^r \neq e_G$  si  $0 < r < N$  et

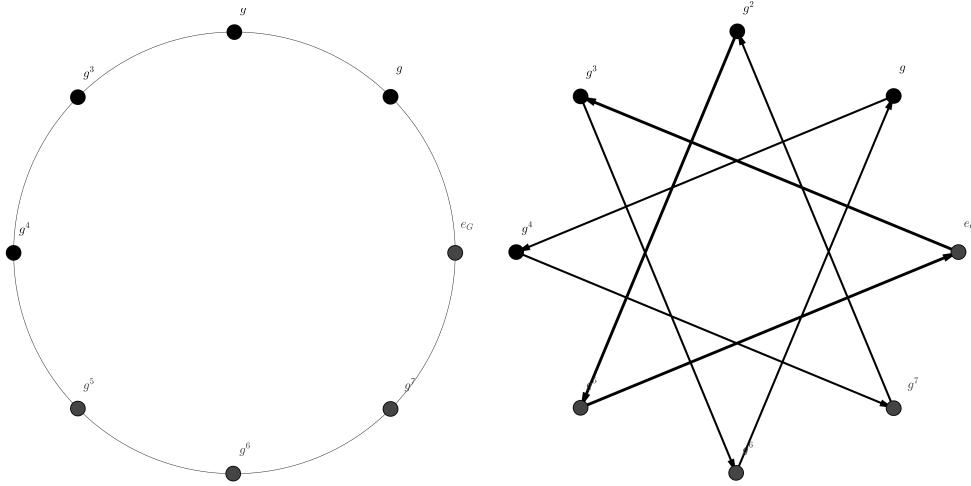


FIGURE 6. Le groupe cyclique  $\langle g \rangle$  a 8 éléments avec  $g$  et avec  $g^3$  comme générateurs

$\ker \exp_{g,N} = \{0\}$ . Le morphisme est injectif et surjectif car les deux groupes ont le même nombre d'éléments et c'est donc un isomorphisme.  $\square$

**PROPOSITION 2.9.** *Tout sous-groupe d'un groupe cyclique est cyclique.*

**Preuve:** Exercice  $\square$

**THÉORÈME 2.6.** *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  $(n,N) = 1$ ,  $g^n$  engendre  $G$  et les générateurs de  $G$  sont les  $g^n$*

$$0 \leq n < N, (n,N) = 1.$$

**Preuve:** Exercice  $\square$

**COROLLAIRE 2.1.** *Soit  $G$  cyclique d'ordre  $N$ . L'application*

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

*est une bijection entre les diviseurs de  $N$  et les sous-groupes de  $G$ . Le sous-groupe correspondant à  $d|N$  est d'ordre  $N/d$ .*

*En particulier, deux éléments de même ordre engendrent le même sous-groupe.*

**Preuve:** Exercice  $\square$

La figure 4.5 représente un groupe cyclique  $G = \langle g \rangle$  à 8 éléments engendré par un élément  $g$  sous la forme de la suite

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

et le même groupe quand on utilise l'élément  $g^3$  comme générateur

$$\{e_G, g^3, g^9 = g, g^4, g^7, g^{10} = g^2, g^5, g^8 = e_g\}.$$

## 5. 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 2.7** (Theoreme de Lagrange). *Soit  $(G, \cdot)$  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  $g$   $\text{ord}(g) = |g\mathbb{Z}|$  divise l'ordre de  $G$ .*

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  $g$ )

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

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

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

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

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

□



## CHAPITRE 3

### Isometries du plan

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

Le plan réel est le produit

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

forme de paires de nombres réels. Étant donné un élément  $(x, y)$  de  $\mathbb{R}^2$ ,  $x$  et  $y$  sont les coordonnées de cet élément. L'élément  $(0, 0)$  est noté **0** et est appelé l'origine. Le sous-ensemble

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

est appelé axe des abscisses et l'ensemble

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

est appelé axe des ordonnées.

**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'élément neutre est l'origine **0**; avec la multiplication par les scalaires définie par

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

c'est même 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 élément  $(x, y) \in \mathbb{R}^2$  s'écrit comme combinaison linéaire

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

et cette écriture est unique.

$\mathbb{R}^2$  vu comme groupe de translation. Étant donné un vecteur  $(u, v)$  de  $\mathbb{R}^2$ , on associe à un tel vecteur une application (dite de translation)  $t_{(u,v)} : \mathbb{R}^2 \mapsto \mathbb{R}^2$  définie 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-même dont l'application réciproque  $t_{(u,v)}^{-1}$  est la translation de vecteur opposé  $t_{(-u,-v)}$ , en effet pour tout point  $P$

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

et

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

Plus généralement on a

PROPOSITION 3.1. *L'application*

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

*est un morphisme de groupe injectif.*

PREUVE. c'est un cas particulier de l'exercice 2.4 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

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

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*

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

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 donnees deux points  $P, Q \in \mathbb{R}^2$  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  $\vec{0P}$  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*

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

*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'image par une translation 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  $D = \mathcal{D}(P, \vec{v})$  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'équation

$$ax + by = c$$

avec

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

Notons que ces representations ne sont pas uniques.

Rappelons egalement les definitions et resultats de base concernant les droites

PROPOSITION 3.3. *Etant donnees 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 donnees deux droites  $D = D(P, \vec{v})$ ,  $D' = D'(P', \vec{v}')$  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 ( $\vec{v}' \neq \lambda \cdot \vec{v}$  pour tout  $\lambda \in \mathbb{R}^\times$ ) ; dans le deuxième cas les droites sont dites paralleles et dans le troisième 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 donnée par

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

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

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

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

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

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

- Separation des points: pour tout  $\vec{u} \in \mathbb{R}^2$ ,  $P, Q \in \mathbb{R}^2$ ,  $\lambda \in \mathbb{R}$

$$\|\vec{u}\| = 0 \iff \vec{u} = \mathbf{0}, \quad d(P, Q) = 0 \iff P = Q.$$

- Symétrie:

$$d(P, Q) = d(Q, P).$$

- Inégalité du triangle:

$$\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|, \quad d(P, R) \leq d(P, Q) + d(Q, R)$$

avec égalité si et seulement si  $P, Q, R$  sont alignés (cad  $\vec{PQ}$  et  $\vec{PR}$  sont proportionnels) et  $Q$  est "entre"  $P$  et  $R$ .

- Homogénéité:

$$\|\lambda \vec{u}\| = |\lambda| \|\vec{u}\|, \quad d(\lambda P, \lambda Q) = |\lambda| d(P, Q)$$

avec  $\lambda P$  l'image de  $P$  par l'homothétie de centre  $\mathbf{0}$  et de rapport  $\lambda$ :

$$[\times \lambda] : \begin{array}{ccc} \mathbb{R}^2 & \mapsto & \mathbb{R}^2 \\ (x, y) & \mapsto & (\lambda x, \lambda y) \end{array}$$

DÉFINITION 3.6. Etant donné  $P \in \mathbb{R}^2$  et  $r \geq 0$ , le cercle de centre  $P$  et de rayon  $r$  est l'ensemble des points du plan à distance  $r$  de  $P$

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

Dans le théorème ci-dessus, le seul point non évident est l'inégalité du triangle. Elle peut être vérifiée "à la main" mais il est plus utile (notamment en vue de généralisations) de la démontrer en introduisant une structure supplémentaire:

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

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

On a donc

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

Rappelons que

PROPOSITION 3.4. le produit scalaire euclidien a les propriétés suivantes:

- symétrique:

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

– bilineaire:

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

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

– défini-positif:

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

et

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

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

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

et combinant les cas + et - de ces deux identités, on a

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

Dans cette proposition, le seul point non évident est l'inégalité du triangle. Elle provient de la proposition suivante

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

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

avec égalité si et seulement si  $\vec{u}$  et  $\vec{v}$  sont proportionnels: 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  $\vec{u} = \mathbf{0} = 0 \cdot \vec{v}$  est colinéaire à  $\vec{v}$ ).

**PREUVE.** On peut supposer  $\vec{v} \neq 0$  (sinon on a  $0 = 0$ ). Pour  $\lambda \in \mathbb{R}$  considérons la fonction

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

C'est un polynôme à coefficients réels de degré  $\leq 2$  et à valeurs positives ou nulles. La dérivée de  $P$  s'annule en

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

et

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

d'où l'inégalité. En cas d'égalité

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

□

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

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

□

#### 1.4. Décomposition dans une base orthogonale.

DÉFINITION 3.7. *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  $(\vec{u}) \cup (\vec{v})$ .*

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

$$\begin{aligned} \lambda a + \mu c &= x \\ \lambda b + \mu d &= y \end{aligned}$$

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

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

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

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

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

$$(1.3) \quad \vec{w} = \langle \vec{w}, \vec{u} \rangle \vec{u} + \langle \vec{w}, \vec{v} \rangle \vec{v} \quad \text{si } (\vec{u}, \vec{v}) \text{ est orthonormee.}$$

*Les nombres*

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

*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 1.1. La base canonique

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

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:

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

On note

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

l'ensemble des isometries du plan. Cet ensemble est non-vide:  $\text{Id}_{\mathbb{R}^2}$  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

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

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

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

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

*Plus précisément, toute isometrie  $\phi$  se décompose de manière unique sous la forme*

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

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

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

THÉORÈME 3.3. *Soit  $\phi$  une isometrie fixant l'origine  $\mathbf{0}$ ; alors  $\phi$  est linéaire: 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 linéaire. En particulier on a*

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

Le théorème précédent induit la définition suivante:

DÉFINITION 3.9. *L'ensemble  $\text{Isom}(\mathbb{R}^2)_{\mathbf{0}}$  s'appelle l'ensemble des isometries linéaires du plan. Par opposition un élément général de  $\text{Isom}(\mathbb{R}^2)$  sera parfois appellé "isometrie affine".*

La preuve de ce theoreme repose sur la

**PROPOSITION 3.7.** *Soit  $\phi \in \text{Isom}_0(\mathbb{R}^2)$ , 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  $\phi \in \text{Isom}_0(\mathbb{R}^2)$ , 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  $\vec{w} = \mathbf{0}\vec{Q}$

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

□

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

$$\begin{aligned} \|\phi(\lambda\vec{u} + \vec{v}) - (\lambda\phi(\vec{u}) + \phi(\vec{v}))\|^2 &= \|\phi(\lambda\vec{u} + \vec{v})\|^2 + \|\lambda\phi(\vec{u})\|^2 + \|\phi(\vec{v})\|^2 \\ &\quad - 2\langle \phi(\lambda\vec{u} + \vec{v}), \lambda\phi(\vec{u}) \rangle - 2\langle \phi(\lambda\vec{u} + \vec{v}), \phi(\vec{v}) \rangle + 2\langle \lambda\phi(\vec{u}), \phi(\vec{v}) \rangle \\ &= \|\lambda\vec{u} + \vec{v}\|^2 + \lambda^2\|\vec{u}\|^2 + \|\vec{v}\|^2 - 2\lambda\langle \lambda\vec{u} + \vec{v}, \vec{u} \rangle - 2\langle \lambda\vec{u} + \vec{v}, \vec{v} \rangle + 2\lambda\langle \vec{u}, \vec{v} \rangle \\ &= \|\lambda\vec{u} + \vec{v} - (\lambda\vec{u} + \vec{v})\|^2 = 0 \end{aligned}$$

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<sup>1</sup>.

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

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

et donc  $\phi^{-1} \in \text{Isom}(\mathbb{R}^2)_0$ ; en particulier  $\phi^{-1}$  est lineaire.

---

<sup>1</sup>C'est un resultat qui est demonstre dans le cours d'algèbre 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

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

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

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

□

### Preuve du Theoreme 3.2.

- L'identite  $\text{Id}_{\mathbb{R}^2}$  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  $\text{Isom}(\mathbb{R}^2)$ ,  $\text{Isom}(\mathbb{R}^2)_{\mathbf{0}}$  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  $\text{Bij}(\mathbb{R}^2)$ .
- Soit  $\phi$  une isometrie generale: montrons que  $\phi$  est la composee d'une translation et d'une isometrie lineaire. A lors  $\phi_{\mathbf{0}} = t_{-\phi(\mathbf{0})} \circ \phi$  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  $\text{Isom}(\mathbb{R}^2)$  est un sous-groupe de  $\text{Bij}(\mathbb{R}^2)$  et  $\text{Isom}(\mathbb{R}^2)_{\mathbf{0}}$  et  $T(\mathbb{R}^2)$  sont des sous-groupes.

- Montrons que la decomposition translation/isometrie lineaire

$$\phi = t \circ \phi_{\mathbf{0}}$$

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

$$\phi = t \circ \phi_{\mathbf{0}} = t' \circ \phi'_{\mathbf{0}}.$$

On a alors

$$t'^{-1} \circ t = \phi'_{\mathbf{0}} \circ \phi_{\mathbf{0}}^{-1}$$

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

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

Il en resulte que

$$t = t', \phi_{\mathbf{0}} = \phi'_{\mathbf{0}}.$$

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

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

et plus précisément

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

On commence par supposer que  $\phi = \phi_0 \in \text{Isom}(\mathbb{R}^2)_0$ . Par linearité de  $\phi_0$ ,

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

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

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

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

□

On déduit de cette décomposition le corollaire suivant qui sera très utile:

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

$$\begin{array}{ccc} \text{lin} = \cdot_0 : & \text{Isom}(\mathbb{R}^2) & \mapsto \text{Isom}(\mathbb{R}^2)_0 \\ & \phi & \mapsto \phi_0 \end{array}$$

qui a une isométrie associée sa partie linéaire est un morphisme de groupe surjectif.

**Preuve:** L'application est surjective: si  $\phi_0$  est une isométrie linéaire alors c'est sa propre partie linéaire. Il s'agit de montrer que si  $\phi$  et  $\psi$  sont deux isométries de parties linéaires  $\phi_0$  et  $\psi_0$  alors

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

On a

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

avec  $t$  et  $t'$  des translations et

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

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

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

se décompose en une translation et une isométrie linéaire. Par unicité de cette décomposition  $\phi_0 \circ \psi_0$  est la partie linéaire de  $\phi \circ \psi$ .

□

Ainsi si on doit identifier une isométrie affine qui est un produit d'isométries connues, on obtient sa partie linéaire en composant les parties linéaires de ses constituants. On peut calculer ensuite la partie translation.

**REMARQUE 2.1.** L'existence et l'unicité de la décomposition d'une isométrie en translation et en partie linéaire est le fait que l'application

$$\begin{array}{ccc} T(\mathbb{R}^2) \times \text{Isom}(\mathbb{R}^2)_0 & \mapsto & \text{Isom}(\mathbb{R}^2) \\ (t, \phi_0) & \mapsto & t \circ \phi_0 \end{array}$$

est une bijection. Par contre ce n'est pas un isomorphisme entre le groupe produit "abstrait"  $T(\mathbb{R}^2) \times \text{Isom}(\mathbb{R}^2)_0$  et le groupe  $\text{Isom}(\mathbb{R}^2)$ . On verra plus tard que si l'on équipe le produit

$T(\mathbb{R}^2) \times \text{Isom}(\mathbb{R}^2)_0$  d'une loi de groupe adequate (dite de "produit semi-direct") on obtient un isomorphisme de groupes.

**2.1. Matrice associee a une isometrie.** Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_0$  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

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

on a

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

Alternativement,  $\phi(x, y) = (X, Y)$  peut se calculer comme le produit matriciel

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

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

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

Comme  $\phi$  est bijective et lineaire,  $\phi^{-1}$  est lineaire et sa une matrice associee est l'inverse de celle de  $M_\phi$ ; ces coefficients sont donnees par la formule

$$M_{\phi^{-1}} = M_\phi^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

ou

$$\det(M_\phi) = ad - bc$$

est le determinant. On a donc

$$(2.2) \quad M_\phi \cdot M_{\phi^{-1}} = M_{\phi^{-1}} \cdot M_\phi = M_{\text{Id}_{\mathbb{R}^2}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dans ce cas precis on a

THÉORÈME 3.5. Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_0$  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

$$(2.3) \quad M_{\phi^{-1}} = M_\phi^{-1} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

On a donc

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et ainsi les egalites

$$(2.4) \quad a^2 + c^2 = b^2 + d^2 = a^2 + b^2 = c^2 + d^2 = 1, \quad ab + cd = ac + bd = 0$$

$$(2.5) \quad \det(M_\phi) = ad - bc = \pm 1.$$

**Preuve:** Pour trouver les coefficients de  $M_{\phi^{-1}} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ , on doit résoudre les deux équations d'inconnues  $(a', c')$  et  $(b', d')$

$$\phi(a', c') = \mathbf{e}_1, \quad \phi(b', d') = \mathbf{e}_2$$

ou encore

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

En d'autres termes on cherche à exprimer les vecteurs  $\mathbf{e}_1$  et  $\mathbf{e}_2$  comme combinaison linéaire des vecteurs  $\mathbf{e}'_1$  et  $\mathbf{e}'_2$ ; comme on l'a déjà vu

$$\phi(\mathcal{B}_0) = (\phi(\mathbf{e}_1), \phi(\mathbf{e}_2)) = (\mathbf{e}'_1, \mathbf{e}'_2)$$

est une base orthonormée de  $\mathbb{R}^2$  et donc on a (cf. (1.3))

$$\begin{aligned} a' &= \langle \mathbf{e}_1, \mathbf{e}'_1 \rangle = \langle \phi(\mathbf{e}_1), \mathbf{e}_1 \rangle = a, & c' &= \langle \mathbf{e}_1, \mathbf{e}'_2 \rangle = \langle \phi(\mathbf{e}_2), \mathbf{e}_1 \rangle = b \\ b' &= \langle \mathbf{e}_2, \mathbf{e}'_1 \rangle = \langle \phi(\mathbf{e}_1), \mathbf{e}_2 \rangle = c, & d' &= \langle \mathbf{e}_2, \mathbf{e}'_2 \rangle = \langle \phi(\mathbf{e}_2), \mathbf{e}_2 \rangle = d. \end{aligned}$$

On a donc montrer que

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

Cela démontre (2.3) et les identités (2.4) résultent immédiatement de (2.2) en identifiant les coefficients des matrices en question. Pour (2.5), on a

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

□

REMARQUE 2.2. Une autre manière de montrer que  $\det(M_\phi) = \pm 1$ : on a

$$\det(M_\phi) \det(M_\phi^{-1}) = \det(M_\phi \cdot M_\phi^{-1}) = \det(\text{Id}) = 1$$

et

$$\det(M_\phi) = ad - bc = ad - cb = \det(M_\phi^{-1})$$

et donc

$$\det(M_\phi)^2 = 1.$$

REMARQUE 2.3. Comme  $\phi$  est une isométrie on a

$$\|\phi(\mathbf{e}_i)\|^2 = \|\mathbf{e}_i\|^2 = 1, \quad i = 1, 2, \quad \langle \phi(\mathbf{e}_1), \phi(\mathbf{e}_2) \rangle = \langle \mathbf{e}_1, \mathbf{e}_2 \rangle = 0$$

La premier identité pour  $i = 1$  donne  $a^2 + c^2 = 1$  et pour  $i = 2$ ,  $b^2 + d^2 = 1$  alors que la troisième donne  $ab + cd = 0$ . On peut alors en déduire les autres relations de (2.4). Ces relations signifient que les vecteurs colonnes (resp. lignes) de  $M_\phi$  forment des vecteurs orthonormaux.

PROPOSITION 3.8. Reciproquement, soit  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  une matrice qui vérifie

$$M^{-1} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

(et qui vérifie donc (2.4)) alors l'application linéaire définie par

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

est une isométrie linéaire.

**Preuve:** On a  $\phi(\mathbf{0}) = \mathbf{0}$  et

$$\begin{aligned}\langle \phi(x, y), \phi(x, y) \rangle &= \langle x(a, c) + y(b, d), x(a, c) + y(b, d) \rangle \\ &= x^2 \langle (a, c), (a, c) \rangle + 2xy \langle (a, c), (b, d) \rangle + y^2 \langle (b, d), (b, d) \rangle \\ &= x^2 + 0 + y^2 = \langle (x, y), (x, y) \rangle.\end{aligned}$$

□

2.1.1. *La transposition.* Soit

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

l'espace des matrices  $2 \times 2$ . C'est un  $\mathbb{R}$ -espace vectoriel de dimension 4 pour l'addition des matrices. Avec la multiplication matricielle  $(M_2(\mathbb{R}), +, \times)$  forme un anneau dont l'élément nul et l'élément unité sont respectivement

$$\mathbf{0}_{M_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{Id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Le groupe des éléments inversibles pour la multiplication est le groupe des matrices de déterminant non-nul: on l'appelle le groupe linéaire et on le note

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, \det(M) = ad - bc \neq 0 \right\}.$$

DÉFINITION 3.1. Soit

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}),$$

la matrice

$${}^t M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbb{R})$$

s'appelle la transposee de  $M$  et l'application

$${}^t \cdot : M \in M_2(\mathbb{R}) \mapsto {}^t M \in M_2(\mathbb{R})$$

est l'application de transposition.

PROPOSITION 3.9. L'application de transposition a les propriétés suivantes

(1)  ${}^t$  est linéaire:

$${}^t(\lambda M + N) = \lambda {}^t M + {}^t N.$$

(2)  ${}^t$  est involutive:

$${}^t \cdot \circ {}^t \cdot = \text{Id}_{M_2(\mathbb{R})}, \quad {}^t({}^t M) = M.$$

(3) La transposition est multiplicativa:

$${}^t M \cdot N = {}^t N \cdot {}^t M.$$

(4) La transposition preserve le déterminant  $\det(M) = ad - bc$ .

$$\det({}^t M) = \det(M).$$

**Preuve:** Exercice. □

2.1.2. *L'ensemble des matrices orthogonales.*

DÉFINITION 3.2. Une matrice  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$  est orthogonale si elle vérifie

$$M \cdot {}^t M = \text{Id}_2$$

ou de manière équivalente

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

Elle vérifie alors automatiquement

$${}^t M \cdot M = \text{Id}_2$$

et

$$(2.6) \quad a^2 + c^2 = b^2 + d^2 = 1, \quad ab + cd = 0$$

et

$$(2.7) \quad \det(M) = ad - bc = \pm 1.$$

Une matrice orthogonale de déterminant  $+1$  est dite spéciale et une matrice orthogonale de déterminant  $-1$  est dite non-spéciale.

On note  $O_2(\mathbb{R})$  (*resp.*  $SO_2(\mathbb{R}) = O_2(\mathbb{R})^+$ ,  $O_2(\mathbb{R})^-$ ) l'ensemble des matrices orthogonales (*resp.* *spéciales et non-spéciales*). On a donc

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

PROPOSITION 3.10. Soit  $M$  une matrice spéciale orthogonale alors il existe  $c, s \in \mathbb{R}$  vérifiant  $c^2 + s^2 = 1$  telle que

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

Soit  $M$  une matrice non-spéciale orthogonale alors il existe  $c, s \in \mathbb{R}$  vérifiant  $c^2 + s^2 = 1$  telle que

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

Une matrice non-spéciale est d'ordre 2: on a

$$M^2 = \text{Id} \text{ et } M \neq \text{Id}.$$

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

$$cb + sd = 0.$$

Comme  $c^2 + s^2 = 1$ ,

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

On a

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

Soit  $M = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}$  une matrice non-spéciale alors  $M \neq \text{Id}$  car  $\det M = -1$  et

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

donc  $M^2 = \text{Id}$ .

□

THÉORÈME 3.6. *On a les propriétés suivantes*

- (1) *L'ensemble des matrices orthogonales  $O_2(\mathbb{R})$  est un sous-groupe du groupe des matrices inversibles  $GL_2(\mathbb{R})$ .*
- (2) *L'ensemble des matrices spéciales orthogonales  $O_2(\mathbb{R})^+$  est un sous-groupe distingué de  $O_2(\mathbb{R})$ .*
- (3) *Le groupe des matrices spéciales orthogonales est commutatif.*
- (4) *L'ensemble des matrices de non-spéciales  $O_2(\mathbb{R})^-$  est le translate multiplicatif (à gauche ou à droite) de  $O_2(\mathbb{R})^+$  par n'importe quelle matrice non-spéciale (par exemple la matrice  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ):*

$$\forall M^- \in O_2(\mathbb{R})^-, \text{ on a } O_2(\mathbb{R})^- = M^-.O_2(\mathbb{R})^+ = O_2(\mathbb{R})^+.M^-.$$

*En d'autres termes, étant donné  $M^- \in O_2(\mathbb{R})^-$ , toute matrice de  $O_2(\mathbb{R})^-$  est de la forme  $M^-.M^+$  (resp.  $M^+.M^-$ ) pour un unique  $M^+$  (resp.  $M'^+$ ) de  $O_2(\mathbb{R})^+$ .*

- (5) *Toute matrice de spéciale s'écrit comme produit de deux matrices de non-spéciales.*  
*En particulier le groupe  $O_2(\mathbb{R})$  est engendré par les matrices orthogonales non-spéciales  $O_2(\mathbb{R})^-$ .*

PREUVE. Toute matrice de  $O_2(\mathbb{R})$  est inversible et son inverse est sa transposée  ${}^t M$  donc  $O_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ . De plus  $M^{-1} = {}^t M$  est aussi dans  $O_2(\mathbb{R})$ .

– Si  $M, N \in O_2(\mathbb{R})$ ,

$$(M.N)^t(M.N) = M.N.{}^t N.{}^t M = M.\text{Id}_2.{}^t M = M.{}^t M = \text{Id}_2$$

donc  $M.N \in O_2(\mathbb{R})$ . Ainsi  $O_2(\mathbb{R})$  est un sous-groupe de  $GL_2(\mathbb{R})$ .

– On rappelle que le déterminant  $\det : GL_2(\mathbb{R}) \mapsto \mathbb{R}^\times$  vérifie

$$\det(MN) = \det(M)\det(N), \quad \det(M^{-1}) = \det(M)^{-1}.$$

En d'autre terme c'est un morphisme du groupe  $(GL_2(\mathbb{R}), \times)$  vers le groupe multiplicatif  $(\mathbb{R}^\times, \times)$ . En particulier la restriction de  $\det$  au sous-groupe  $O_2(\mathbb{R})$  est un morphisme de groupes (son image est le sous-groupe  $\{\pm 1\}$ ). L'ensemble des matrices spéciales orthogonales

$$O_2(\mathbb{R})^+ = \{M \in O_2(\mathbb{R}), \det M = 1\} = \ker(\det|_{O_2(\mathbb{R})})$$

est le noyau de ce morphisme (restreint au sous-groupe  $O_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ ), c'est donc un sous-groupe qui est de plus distingué.

– Soient  $M = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}$  et  $M' = \begin{pmatrix} c' & -s' \\ s' & c' \end{pmatrix}$  deux matrices spéciales, 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

$$c'' = cc' - ss', \quad s'' = cs' + sc'.$$

On remarque que ces expressions ne changent pas si on échange  $c \leftrightarrow c'$  et  $s \leftrightarrow s'$  donc

$$M.M' = M'.M;$$

en d'autres termes, le groupe  $O_2(\mathbb{R})^+$  est commutatif.

– Soit  $M^- \in O_2(\mathbb{R})^-$  (par exemple  $w = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ) et  $M^+ \in O_2(\mathbb{R})^+$  alors  $M = M^+.M^-$  verifie

$$\det(M) = \det(M^+) \det(M^-) = -1$$

et  $M \in O_2(\mathbb{R})^-$ : on a  $O_2(\mathbb{R})^+.M^- \subset O_2(\mathbb{R})^-$ . Reciproquement soit  $M \in O_2(\mathbb{R})^-$  et  $M' = M.(M^-)^{-1}$  alors

$$\det(M') = \det(M) \det((M^-)^{-1}) = -1 \cdot -1 = 1$$

et  $M' \in O_2(\mathbb{R})^+$  et  $M = M'.M^-$  donc  $O_2(\mathbb{R})^- \subset O_2(\mathbb{R})^+.M^-$  et  $O_2(\mathbb{R})^- = O_2(\mathbb{R})^+.M^-$ . De meme on montre que  $O_2(\mathbb{R})^- = M^-.O_2(\mathbb{R})^+$ .

– Soit  $M^+ \in O_2(\mathbb{R})^+$  alors  $M^-.M^+ = M \in O_2(\mathbb{R})^-$  et

$$M^+ = (M^-)^{-1}.M^-.M^+ = (M^-)^{-1}.M$$

est le produit de deux matrices non-speciales ( $\det((M^-)^{-1}) = (-1)^{-1} = -1$ ; en fait comme on l'a vu  $(M^-)^{-1} = M^-$ ). Ainsi tout element de  $O_2(\mathbb{R})$  s'ecrit comme produit de une ou deux matrices non-speciales suivant qu'il est dans  $O_2(\mathbb{R})^-$  ou dans  $O_2(\mathbb{R})^+$ :  $O_2(\mathbb{R})$  est engendre par l'ensemble  $O_2(\mathbb{R})^-$ .  $\square$

### 3. Classification des isometries lineaires

On a vu que l'application

$$\begin{aligned} \text{Isom}(\mathbb{R}^2)_0 &\mapsto O_2(\mathbb{R}) \\ \phi &\mapsto M_\phi \end{aligned}$$

qui a une isometrie lineaire associe sa matrice (dans la base  $(\mathbf{e}_1, \mathbf{e}_2)$ ) est une bijection: elle est injective car une application lineaire est entierement determinee par les images des vecteurs  $\mathbf{e}_1, \mathbf{e}_2$  et surjective par la Proposition 3.8. On a mieux:

**THÉORÈME 3.7.** *L'application  $\text{Isom}(\mathbb{R}^2)_0 \mapsto O_2(\mathbb{R})$  qui a une isometrie lineaire associe sa matrice (dans la base  $(\mathbf{e}_1, \mathbf{e}_2)$ ) est un isomorphisme de groupes. Une isometrie lineaire dont la matrice associee est une matrice speciale (resp. non-speciale) sera dite isometrie lineaire speciale (resp. non-speciale).*

**PREUVE.** En effet il resulte du cours d'algebre lineaire que quand on identifie un endomorphisme d'espace vectoriel a une matrice par le choix d'une base, la composition des applications correspond au produit des matrices et l'application reciproque a l'inversion des matrices.  $\square$

On defini alors les isometries lineaires speciales ou non-speciales comme etant celles dont la matrice associee est speciale ou non:

**DÉFINITION 3.3.** *On notera*

$$\text{Isom}(\mathbb{R}^2)_0^\pm = \{\phi \in \text{Isom}(\mathbb{R}^2)_0, M_\phi \in O_2(\mathbb{R})^\pm\}$$

*les sous-ensembles des isometries lineaires speciales (resp. non-speciales). On a donc*

$$\text{Isom}(\mathbb{R}^2)_0 = \text{Isom}(\mathbb{R}^2)_0^+ \sqcup \text{Isom}(\mathbb{R}^2)_0^-,$$

On deduit du Theoreme 3.7 le

**THÉORÈME 3.8.** *On a les proprietes suivantes*

- (1) *L'ensemble des isometries lineaires speciales  $\text{Isom}(\mathbb{R}^2)_0^+$  est un sous-groupe distingué du groupe  $\text{Isom}(\mathbb{R}^2)_0$  des isometries lineaires.*

- (2) *Le groupe  $\text{Isom}(\mathbb{R}^2)_0^+$  est commutatif.*
- (3) *L'ensemble des isometries lineaires non-speciales  $\text{Isom}(\mathbb{R}^2)_0^-$  est le translate mpour la composition (a gauche ou a droite) de  $\text{Isom}(\mathbb{R}^2)_0^+$  par n'importe quelle isometrie lineaire non-speciale :*
- $$\forall \phi^- \in \text{Isom}(\mathbb{R}^2)_0^-, \text{ on a } \text{Isom}(\mathbb{R}^2)_0^- = \phi^- \circ \text{Isom}(\mathbb{R}^2)_0^+ = \text{Isom}(\mathbb{R}^2)_0^+ \cdot \phi^-.$$
- En d'autres termes, etant donne  $\phi^- \in O_2(\mathbb{R})^-$ , toute isometrie lineaire non-speciale est de la forme  $\phi^- \circ \phi^+$  (resp.  $\phi'^+ \circ \phi^-$ ) pour un unique  $\phi^+$  (resp.  $\phi'^+$ ) de  $\text{Isom}(\mathbb{R}^2)_0^+$ .*
- (4) *Toute isometrie lineaire speciale s'ecrit comme produit de deux isometries lineaires non-speciales. En particulier le groupe  $\text{Isom}(\mathbb{R}^2)_0$  est engendre par  $\text{Isom}(\mathbb{R}^2)_0^-$ .*
- (5) *Une isometrie lineaire non-speciale est d'ordre 2:  $\forall \phi \in \text{Isom}(\mathbb{R}^2)^-$ , on a*

$$\phi \neq \text{Id}, \phi \circ \phi = \text{Id}.$$

**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 3.10. Soit  $X$  un ensemble et  $\phi \in \text{Bij}(X)$  une bijection sur cet ensemble; l'ensemble des points fixes de  $\phi$  est defini par

$$\text{Fix}(\phi) = \{x \in X, \phi(x) = x\}.$$

On considere le cas  $X = \mathbb{R}^2$  et  $\phi \in \text{Isom}(\mathbb{R}^2)_0$ .

PROPOSITION 3.11. Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_0$  une isometrie lineaire alors l'ensemble de ses points fixes  $\text{Fix}(\phi)$  est un sous-espace vectoriel de  $\mathbb{R}^2$  et donc est soit

$$\{\mathbf{0}\}, \text{ Une droite } \mathbb{R}\vec{u}, \mathbb{R}^2.$$

**Preuve:** On a

$$\vec{x} \in \text{Fix}(\phi) \iff \phi(\vec{x}) = \vec{x} \iff \phi(\vec{x}) - \vec{x} = (\phi - \text{Id}_{\mathbb{R}^2})(\vec{x}) = \mathbf{0}.$$

ainsi l'ensemble des points fixes,  $\text{Fix}(\phi)$  est exactement le noyau  $\ker(\phi - \text{Id}_{\mathbb{R}^2})$  de l'application lineaire  $\phi - \text{Id}_{\mathbb{R}^2}$ : c'est donc un sous-espace vectoriel de dimension 0, 1 ou 2.  $\square$

REMARQUE 3.1. Si  $\text{Fix}(\phi) = \mathbb{R}^2$  alors  $\phi = \text{Id}$

PROPOSITION 3.12. Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_0$  une isometrie lineaire alors

- Si  $\phi = \text{Id}$ ,  $\text{Fix}(\phi) = \mathbb{R}^2$ ,
- Si  $\phi \in \text{Isom}(\mathbb{R}^2)_0^+$ ,  $\text{Fix}(\phi) = \{\mathbf{0}\}$ ,
- Si  $\phi \in \text{Isom}(\mathbb{R}^2)_0^+$ ,  $\text{Fix}(\phi) = \mathbb{R}\vec{u}$  avec  $\vec{u} \neq \mathbf{0}$ .

**Preuve:** Soit  $M$  la matrice associee a  $\phi$ ; l'ensemble des points fixes  $\text{Fix}(\phi)$  est l'ensemble des solution du systeme lineaire

$$M \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \iff \begin{cases} (a-1)x + by = 0 \\ cx + (d-1)y = 0 \end{cases}$$

- Si  $\phi = \text{Id}$ , alors  $a-1 = b = c = d-1 = 0$  et  $\text{Fix}(\phi) = \mathbb{R}^2$ .
- Supposons  $\phi$  speciale et  $\neq \text{Id}$  le systeme devient

$$\begin{cases} (c-1)x - sy = 0 \\ sx + (c-1)y = 0 \end{cases}$$

et le determinant de ce système vaut

$$(c - 1)^2 + s^2 \neq 0$$

(car sinon  $c - 1 = s$  ce qui est exclu) dont la seule solution est  $\mathbf{0}$ .

– Supposons  $\phi$  non-spéciale, le système devient

$$\begin{cases} (c - 1)x + sy = 0 \\ sx - (c + 1)y = 0 \end{cases}$$

et le determinant de ce système vaut

$$(c^2 - 1) - s^2 = 0$$

de plus le système est non-trivial (si  $s = 0$  alors  $c - 1$  ou  $c + 1$  est non-nul) et donc le système est équivalent à une de ses lignes (une de celles qui est non-nulle). L'ensemble des solutions est donc de la forme  $\mathbb{R}\vec{u}$ .  $\square$

**3.2. Rotations.** Dans le premier cas on fait la définition suivante:

DÉFINITION 3.4. Si  $\phi$  est spéciale on dira que  $\phi$  est une rotation et que sa matrice est une matrice de rotation. Le groupe  $\text{Isom}(\mathbb{R}^2)_\mathbf{0}^+$  des isométries spéciales est encore appellé le groupe des rotations de centre  $\mathbf{0}$ .

Le groupe des rotations a la propriété fondamentale suivante:

THÉORÈME 3.9. Soit

$$\mathbf{C}^1 = \{(x, y) \in \mathbb{R}^2, x^2 + y^2 = 1\}$$

le cercle unité (le cercle de rayon 1 centre en  $\mathbf{0}$ ). Soient  $P, Q \in \mathbf{C}^1$  il existe une unique rotation linéaire  $r = r_{P,Q}$  telle que

$$r(P) = Q.$$

En particulier, pour tout  $P \in \mathbf{C}^1$  l'application

$$\begin{aligned} \text{ev}_P : \text{Isom}(\mathbb{R}^2)_\mathbf{0}^+ &\mapsto \mathbf{C}^1 \\ r &\mapsto r(P) \end{aligned}$$

est une bijection.

**Preuve:** Montrons ce résultat pour  $P = \mathbf{e}_1 = (1, 0)$ . Soit  $Q = (c, s) \in \mathbf{C}^1$  un point du cercle unité ( $c^2 + s^2 = 1$ ) alors la rotation  $r_{(0,1),Q}$  de matrice

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix}$$

envoie  $(1, 0)$  sur  $Q$  et c'est la seule possible (puisque qu'une matrice de rotation est déterminée entièrement par sa première colonne). En général, soit  $P \in \mathbf{C}^1$  un point du cercle alors pour tout  $Q$  la rotation

$$r_{P,Q} = r_{(0,1),Q} \circ r_{(0,1),P}^{-1}$$

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'identité.  $\square$

Le théorème précédent permet donc d'identifier le groupe des rotations linéaires avec cercle unité. On reverra plus tard cette identification avec les nombres complexes.

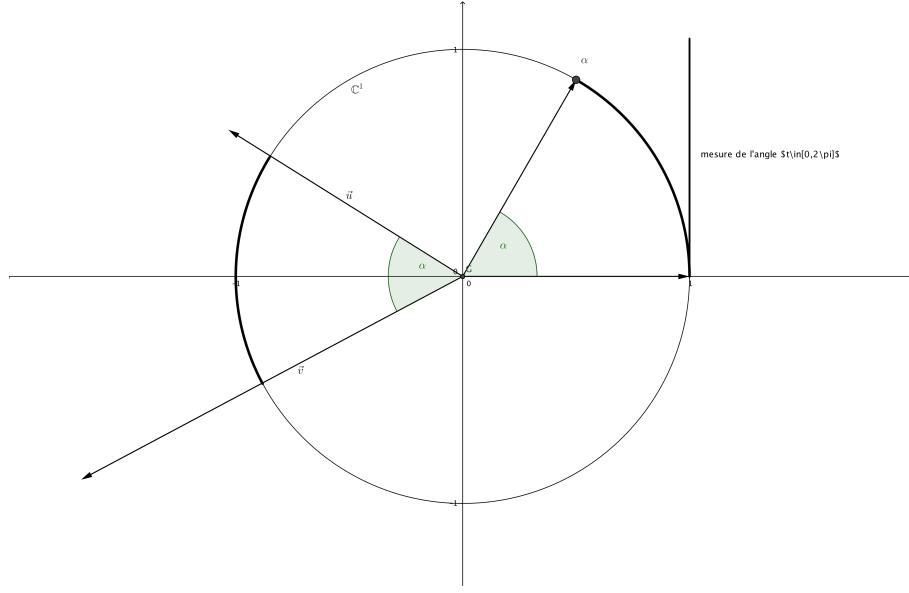


FIGURE 1. Deux paires de vecteurs representant le même angle

### 3.2.1. Angle de deux vecteurs.

DÉFINITION 3.5. Soit  $\vec{u}, \vec{v} \in \mathbf{C}^1$  des vecteurs de longueur 1, leur angle est l'unique rotation  $r_{\vec{u}, \vec{v}}$  qui envoie  $\vec{u}$  sur  $\vec{v}$ .

-Soit  $\vec{u}, \vec{v}$  deux vecteurs non-nuls, leur angle  $r_{\vec{u}, \vec{v}}$  est l'unique rotation qui envoie  $\vec{u}/\|\vec{u}\|$  sur  $\vec{v}/\|\vec{v}\|$ . C'est également l'unique rotation qui envoie la demi-droite  $\mathbb{R}_{\geq 0}\vec{u}$  sur la demi-droite  $\mathbb{R}_{\geq 0}\vec{v}$ . On le note

$$\widehat{\vec{u}\vec{v}}.$$

-Soit  $[P, Q]$  et  $[P', Q']$  deux segments orientés, leur angle est l'angle

$$\widehat{\overrightarrow{PQ}\overrightarrow{P'Q'}}.$$

-Soit  $\mathbb{R}\vec{u}, \mathbb{R}\vec{v}$  deux droites, il existe exactement deux rotations qui envoient la droite  $\mathbb{R}\vec{u}$  sur la droite  $\mathbb{R}\vec{v}$  ( $r_{\vec{u}, \vec{v}}$  et  $r_{\vec{u}, -\vec{v}} = -r_{\vec{u}, \vec{v}}$ ). On définit leur angle comme étant l'ensemble de ces deux angles  $\{r_{\vec{u}, \vec{v}}, -r_{\vec{u}, \vec{v}}\}$ .

REMARQUE 3.2. (1) L'ensemble des angles est l'ensemble des rotations  $\text{Isom}(\mathbb{R}^2)_0^+$ ; c'est donc un groupe abélien et étant donné  $r, r'$  deux angles l'angle obtenu par composition  $r \circ r' = r' \circ r$  est la "somme" des angles.

(2) On définit de même la somme de deux angles entre deux droites comme la paire  $\{r \circ r', -r \circ r'\}$ .

(3) On peut identifier une rotation (donc un angle) avec sa matrice et donc avec le vecteur de  $\mathbb{R}^2$ ,  $(c, s)$ . Dans ce cas la "somme" de deux angles  $(c, s)$  et  $(c', s')$  est  $(cc' - ss', sc' + cs')$ .

EXERCICE 3.1. Étant donné 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 moitié.

### 3.2.2. Mesure d'un angle.

DÉFINITION 3.6. La mesure d'un angle  $r$  représentée par  $(c, s)$  est la longueur de l'arc du cercle unité allant de  $(1, 0)$  à  $(c, s)$  parcouru dans le sens inverse des aiguilles d'une montre; c'est un nombre réel compris entre  $0$  et  $2\pi$  (la longueur du cercle unité).

Le problème avec cette définition est qu'il faut d'abord définir les notions de

- "longueur de l'arc du cercle unité allant de..." ,
- "parcouru dans le sens inverse des aiguilles d'une montre"

Pour cela on a besoin de la notion de courbe paramétrée et de longueur d'une telle courbe.

DÉFINITION 3.7. Soit  $\mathbb{R}/2\pi\mathbb{Z}$  l'ensemble  $[0, 2\pi[$  muni de la loi de composition

$$\theta \oplus \theta' = \text{l'unique élément de l'intersection } [0, 2\pi[ \cap \theta + \theta' + 2\pi\mathbb{Z}.$$

Alors

$$\mathbb{R}/2\pi\mathbb{Z} = ([0, 2\pi[, \oplus)$$

est un groupe abélien en bijection avec  $C^1$  et  $\text{Isom}(\mathbb{R}^2)_{\mathbf{0}}^+$ .

**3.3. Symétries.** On étudie maintenant le cas où  $\phi$  est non-spéciale.

LEMME 3.2. 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 éléments de  $\vec{u}^\perp$  sont les vecteurs  $\vec{v} = (x, y)$  vérifiant le système linéaire

$$ax + by = 0$$

c'est à dire l'ensemble

$$\mathbb{R}(-b, a) = \{\lambda(-b, a), \lambda \in \mathbb{R}\}.$$

□

THÉORÈME 3.10. Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_{\mathbf{0}}^-$  et  $\text{Fix}(\phi) = \mathbb{R}\vec{u}$  la droite de ces points fixes. Soit  $\vec{v}$  un vecteur non-nul perpendiculaire à  $\vec{u}$  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

$$(3.1) \quad \phi(\vec{u}) = \vec{u}, \quad \phi(\vec{v}) = -\vec{v}.$$

Reciproquement pour  $\vec{v} \neq 0$ , l'application  $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  donnée par

$$\phi(\vec{w}) = \vec{w} - 2 \frac{\langle \vec{w}, \vec{v} \rangle}{\langle \vec{v}, \vec{v} \rangle} \vec{v}$$

est une isométrie linéaire non-spéciale.

**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

$$\phi(\vec{v}) = \lambda \vec{v}, \quad \lambda \in \mathbb{R}.$$

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 à  $\vec{u}$ . On a donc démontre (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

$$\begin{aligned} \phi(\vec{w}) &= \frac{\langle \vec{w}, \vec{u} \rangle}{\langle \vec{u}, \vec{u} \rangle} \phi(\vec{u}) + \frac{\langle \vec{w}, \vec{v} \rangle}{\langle \vec{v}, \vec{v} \rangle} \phi(\vec{v}) \\ &= \frac{\langle \vec{w}, \vec{u} \rangle}{\langle \vec{u}, \vec{u} \rangle} \vec{u} - \frac{\langle \vec{w}, \vec{v} \rangle}{\langle \vec{v}, \vec{v} \rangle} \vec{v} = \vec{w} - 2 \frac{\langle \vec{w}, \vec{v} \rangle}{\langle \vec{v}, \vec{v} \rangle} \vec{v}. \end{aligned}$$

Reciproquement si  $\phi$  est de cette forme elle est linéaire (par bilinéaire 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 isométrie linéaire. Par ailleurs si  $\vec{w}$  est perpendiculaire à  $\vec{v}$  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 isométrie non-spéciale.  $\square$

**DÉFINITION 3.8.** Une isométrie linéaire non-spéciale de points fixes la droite  $\mathbb{R}\vec{u}$  sera appellée la symétrie orthogonale d'axe  $\mathbb{R}\vec{u}$ .

Les isométries linéaires non-spéciales seront appellées symétries et les matrices non-spéciales, matrices de symétrie.

**3.4. Explication des symétries.** On a le formulaire suivant

THÉORÈME 3.11. Soit  $s$  une symétrie linéaire de matrice associée

$$M = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}$$

avec  $c, s \in \mathbb{R}$  vérifiant  $c^2 + s^2 = 1$ . Les vecteurs non-nuls définis par

$$(3.2) \quad \begin{cases} \vec{u} = (1, 0), \quad \vec{v} = (0, 1) & \text{si } c = 1, \\ \vec{u} = (0, 1), \quad \vec{v} = (1, 0) & \text{si } c = -1 \\ \vec{u} = (s, -(c-1)), \quad \vec{v} = (s, -(c+1)). \end{cases}$$

verifient

$$s(\vec{u}) = \vec{u}, \quad s(\vec{v}) = -\vec{v}$$

et plus généralement pour tout  $\vec{w} \in \mathbb{R}^2$

$$(3.3) \quad s(\vec{w}) = \vec{w} - 2 \frac{\langle \vec{v}, \vec{w} \rangle}{\|\vec{v}\|^2} \vec{v}.$$

Reciproquement étant donné deux vecteurs  $\vec{u}, \vec{v}$  perpendiculaires non nuls et

$$\text{sym}_{\vec{u}} : \vec{w} \mapsto \vec{w} - 2 \frac{\langle \vec{v}, \vec{w} \rangle}{\|\vec{v}\|^2} \vec{v}$$

la symétrie correspondante; si les composantes de  $\vec{v}$  sont  $\vec{v} = (C, S)$ , les composantes  $c$  et  $s$  de la matrice  $M$  de  $\text{sym}_{\vec{u}}$  sont de la forme

$$(3.4) \quad c = 1 - 2 \frac{C^2}{C^2 + S^2}, \quad s = -2 \frac{CS}{C^2 + S^2}.$$

**Preuve:** Pour trouver  $\vec{u}$  et  $\vec{v}$  on doit résoudre le système linéaire

$$\begin{cases} (c-1)x + sy = 0 \\ sx - (c+1)y = 0 \end{cases} \quad \begin{cases} (c+1)x' + sy' = 0 \\ sx' - (c-1)y' = 0 \end{cases}.$$

Si  $c = \pm 1$ , on a  $s = 0$  et des solutions sont pour  $c = 1$ , de la forme

$$\vec{u} = \alpha \mathbf{e}_1 = (\alpha, 0), \quad \vec{v} = \beta \mathbf{e}_2 = (0, \beta), \quad \alpha, \beta \in \mathbb{R}.$$

et pour  $c = -1$

$$\vec{u} = \alpha \mathbf{e}_2 = (0, \alpha), \quad \vec{v} = \beta \mathbf{e}_1 = (\beta, 0), \quad \alpha, \beta \in \mathbb{R}.$$

Si  $c \neq \pm 1$ , utilisant le fait que

$$c^2 + s^2 - 1 = (c-1)(c+1) + s^2 = 0$$

on trouve que ses systèmes sont équivalents à

$$\begin{cases} (c-1)x + sy = 0 \\ 0 = 0 \end{cases} \quad \begin{cases} (c+1)x' + sy' = 0 \\ 0 = 0 \end{cases}$$

et les solutions sont de la forme

$$\vec{u} = \alpha(s, -(c-1)), \quad \vec{v} = \beta(s, -(c+1)), \quad \alpha, \beta \in \mathbb{R}.$$

On peut vérifier directement que  $\vec{u}$  et  $\vec{v}$  sont bien perpendiculaires mais un argument plus général (sans coordonnées) 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, étant donné  $\vec{u}$  et  $\vec{v}$  deux vecteurs perpendiculaires non-nuls, considérons la symétrie orthogonale (3.3); on veut calculer sa matrice. Notons que cette définition ne dépend 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

$$\vec{v} = (C, S) = (\langle \vec{v}, \mathbf{e}_1 \rangle, \langle \vec{v}, \mathbf{e}_2 \rangle), \quad C^2 + S^2 = 1.$$

Calculons

$$\text{sym}_{\vec{u}}(\mathbf{e}_1) = \mathbf{e}_1 - 2C(C\mathbf{e}_1 + S\mathbf{e}_2) = (1 - 2C^2)\mathbf{e}_1 - 2CS\mathbf{e}_2 = c\mathbf{e}_1 + s\mathbf{e}_2$$

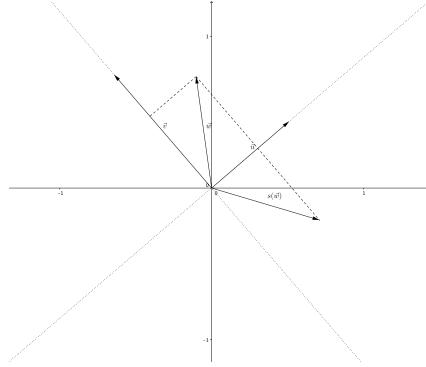


FIGURE 2. Exemple de symetrie lineaire.

$\text{sym}_{\vec{u}}(\mathbf{e}_2) = \mathbf{e}_2 - 2S(C\mathbf{e}_1 + S\mathbf{e}_2) = -2CS\mathbf{e}_1 + (1 - 2S^2)\mathbf{e}_2 = s\mathbf{e}_1 - c\mathbf{e}_2$   
en posant  $c = (1 - 2C^2)$  et  $s = -2CS$  car

$$(1 - 2C^2) + (1 - 2S^2) = 2 - 2(C^2 + S^2) = 0.$$

Ainsi la matrice de  $\text{sym}_{\vec{u}}$  est de la forme

$$\begin{pmatrix} c & s \\ s & -c \end{pmatrix} \text{ avec } c^2 + s^2 = 1 - 4C^2 + 4C^4 + 4C^2(1 - S^2) = 1.$$

□

**3.5. Classification des isometries affines.** On classifie maintenant les isometries 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

$$\text{Isom}(\mathbb{R}^2)^+ \text{ et } \text{Isom}(\mathbb{R}^2)^-$$

les ensembles d'isometries speciales ou non (rotations ou symetries affines). On a donc

$$\text{Isom}(\mathbb{R}^2) = \text{Isom}(\mathbb{R}^2)^+ \sqcup \text{Isom}(\mathbb{R}^2)^-.$$

Le resultat suivant est en grande partie laisse en exercice:

THÉORÈME 3.12. L'ensemble  $\text{Isom}(\mathbb{R}^2)^+$  est un sous-groupe distingué du groupe  $\text{Isom}(\mathbb{R}^2)$  et l'ensemble  $\text{Isom}(\mathbb{R}^2)^-$  est le translate (a gauche ou a droite) de  $\text{Isom}(\mathbb{R}^2)^+$  par un element quelconque de  $\text{Isom}(\mathbb{R}^2)^-$ .

**Preuve:** Montrons que  $\text{Isom}(\mathbb{R}^2)^+$  est un sous-groupe distingué du groupe  $\text{Isom}(\mathbb{R}^2)$ . On considere l'application

$$\det \circ \text{lin} : \phi \in \text{Isom}(\mathbb{R}^2) \mapsto \phi_0 \in \text{Isom}(\mathbb{R}^2)_0 \mapsto \det(M_{\phi_0}) \in \{\pm 1\}$$

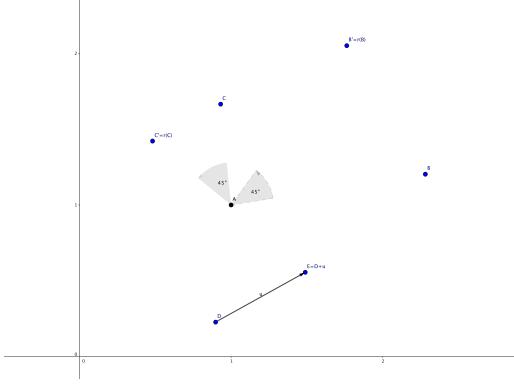


FIGURE 3. Exemple de translation, rotation ...

qui a une isométrie affine  $\phi$  associe le déterminant de la matrice de la partie linéaire de  $\phi$ . C'est un morphisme de groupe (car l'application partie linéaire l'est -Thm. 3.4- ainsi que le déterminant).  $\square$

REMARQUE 3.3. Attention !

- Le groupe  $\text{Isom}(\mathbb{R}^2)^+$  n'est pas commutatif.
- Une symétrie affine n'est pas forcément d'ordre 2.

### 3.6. Rotations affines.

THÉORÈME 3.13. Soit  $r \in \text{Isom}(\mathbb{R}^2)^+$  une rotation affine qui n'est pas une translation (sa partie linéaire n'est pas l'identité). L'ensemble  $\text{Fix}(r)$  des points fixes de  $r$  est réduit à 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

$$M = M_{r_0} = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}, \quad c^2 + s^2 = 1$$

la matrice de la partie linéaire de  $r$ ; on a  $c \neq 1$  (sinon  $M$  serait la matrice identité). Nous devons résoudre l'équation

$$(x, y) = (x_0 + cx - sy, y_0 + sx + cy)$$

ou encore

$$\begin{cases} (1-c)x + sy = x_0 \\ -sx + (1-c)y = y_0 \end{cases} \iff \begin{cases} ((1-c)^2 + s^2)x = (1-c)x_0 - sy_0 \\ ((1-c)^2 + s^2)y = (1-c)y_0 + sx_0 \end{cases} \iff \begin{cases} x = \frac{(1-c)x_0 - sy_0}{(1-c)^2 + s^2} \\ y = \frac{(1-c)y_0 + sx_0}{(1-c)^2 + s^2} \end{cases}$$

car  $(1-c)^2 + s^2 > 0$ . Le point fixe est donc unique.  $\square$

PROPOSITION 3.13. Soit  $P \in \mathbb{R}^2$  et  $\text{Isom}(\mathbb{R}^2)_P^+$  l'ensemble des rotations de centre  $P$  alors  $\text{Isom}(\mathbb{R}^2)_P^+$  est un groupe conjugué au groupe des rotations linéaires  $\text{Isom}(\mathbb{R}^2)_\mathbf{0}^+$  (en particulier ils sont isomorphes.)

Preuve: Exercice.  $\square$

**3.7. Symétries affines.** Soit  $s = t_{s(\mathbf{0})} \circ s_0$  une symétrie affine de partie linéaire  $s_0$  d'axe  $\mathbb{R}\vec{u}$  et  $\vec{v} \neq \mathbf{0}$  perpendiculaire à  $\vec{u}$ .

THÉORÈME 3.14. *L'ensemble des points fixes  $\text{Fix}(s)$  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 à l'axe  $\mathbb{R}\vec{u}$ .*

Dans ce cas  $\text{Fix}(s)$  est la droite affine

$$D_s = D(P_0, \vec{u}) = P_0 + \mathbb{R}\vec{u}$$

parallèle à 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 caractérisée uniquement par les propriétés suivantes

- Le vecteur  $\overrightarrow{Ps(P)}$  est perpendiculaire à  $\vec{u}$
- Le milieu  $\frac{1}{2}(P + s(P))$  du segment  $[P, s(P)]$  appartient à la droite  $D_s$ .

La droite  $D_s$  est l'axe de la symétrie  $s$  et  $s$  est d'ordre 2:

$$s \circ s = \text{Id.}$$

DÉFINITION 3.10. Une symétrie affine  $s$  est appelée:

- symétrie glissée si  $\text{Fix}(s) = \emptyset$ .
- symétrie orthogonale (ou axiale) si  $\text{Fix}(s)$  est une droite affine. Cette droite l'axe de la symétrie.

PREUVE. On a vu que tout point  $P$  s'écrit de manière 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 symétrie  $s = t_{s(\mathbf{0})} \circ s_0$  s'exprime de la manière suivante (cf. (3.3))

$$s(P) = s(\mathbf{0}) + P - 2 \frac{\langle P, \vec{v} \rangle}{\|\vec{v}\|^2}\vec{v} = s(\mathbf{0}) + \frac{\langle P, \vec{u} \rangle}{\|\vec{u}\|^2}\vec{u} - \frac{\langle P, \vec{v} \rangle}{\|\vec{v}\|^2}\vec{v}.$$

Résolvons l'équation

$$(3.5) \quad s(P) = P \iff s(\mathbf{0}) = 2 \frac{\langle P, \vec{v} \rangle}{\|\vec{v}\|^2}\vec{v}$$

Ainsi l'équation n'a de solution que si  $s(\mathbf{0})$  est colinéaire à  $\vec{v}$  (ie. perpendiculaire à  $\vec{u}$ ). 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

$$P = \frac{1}{2}s(\mathbf{0}) + \lambda\vec{u}, \quad \lambda \in \mathbb{R}.$$

$P$  appartient donc à la droite  $\frac{1}{2}s(\mathbf{0}) + \mathbb{R}\vec{u}$ ; reciprocement on vérifie de même que tout point de cette droite vérifie l'équation (3.5). D'autre part

$$s(P) - P = \overrightarrow{Ps(P)} = s(\mathbf{0}) - 2 \frac{\langle P, \vec{v} \rangle}{\|\vec{v}\|^2}\vec{v}$$

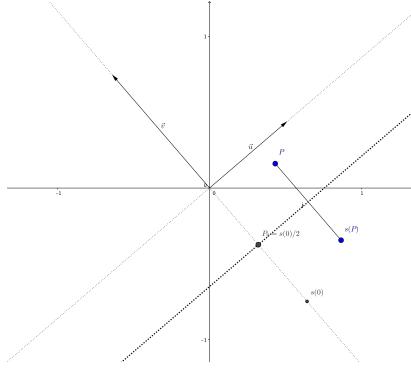
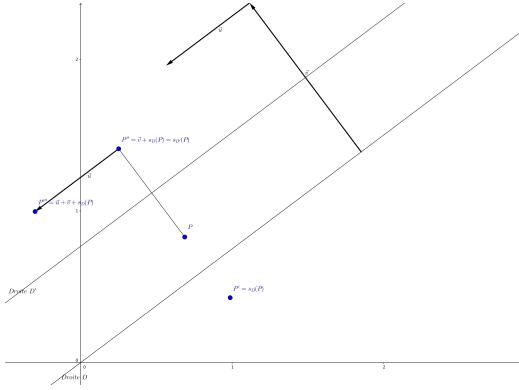


FIGURE 4. Exemple de symetrie affine axiale.

FIGURE 5. Exemple de symetrie affine glissée:  $P''' = t_{\vec{u}} \circ t_{\vec{v}} \circ s_D$ .

est proportionnel à  $\vec{v}$  donc perpendiculaire à  $\vec{u}$  et le milieu du segment  $[Ps(P)]$  vérifie bien

$$\frac{1}{2}(P + s(P)) = \frac{1}{2}s(\mathbf{0}) + P - \mu(P)\vec{v} = \frac{1}{2}s(\mathbf{0}) + \lambda(P)\vec{u} \in D\left(\frac{1}{2}s(\mathbf{0}), \vec{u}\right).$$

Compte-tenu de la caractérisation de  $s(P)$  ( $[P, s(P)]$  est perpendiculaire à  $\vec{u}$  et son milieu est sur l'axe de  $s$ ) on voit que  $s$  envoie  $s(P)$  sur  $P$  donc  $s(s(P)) = P$ .  $\square$

**COROLLAIRE 3.1.** *Une symétrie affine  $s$  se décompose sous la forme suivante:*

$$s = t' \circ s'$$

ou  $t' = t_{\vec{u}'}$  est une translation de vecteur  $\vec{u}'$  parallèle à l'axe  $\mathbb{R}\vec{u}$  de la partie linéaire de  $s$  et  $s'$  est une symétrie axiale d'axe parallèle à  $\mathbb{R}\vec{u}$ . De plus  $t'$  et  $s'$  commutent.

*La décomposition est unique et la symétrie  $s$  est glissée 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  $(\vec{u}, \vec{v})$ .  $\square$

**3.7.1. Exemple.** Considerons les deux symetries  $s_1, s_2$  par rapport aux droites d'équation:

$$3x + 4y = 2, \quad -2x + 5y = 3.$$

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 donnees par les vecteurs

$$\vec{v}_1 = (3, 4), \quad \vec{v}_2 = (-2, 5).$$

Ainsi les matrices associes sont donnees par

$$\begin{pmatrix} c_1 & s_1 \\ s_1 & -c_1 \end{pmatrix}, \quad \begin{pmatrix} c_2 & s_2 \\ s_2 & -c_2 \end{pmatrix}$$

avec

$$c_1 = \frac{7}{25}, \quad s_1 = -\frac{24}{25}, \quad c_2 = \frac{21}{29}, \quad s_2 = \frac{20}{29}.$$

Ainsi la partie lineaire de  $s_1 \circ s_2$  qui est une rotation a pour matrice

$$\begin{pmatrix} c_3 & -s_3 \\ s_3 & c_3 \end{pmatrix} \text{ avec } c_3 = c_1 c_2 + s_1 s_2 = -\frac{333}{725}, \quad s_3 = s_1 c_2 - c_1 s_2 = -\frac{644}{725}.$$

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

$$3x + 4y = 2, \quad -2x + 5y = 3$$

et on trouve

$$P = \left( \frac{-2}{23}, \frac{13}{23} \right).$$

#### 4. Conclusion

Pour resumer, les isometries du plan sont constituees des

- **translations:** les elements de  $T(\mathbb{R}^2)$ ; elles n'ont aucun point fixe sauf la translation par le vecteur **0**,
- **les rotations:** ce sont les elements de  $\text{Isom}(\mathbb{R}^2)^+$ ; elles sont composees d'une translation et d'une rotation lineaire; elle ont exactement un point fixe, le centre de la rotation.
- **les symetries axiales:** elles appartiennent a  $\text{Isom}(\mathbb{R}^2)^-$  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 point fixe est la droite parallele a l'axe de la symetrie lineaire et passant par le milieu du segment de translation.
- **les symetries glissees:** elles appartiennent a  $\text{Isom}(\mathbb{R}^2)^-$  et sont composees d'une translation et d'une symetrie lineaire telle que le vecteur de la translation n'est pas perpendiculaire a celui de l'axe de la symetrie. Elles n'ont pas de point fixe.

## CHAPITRE 4

### Isometries et nombres complexes

Nous commençons 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

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ qui verifie } I^2 = -\text{Id}_2$$

L'ensemble des nombres complexes est l'ensemble des combinaisons linéaires de  $\text{Id}$  et  $I$ , c'est à dire l'ensemble des matrices de la forme

$$Z = x\text{Id} + yI = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}, \quad x, y \in \mathbb{R}.$$

en d'autre termes

$$\mathbb{C} = \mathbb{R}\text{Id} + \mathbb{R}I \subset M_2(\mathbb{R}),$$

1.0.2. *Structure d'espace vectoriel.* C'est un  $\mathbb{R}$ -espace vectoriel de dimension 2 (engendré par la famille libre  $(\text{Id}, I)$ ): en particulier  $\mathbb{C}$  est stable par addition et multiplication par les scalaires

$$\begin{aligned} \forall Z, Z' \in \mathbb{C}, \quad Z + Z' &= \begin{pmatrix} x + x' & -y - y' \\ y + y' & x + x' \end{pmatrix} = (x + x')\text{Id} + (y + y')I \in \mathbb{C}, \\ \forall Z \in \mathbb{C}, \quad \lambda \in \mathbb{R}, \quad \lambda.Z &= \begin{pmatrix} \lambda.x & -\lambda.y \\ \lambda.y & \lambda.x \end{pmatrix} = \lambda x\text{Id} + \lambda yI \in \mathbb{C}. \end{aligned}$$

DÉFINITION 4.1. Les coordonnées de  $Z \in \mathbb{C}$  sont appelées parties réelles et imaginaire de  $Z$ :

$$Z = x\text{Id} + yI, \quad x = \text{Re}(Z), \quad y = \text{Im}(Z).$$

L'application

$$(1.1) \quad Z = x\text{Id} + yI \in \mathbb{C} \mapsto (x, y) = (\text{Re}Z, \text{Im}Z) \in \mathbb{R}^2$$

est un isomorphisme d'espace vectoriels et permet donc d'identifier  $\mathbb{C}$  avec le plan réel  $\mathbb{R}^2$ .

1.0.3. *Structure d'anneau.* Comme  $I^2 = -\text{Id} \in \mathbb{C}$  on a pour  $Z, Z' \in \mathbb{C}$

$$Z \cdot Z' = (x\text{Id} + yI) \cdot (x'\text{Id} + y'I) = (xx' - yy')\text{Id} + (xy' + x'y)I \in \mathbb{C}(\mathbb{R}).$$

Ainsi  $\mathbb{C}(\mathbb{R})$  est stable par produit. C'est donc un sous-anneau de  $M_2(\mathbb{R})$  qui est de plus commutatif:

$$\forall Z, Z' \in \mathbb{C} \quad Z \cdot Z' = Z' \cdot Z.$$

1.0.4. *Structure de corps.* Pour tout  $Z \in \mathbb{C}$ ,

$$\det(Z) = x^2 + y^2 = 0 \iff Z = \mathbf{0}.$$

Ainsi toute matrice  $Z \in \mathbb{C}$  non-nulle est inversible:  $\mathbb{C}$  est un corps. de plus pour  $Z \neq 0$  son inverse est donnee par la formule usuelle

$$(1.2) \quad Z^{-1} = (x^2 + y^2)^{-1} \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

1.0.5. *Conjugaison complexe.* Pour  $Z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathbb{C}$  la transposee de  $Z$  est encore dans  $\mathbb{C}$ :

$${}^t Z = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x\text{Id} - yI \in \mathbb{C}$$

DÉFINITION 4.2. La restriction de la transposee defini une bijection de  $\mathbb{C}$  sur  $\mathbb{C}$  (d'inverse la transposee). La restriction a  $\mathbb{C}$  de la transposition s'appelle la conjugaison complexe et se note

$$Z \in \mathbb{C} \mapsto \overline{Z} \in \mathbb{C}.$$

On a

$$\overline{\overline{Z}} = Z, \quad \overline{Z \cdot Z'} = {}^t Z \cdot Z' = {}^t Z' \cdot {}^t Z = \overline{Z'} \cdot \overline{Z} = \overline{Z} \cdot \overline{Z'}$$

et

$$Z \cdot \overline{Z} = \det(Z)\text{Id} = (x^2 + y^2)\text{Id}$$

ainsi pour  $Z \neq \mathbf{0}$

$$(1.3) \quad Z^{-1} = (x^2 + y^2)^{-1} \overline{Z}.$$

La quantite

$$\det(Z)^{1/2} = (x^2 + y^2)^{1/2} = |Z|$$

s' appelle le module de  $Z$ .

1.0.6. *Structure euclidienne.* L'ensemble des nombres complexes est muni d'un produit scalaire (bilineaire, symetrique, defini positif) donne par

$$\langle Z, Z' \rangle_{\mathbb{C}} := \text{Re}(Z \overline{Z'}) = xx' + yy'$$

et

$$\|Z\|^2 = |Z|^2 = \langle Z, Z \rangle = x^2 + y^2.$$

Ainsi l'isomorphisme (1.1) interchange les produits scalaires  $\langle \cdot, \cdot \rangle_{\mathbb{C}}$  et le produit scalaire usuel  $\langle \cdot, \cdot \rangle_{\mathbb{R}^2}$ : 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  $(\mathbb{C}, \langle \cdot, \cdot \rangle_{\mathbb{C}})$  et  $(\mathbb{R}^2, \langle \cdot, \cdot \rangle_{\mathbb{R}^2})$ .

### 1.1. Notation simplificatrice.

L'application

$$x \in \mathbb{R} \hookrightarrow x\text{Id} \in \mathbb{C}$$

est un morphisme d'anneau

$$(x + x')\text{Id} = x.\text{Id} + x'.\text{Id}, \quad (x.x')\text{Id} = x\text{Id}x'\text{Id}$$

qui est injectif ( $x\text{Id} = \mathbf{0} \iff x = 0$ ) qui donc envoie l'element neutre 1 sur la matrice identite  $\text{Id}$ : le corps des reels  $\mathbb{R}$  s'identifie 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

$$z = x + iy.$$

## 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.

*Translation.* 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  $\rho = c + is \in \mathbb{C}$ , 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

$$[\times \rho]1_{\mathbb{C}} = c + is, \quad [\times \rho]i = (c + is)i = -s + ic$$

et la matrice ce cette application dans la base  $\{1_{\mathbb{C}}, i\}$  s'ecrit

$$M_{\rho} = \begin{pmatrix} c & -s \\ s & c \end{pmatrix} = c.\text{Id} + s.I$$

(c'est a dire le nombre complexe  $\rho$  dans la notation non-simplifiee). En particulier si

$$|\rho|^2 = c^2 + s^2 = 1$$

$M_{\rho}$  est la matrice d'une isometrie de  $\text{SO}_2(\mathbb{R})$  qu'on appellera rotation de parametre complexe  $\rho$  et qu'on notera  $r_{\rho}$ .

On note

$$\mathbb{C}^1 = \{\rho = c + is, c, s \in \mathbb{R}, c^2 + s^2 = 1\}$$

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*

$$\begin{aligned} (\mathbb{C}^1, \times) &\mapsto (\text{Isom}(\mathbb{R}^2)_0^+, \circ) \\ \rho &\mapsto r_\rho \end{aligned}$$

est un isomorphisme de groupes.

*Symetries lineaires.* La conjugaison complexe est definie (en notation simplifiee) est definie par

$$z = x + iy \mapsto \bar{z} = x - iy.$$

Elle verifie

– Linearite:

$$\forall z, z' \in \mathbb{C}, \lambda \in \mathbb{R}, \overline{\lambda z + z'} = \lambda \bar{z} + \bar{z}'.$$

– Involutivite:  $\bar{\bar{z}} = z$ .

– Multiplicativite:

$$\overline{zz'} = \overline{z'}\overline{z} = \bar{z}\bar{z}'.$$

– Norme:

$$z\bar{z} = x^2 + y^2 = \|(x, y)\|^2.$$

Le nombre  $(z\bar{z})^{1/2} = (x^2 + y^2)^{1/2}$  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

$$z^{-1} = \frac{\bar{z}}{|z|^2}.$$

En particulier si  $|z| = 1$ ,

$$z^{-1} = \bar{z}.$$

– Produit scalaire

$$\text{Re}(z.\bar{z}') = xx' + yy' = \langle (x, y), (x', y') \rangle$$

– Caracterisation des nombres reels et nombres imaginaires:

$$\bar{z} = z \Leftrightarrow z = x, x \in \mathbb{R}, \bar{z} = -z \Leftrightarrow z = iy, y \in \mathbb{R}.$$

On a

$$\bar{1} = 1, \bar{i} = -i$$

et donc la matrice de cette application lineaire dans la base  $(1, i)$  est

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

Cette application  $z \mapsto \bar{z}$  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

$$s = s_{\mathbf{e}_1} \circ r \quad (\text{et } M_s = M_{s_{\mathbf{e}_1}} \times M_r).$$

On obtient ainsi que toute symetrie lineaire correspond a une unique transformation du corps des complexes de la forme

$$s_\rho : z \mapsto \overline{\rho z}, \quad \rho \in \mathbb{C}^1.$$

*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

$$h_{\rho,0} : \mathbb{R}^2 \mapsto \mathbb{R}^2$$

de centre  $\mathbf{0}$  et de rapport  $\rho$  qui est l'application 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 l'homothetie lineaire de rapport  $\lambda$ .*

La matrice de cette application lineaire est la matrice scalaire

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda \cdot \text{Id.}$$

Soit  $\gamma \in \mathbb{C}^\times$  un nombre complexe non-nul general;  $\gamma$  peut s'ecrire

$$\gamma = \lambda \cdot \rho \text{ avec } \lambda = |\gamma| \text{ le module et } \rho = \frac{\gamma}{|\gamma|}. \text{ la partie de module 1.}$$

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  $h_{\rho,0} \circ r_\rho$  de la rotation lineaire  $r_\rho$  et de l'homothetie  $h_{\lambda,0}$  de rapport  $\lambda$  et de centre  $\mathbf{0}$ .

*Homothetie 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 apelée homothetie affine de rapport  $\lambda \in \mathbb{R}^\times$ .*

REMARQUE 2.1. C'est une application affine, bijective et telle que  $\text{Fix}(h_{\lambda, \vec{u}})$  est reduit a un point sauf si  $\lambda = 1$ ; dans ce dernier car  $\text{Fix}(h_{1, \vec{u}}) = \mathbb{R}^2$  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 honothtie affine correspond a la transformation de  $\mathbb{C}$  donnee par

$$z \mapsto \lambda z + \nu, \quad \lambda \in \mathbb{R}^\times, \quad \nu \in \mathbb{C}.$$

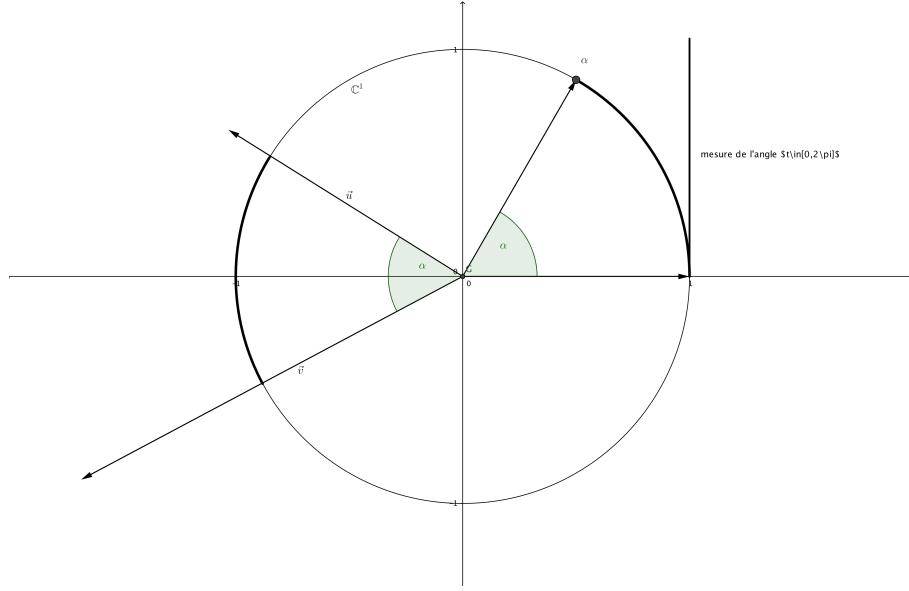


FIGURE 1. Deux paires de vecteurs representant le même angle

### Isometries generales.

THÉORÈME 4.1. *Toute isometrie  $\varphi$  de  $\mathbb{R}^2$  s'identifie à une transformation complexe de la forme*

$$r_{\rho,\nu} : z \mapsto \nu + \rho.z, \quad s_{\rho,\nu} : z \mapsto \nu + \overline{\rho}.\bar{z}$$

avec

$$\nu \in \mathbb{C}, \quad \rho = c + is \in \mathbb{C}^1 \text{ (ie. } c^2 + s^2 = 1)$$

La partie lineaire  $\varphi_0$  est donnée par

$$r_\rho = r_{\rho,0} : z \mapsto \rho, \quad s_\rho = s_{\rho,0} : z \mapsto \bar{\rho}$$

et leur matrices sont données par

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c & -s \\ s & c \end{pmatrix} = \begin{pmatrix} c & -s \\ -s & -c \end{pmatrix}.$$

Dans le premier cas  $\varphi \in \text{Isom}(\mathbb{R}^2)^+$  et dans le second  $\varphi \in \text{Isom}(\mathbb{R}^2)^-$ .

### 2.1. Angle et nombre complexes.

**2.2. Mesure d'un angle.** Un angle correspond donc à une rotation et donc à un nombre complexe de module 1,  $\alpha$ , ou encore un point sur le cercle unité. Pour des raisons pratiques, on préférera souvent représenter un angle par un nombre réel: pour cela on mesure la longueur de l'arc du cercle unité  $\mathbb{C}^1$  compris entre 1 et  $\alpha$  (ou encore la longueur de l'arc de cercle unité déterminé par les deux vecteurs  $\vec{u}, \vec{v}$ : cela nécessite de définir rigoureusement ce qu'est la longueur d'un arc de cercle ce qui implique la notion d'intégrale le long de courbe; cela sera défini rigoureusement au semestre de printemps).

Au lieu de cela, on admettra le résultat suivant de nature algébrique/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*

$$\ker \phi_1 = 2\pi\mathbb{Z} \subset \mathbb{R}$$

*ou  $\pi = 3.14159 \dots$  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'égalité de deux fonctions de la variable  $s$ :

$$s \mapsto \phi(s+t), \quad s \mapsto \phi(s)\phi(t).$$

Les dérivées en  $s$  sont donc égales: 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'interprète en disant que  $\phi(t)$  parcourt le cercle  $\mathbb{C}^1$  à vitesse constante.

Notons  $\phi_1(t) := \phi(t/\lambda)$ ; c'est un morphisme de groupe non-constant qui vérifie  $\phi'_1(0) = i$ .

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

$$\varphi'(0) = \mu^{-1}\mu - 1 = 0.$$

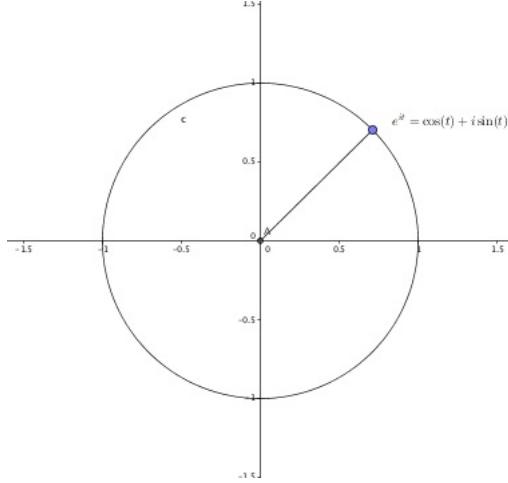


FIGURE 2. Le cercle trigonométrique

Ce morphisme est donc constant égal à 1.

□

Ainsi tout nombre complexe de module 1,  $z = x + iy$  tel que  $x^2 + y^2 = 1$ , est représenté de manière unique par un nombre réel  $t \in [0, 2\pi[$ : l'unique élément  $t$  dans cet intervalle tel que

$$z = e^{it} = \cos(t) + i \sin(t);$$

alternativement  $z$  est représenté de manière unique par le sous-ensemble de  $\mathbb{R}$  (l'ensemble des translates de  $t$  par les éléments du sous-groupe  $(2\pi\mathbb{Z}, +)$ )

$$t \pmod{2\pi} = t + 2\pi\mathbb{Z} \subset \mathbb{R}.$$

( si si  $t' \in t \pmod{2\pi}$ ,  $t' \pmod{2\pi} = t \pmod{2\pi}$ . ) Ce nombre  $t$  (ou cette classe de nombres) est appellé l'argument de  $z$  et est note  $\arg(z)$ .

Si on considère l'angle formé par les deux vecteurs  $(1, 0)$  sur  $(x, y)$ ; le paramètre complexe qui envoie le premier vecteur sur le second est précisément  $z$  qu'on identifie avec  $t$ . On parlera "d'angle de mesure  $t$ " ou par abus de langage "d'angle  $t$ ".

Ainsi dans ce langage on a le résultat tautologique suivant:

**THÉORÈME 4.3.** *Les isométries préservent les angles au sens suivant: soit  $O, A, B$  trois points avec  $A, B \neq O$  et  $t \pmod{2\pi}$  la mesure de l'angle  $\widehat{AOB}$ ; soit  $\varphi \in \text{Isom}(\mathbb{R}^2)$  et*

$$A' = \varphi(A), \quad B' = \varphi(B), \quad O' = \varphi(O);$$

- si  $\varphi \in \text{Isom}(\mathbb{R}^2)^+$  alors la mesure de l'angle  $\widehat{A'O'B'}$  vaut  $t$ ;
- si  $\varphi \in \text{Isom}(\mathbb{R}^2)^-$  alors la mesure de l'angle  $\widehat{A'O'B'}$  vaut  $2\pi - t = -t \pmod{2\pi}$ .

Cette paramétrisation 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 paramètre réel dans  $[0, 2\pi[$  est plus petit que celui de l'autre angle; on peut également parler de secteur angulaire par rapport à un segment orienté  $[P, Q]$  associé à un intervalle  $I \subset [0, 2\pi[$  comme étant l'ensemble des points  $R$  du plan tel que le paramètre réel associé à l'angle  $\widehat{QPR}$  appartienne à l'intervalle  $I$ .

2.2.1. *Trigonometrie.* En peut également en deduire les propriétés 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 propriétés suivantes*

(1) *Elles ont les expressions suivantes*

$$\cos(t) = \operatorname{Re}(e^{it}) = \frac{e^{it} + e^{-it}}{2}, \quad \sin(t) = \operatorname{Im}(e^{it}) = \frac{e^{it} - e^{-it}}{2};$$

(2) *elles sont périodiques de période  $2\pi$ :*

$$\cos(t + 2\pi k) = \cos(t), \quad \sin(t + 2\pi k) = \sin(t);$$

(3)  *$\cos(t)$  est paire et  $\sin(t)$  est impaire.*

(4) *elles sont dérivables et vérifient*

$$\cos'(t) = -\sin(t), \quad \sin'(t) = \cos(t);$$

(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  $t$ ,*

$$\cos(\pi - t) = -\cos(t), \quad \sin(\pi - t) = \sin(t)$$

*de sorte que  $\cos(t)$  et  $\sin(t)$  sont déterminées par leur restriction à 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 première est strictement décroissante et la seconde strictement croissante.*



## CHAPITRE 5

# Groupes finis d'isometries et polygones reguliers

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 que l'on a deja etudies un peu et les groupe dihedraux que l'on discute maintenant d'un point de vue abstrait.

### 1. Groupes dihedraux

On rappelle qu'un groupe fini  $G$  est cyclique si il est engendre par un element

$$G = \langle r \rangle = r^{\mathbb{Z}} = \{e_G, r, r^2, \dots, r^{n-1}\}$$

ou

$$n = |G| = \text{ord}(r) \geqslant 1$$

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 1.1.** 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.

**PROPOSITION 5.1.** *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  $s' \in G^-$ ,*

$$s'rs'^{-1} = r^{-1}, \quad G^- = s'G^+ = G^+.s', \quad G^+ = s'G^- = G^-.s'.$$

*Deux groupes dihedraux de meme ordre sont isomorphes.*

On designera par  $\mathcal{D}_{2n}$  un groupe dihederal d'ordre  $2n$  pris a isomorphisme pres.

**PREUVE.** Comme  $r, s$  engendrent  $G$ , tout élément de  $G$  est de la forme

$$g = r^{k_1} s^{l_1} r^{k_2} \cdots s^{l_p} \cdots r^{k_p} s^{l_p}, \quad k_1, l_1, \dots, k_p, l_p \in \mathbb{Z}.$$

de plus comme  $s^2 = e_G$  on peut supposer que les  $l_i$  valent tous 1 (si  $g$  n'appartient pas à  $G^+$  car alors  $g = r^k$ ). Mais on a

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

donc si  $g \notin G^+$  on peut toujours supposer que  $g$  est de la forme

$$sr^k.$$

Cela montre que  $G = G^+ \cup G^-$ . Supposons que  $g \in G^+ \cap G^-$  alors  $g = r^k = sr^{k'}$  et  $s = r^{k-k'} \in G^+$  ce qui est absurde car on a supposé que  $s \notin G^+$  ainsi  $G^+ \cap G^- = \emptyset$ .

Cela implique que  $|G| = |G^+| + |G^-| = 2|G^+|$  car  $|G^-| = |sG^+| = |G^+|$ .

Soit  $s' \in G^-$ , alors  $s' = sr^k$  et  $(s')^2 = sr^k sr^k = r^{-k} r^k = e_G$ , on a également

$$s'rs'^{-1} = sr^k rr^{-k} s^{-1} = srs^{-1} = r^{-1}.$$

Cette relation montre également que  $G^+$  est distingué dans le générateur  $r$  de  $G^+$  est envoyé dans  $G^+$  par conjugaison.

On démontre les autres identités de la même manière.

Soient  $G = \langle r, s \rangle$  et  $G' = \langle r', s' \rangle$  de groupes diédraux de même ordre ( $|G| = |G'|$ ) alors  $|G| = |G'| = 2|G^+| = 2|G'^+|$  donc  $r$  et  $r'$  sont de même ordre, disons  $n$ . Tout élément de  $G$  s'écrit de manière unique sous la forme

$$g = r^k \text{ ou } g = sr^k, \quad 0 \leq k \leq n-1.$$

Posons

$$\begin{array}{ccc} G & \mapsto & G' \\ r^k, sr^k & \mapsto & (r')^k, s'(r')^k \end{array}$$

alors  $\phi$  est une bijection et on vérifie que c'est un morphisme de groupes: il est clair que le morphisme  $\phi$  restreint à  $G^+$  est un isomorphisme de groupes de  $G^+$  vers  $G'^+$ , pour le reste on a que

$$\begin{aligned} \phi(sr^k) &= \phi(s)\phi(r)^k \\ \phi(sr^k \cdot sr^{k'}) &= \phi(r^{-k}r^{k'}) = \phi(r)^{-k+k'} = \phi(sr^k)\phi(sr^{k'}) \\ \phi(r^{k'}sr^k) &= \phi(ssr^{k'}sr^k) = \phi(sr^{k-k'}) = s'(r')^{k-k'} = \phi(r^{k'})\phi(sr^k). \end{aligned}$$

□

## 2. Classification des sous-groupes finis d'isométries

Dans cette section, on classe les sous-groupes finis d'isométries du plan. On va montrer qu'un groupe fini d'isométries est soit un groupe cyclique, soit un groupe diédral.

**THÉORÈME 5.1.** *Soit  $G \subset \text{Isom}(\mathbb{R}^2)$  un sous-groupe fini d'isométries. Alors*

- $G$  est soit cyclique soit diédral.
- Si on note  $G^+ = G \cap \text{Isom}(\mathbb{R}^2)^+$  (le sous-groupe des rotations de  $G$ ) alors  $G^+$  est cyclique et distingué dans  $G$ .  $G$  est cyclique si et seulement si  $G = G^+$ .
- $G$  (resp.  $G^+$ ) est conjugué à un sous-groupe fini du groupe des isométries linéaires  $\text{Isom}(\mathbb{R}^2)_0$  (resp.  $\text{Isom}(\mathbb{R}^2)_0^+$ ).

On commence par montrer la

**PROPOSITION 5.2.** *Soit  $G \subset \text{Isom}(\mathbb{R}^2)$  un sous-groupe fini alors il existe un point  $P = P(G) \in \mathbb{R}^2$  qui est fixe pour tous les éléments de  $G$ .*

**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 différentes images de  $Q$  par les éléments de  $G$  pour les poids uniformes  $|G|^{-1}$ . Soit  $\psi \in G$  alors  $\psi$  préserve le barycentre:  $\psi(P)$  est le barycentre des points  $\{\psi(\varphi(Q))\}_{\varphi \in G}$  et 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

$$G_0 = \text{Ad}(t_{-P})(G) = t_{-P} \circ G \circ t_P$$

le groupe conjugué 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  $G_0 \subset \text{Isom}(\mathbb{R}^2)_0$ .

Quitte à remplacer  $G$  par le groupe isomorphe  $G_0$ , on peut donc supposer que  $G \subset \text{Isom}(\mathbb{R}^2)_0$ .

Soit

$$G^+ = G \cap \text{Isom}(\mathbb{R}^2)_0^+;$$

c'est un sous-groupe des rotations linéaires de  $G$ ; soit  $n$  son ordre. Interprétées en terme de nombres complexes,  $G^+$  correspond à un sous-groupe fini du groupe  $\mathbb{C}^1$  des nombres complexes de module 1

$$(\{\alpha_1, \dots, \alpha_n\}, \times) \subset (\mathbb{C}^1, \times).$$

**THÉORÈME 5.2.** *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 égal à l'ensemble*

$$\mu_n = \{\alpha \in \mathbb{C}, \alpha^n = 1\}$$

des racines  $n$ -ièmes de l'unité: les racines complexes du polynôme  $X^n - 1$ . En particulier le groupe  $\mu_n$  est l'unique sous-groupe de  $\mathbb{C}^\times$  d'ordre  $n$ .

On rappelle le

**THÉORÈME 5.3** (Théorème de Lagrange). *Soit  $(G, \cdot)$  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 également besoin du lemme suivant

**LEMME 5.1.** *Soit  $G$  un groupe commutatif et  $g, h \in G$  des éléments d'ordre  $m$  et  $n$ , alors le sous-groupe  $\langle g, h \rangle$  contient un élément  $k$  d'ordre exactement  $[m, n]$ .*

PREUVE. Supposons que  $(m, n) = 1$  alors  $[m, n] = mn$  et prenons  $k = g.h$ ; on a

$$(g.h)^{mn} = (g^m)^n \cdot (h^n)^m = e_G$$

donc  $\text{ord}(g.h)|mn$ . 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 Théorème de Lagrange, et donc  $e|(m, n) = 1$ . Ainsi

$$g^d = g' = e_G$$

donc  $m|d$ ; de même  $n|d$  donc  $mn|d$  car  $(m, n) = 1$ . Ainsi  $mn|d$  et  $gh$  est d'ordre  $mn$ .

En général, il existe  $m'|m$  et  $n'|n$  tel que  $m'n' = [m, n]$  et  $(m', n') = 1$ . Rappelons que si on décompose  $m$  et  $n$  en produit de nombres premiers on a

$$m = \prod_p p^{\alpha_p}, \quad n = \prod_p p^{\beta_p}, \quad [m, n] = \prod_p p^{\max(\alpha_p, \beta_p)}, \quad (m, n) = \prod_p p^{\min(\alpha_p, \beta_p)}.$$

On définit alors

$$m' = \prod_{\substack{p \\ \alpha_p \geq \beta_p}} p^{\alpha_p}, \quad n' = \prod_{\substack{p \\ \beta_p > \alpha_p}} p^{\beta_p}.$$

Ces entiers sont premiers entre eux car les conditions  $\alpha_p \geq \beta_p$  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 décomposition sont inférieurs ou égaux à ceux des décompositions de  $m$  et  $n$  et enfin on a

$$[m, n] = \prod_p p^{\max(\alpha_p, \beta_p)} = \prod_{\substack{p \\ \alpha_p \geq \beta_p}} p^{\alpha_p} \prod_{\substack{p \\ \alpha_p < \beta_p}} p^{\beta_p} = m'n'.$$

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  $g$ .

Comme  $(m', n') = 1$  le produit  $g'.h'$  est d'ordre  $m'n'$ .  $\square$

**2.0.2. Preuve du Théorème 5.4.** Soit  $G \subset \mathbb{C}^\times$  un groupe fini d'ordre  $n$ . Par le théorème 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  $G \subset \mu_n$  et donc  $n \leq |\mu_n|$ . Comme  $|\mu_n| \leq n$  on a  $n = |\mu_n|$  et

$$G = \mu_n.$$

Montrons que  $G$  est cyclique: soit  $\alpha \in G$  un élément 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. Comme  $n_\alpha \leq n$  il suffit de montrer que  $n_\alpha \geq n$ . Soit  $\beta$  un autre élément de  $G$  d'ordre  $n_\beta$ , alors, par le lemme 5.1, il existe dans  $G$  un élément  $\gamma$  d'ordre  $[n_\alpha, n_\beta]$ ;

mais si  $n_\beta \nmid n_\alpha$ , alors  $[n_\alpha, n_\beta]$  est  $> n_\alpha$  ce qui contredit par maximalite de  $n_\alpha$ , on en deduit que

$$\forall \beta \in G, \quad n_\beta \mid n_\alpha.$$

Ainsi tout element de  $G$  est d'ordre divisible par  $n_\alpha$ : en particulier

$$\forall \beta \in G \subset \mathbb{C}^\times, \quad \beta^{n_\alpha} - 1 = 0.$$

Le nombre de racines distinctes du polynome  $X^{n_\alpha} - 1$  est  $\leq n_\alpha$  donc  $n = |G| \leq n_\alpha$  et donc

$$|G| = n = n_\alpha \text{ et } G = \alpha^{\mathbb{Z}} = \mu_n$$

est cyclique d'ordre  $n$ . □

**REMARQUE 2.1.** 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  $\leq n$ . On a en fait le resultat plus general suivant:

**THÉORÈME 5.4.** *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*

$$\mu_n(K) = \{\alpha \in K^\times, \quad \alpha^n = 1_K\}.$$

2.0.3. *Fin de la preuve du Théorème 5.1.* Soit  $G \subset \text{Isom}(\mathbb{R}^2)_0$  un groupe fini et

$$G^+ = G \cap \text{Isom}(\mathbb{R}^2)_0^+, \quad G^- = G \cap \text{Isom}(\mathbb{R}^2)_0^-$$

et soit  $n$  l'ordre de  $G^+$ ; on viens de montrer que  $G^+ = \langle r_\alpha \rangle$  est cyclique engendre par une rotation  $r = r_\alpha$  de parametre complexe  $\alpha$  un generateur de  $\mu_n$ . Si  $G^+ = G$ ,  $G$  est cyclique comme annonce.

Sinon, soit  $s \in G^- = G \cap \text{Isom}(\mathbb{R}^2)_0^-$  alors  $s$  est d'ordre 2; calculons  $s \circ r_\alpha \circ s^{-1}$ : en posant  $s = s_\beta$ , on trouve que

$$s_\beta \circ r_\alpha \circ s_\beta^{-1} = s_\beta \circ r_\alpha \circ s_\beta = r_{\bar{\beta} \cdot \bar{\alpha} \cdot \beta} = r_{\bar{\alpha} \bar{\beta} \cdot \beta} = r_{\alpha^{-1}} = r^{-1}$$

car

$$\alpha^{-1} = \bar{\alpha} \text{ et } \beta^{-1} = \bar{\beta}.$$

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  $\alpha, \beta, \gamma \in \mathbb{C}^1$

$$r_\gamma \circ r_\alpha \circ r_\gamma^{-1} = r_\alpha, \quad r_\gamma \circ s_\beta \circ r_\gamma^{-1} = s_{\bar{\gamma}^2 \beta};$$

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 5.3.** *Tout sous-groupe fini de  $\text{Isom}(\mathbb{R}^2)$  est conjugue (par une rotation affine) a un sous-groupe d'un groupe dihederal de la forme*

$$\{r_\alpha, \quad s_1 \circ r_\alpha, \quad \alpha \in \mu_n\}.$$

## 2.1. Existence de sous-groupes cycliques.

THÉORÈME 5.5. *Pour tout  $n \geq 1$ , il existe dans  $\text{Isom}(\mathbb{R}^2)_0$  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  $n \geq 1$

$$\mu_n = \{\alpha \in \mathbb{C}, \alpha^n = 1\},$$

est d'ordre  $n$  exactement. Comme'est l'ensemble des racines du polynome  $X^n - 1$  et egale-ment 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  $\leq n$  et cyclique en vertu des resultats precedents. On a par le theoreme fondamental de l'algebre

$$X^n - 1 = \prod_{\alpha \in \mu_n} (X - \alpha)^{\mu(\alpha)}, \text{ avec } \mu(\alpha) \geq 1.$$

On a  $\sum_{\alpha} \mu(\alpha) = 1$ . Supposons que  $\mu(\alpha_0)$  soit  $\geq 2$  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  $s_1^2 = \text{Id}_{\mathbb{C}}$  et

$$s_1 r_{\alpha} s_1 : z \mapsto \overline{\alpha \bar{z}} = \overline{\alpha z} = \alpha^{-1} z = r_{\alpha}^{-1}(z).$$

Ainsi le groupe endrendre par  $r_{\alpha}$  et  $s_1$  est dihedral d'ordre  $2n$ .

Soit  $r$  un rotation qui n'appartient pas 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.  $\square$

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 2.2. 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; il existe un corps  $\overline{\mathbb{F}_p}$  contenant  $\mathbb{F}_p$  et verifiant le Theoreme Fondamental de l'Algebre (ie. tout polynome a coefficients dans  $K$  se decompose en produit de facteurs lineaires) tel que

$$\mu_p = \{z \in \overline{\mathbb{F}_p}^\times, z^p = 1_{\mathbb{F}_p}\} = \{1_{\mathbb{F}_p}\} !$$

En effet, on a (binôme 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

$$C_p^k (-1_{\mathbb{F}_p})^{p-k} = q \times p \cdot 1_{\mathbb{F}_p} (-1_{\mathbb{F}_p})^{p-k} = 0_{\mathbb{F}_p}$$

de sorte que

$$(X - 1_{\mathbb{F}_p})^p = X^p - 1_{\mathbb{F}_p}$$

et  $1_{\mathbb{F}_p}$  est la seule racine de  $X^p - 1_{\mathbb{F}_p}$ .



## CHAPITRE 6

### Polygones reguliers

Dans ce chapitre, on va utiliser la classification des groupes finis d'isométries pour étudier les polygones réguliers du plan. Commençons par définir un polygone.

#### 1. Polygones généralisés et polygones réguliers

**DÉFINITION 6.1.** Soit  $n \geq 3$  un entier, un polygone généralisé à  $n$  cotés  $\mathbf{P} \subset \mathbb{R}^2$  est une réunion de segments (appelés cotés du polygone) de la forme

$$\mathbf{P} = \bigcup_{i=1 \dots n} [P_i P_{i+1}]$$

avec

$$P_1, \dots, P_n, \quad P_{n+1} = P_1$$

un ensemble de  $n$  points **distingués** du plan (qu'on appelle sommets du polygone et on notera  $\Sigma$  l'ensemble des sommets), tels que deux cotés consécutifs ne sont pas alignés. On notera

$$\mathbf{P} = [P_1 \dots P_n].$$

En séance d'exercices on a vu une notion de polygone un peu plus restrictive:

**DÉFINITION 6.2.** Un polygone à  $n$  cotés est un polygone généralisé

$$\mathbf{P} = \bigcup_{i=1 \dots n} [P_i P_{i+1}]$$

avec  $P_{n+1} = P_1$  tel que deux cotés ne se coupent que s'ils sont consécutifs; ils se coupent alors en un seul point (le sommet bordant les deux cotés). Un polygone à 3 cotés est un triangle, à 4 un quadrilatère etc... Un triangle rectangle est un triangle dont deux cotés sont perpendiculaires. Un parallélogramme est un quadrilatère  $[PQRS]$  tel que les paires  $([PQ], [RS])$  et  $([QR], [SP])$  sont parallèles, etc...

Si un polygone généralisé n'est pas un polygone on dit qu'il est "croisé". Rappelons également

**DÉFINITION 6.3.** Soit  $\mathbf{P} \subset \mathbb{R}^2$  un sous-ensemble de  $\mathbb{R}^2$ , le groupe d'isométries de  $\mathbf{P}$  est l'ensemble

$$\text{Isom}(\mathbb{R}^2)_{\mathbf{P}} = \{\varphi \in \text{Isom}(\mathbb{R}^2), \quad \varphi(\mathbf{P}) = \mathbf{P}\}.$$

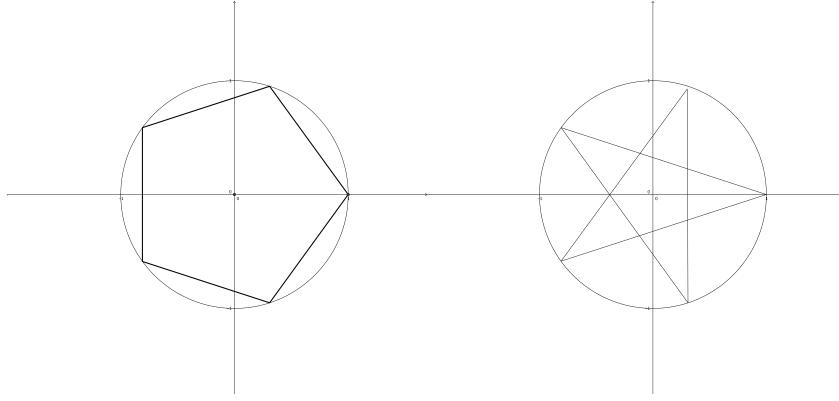


FIGURE 1. Pentagone régulier et pentagone régulier généralisé.

**THÉORÈME 6.1.** *Soit  $\mathbf{P}$  un polygone généralisé alors son groupe d'isométries est fini; il est donc cyclique ou bien diédral. Un centre de  $\text{Isom}(\mathbb{R}^2)_{\mathbf{P}}$  est le barycentre des sommets de  $\mathbf{P}$ .*

**PREUVE.** Considerons un cote  $[P_i, P_{i+1}]$ ; si  $\varphi$  est une isométrie préservant  $\mathbf{P}$  alors le segment

$$\phi([P_i, P_{i+1}]) = [\phi(P_i), \phi(P_{i+1})]$$

est un autre cote  $[P_{i'}, P_{i'+1}]$  (il est contenu dans un autre cote  $[P_{i'}, P_{i'+1}]$  et si il était strictement contenu dedans le cote originel  $[P_i, P_{i+1}]$  serait contenu strictement dans le segment  $[\phi^{-1}(P_{i'}), \phi^{-1}(P_{i'+1})] \subset \mathbf{P}$  contredisant le fait que  $[P_i, P_{i+1}]$  est un cote). Ainsi chaque élément du groupe des isométries de  $\mathbf{P}$  induit une bijection de l'ensemble des sommets de  $\mathbf{P}$ ,  $\Sigma_{\mathbf{P}}$  et on dispose d'un morphisme de groupes

$$\text{Isom}(\mathbb{R}^2)_{\mathbf{P}} \hookrightarrow \mathfrak{S}(\Sigma_{\mathbf{P}}).$$

ce morphisme est injectif: supposons que  $\phi$  induise l'identité sur  $\Sigma_{\mathbf{P}}$ :  $\forall P_i, \sigma(P_i) = P_i$  et soit  $P_i, P_j, P_k$  trois points non-alignés: alors les droites distinctes  $(P_i, P_j)$   $(P_i, P_k)$  sont des droites de points fixes pour  $\phi$  et par la classification des points fixes des différentes isométries la seule possibilité est que  $\phi = \text{Id}_{\mathbb{R}^2}$ .

Ainsi  $\text{Isom}(\mathbb{R}^2)_{\mathbf{P}}$  est fini (il s'injecte dans un groupe fini).

Soit  $\text{Bar}(\Sigma(\mathbf{P}))$  le barycentre des sommets de  $\mathbf{P}$ , et  $\phi \in \text{Isom}(\mathbb{R}^2)_{\mathbf{P}}$  alors comme  $\phi$  est affine

$$\phi(\text{Bar}(\Sigma(\mathbf{P}))) = \phi\left(\frac{1}{|\Sigma(\mathbf{P})|} \sum_{P \in \Sigma(\mathbf{P})} P\right) = \frac{1}{|\Sigma(\mathbf{P})|} \sum_{P \in \Sigma(\mathbf{P})} \phi(P) = \text{Bar}(\Sigma(\mathbf{P}))$$

car  $\phi$  induit une permutation de  $\Sigma(\mathbf{P})$ . ainsi le barycentre des sommets de  $\mathbf{P}$  est un point fixe du groupe des isométries.  $\square$

**DÉFINITION 6.4.** *Un polygone généralisé (croisé ou pas)  $\mathbf{P}$  a n cotes est régulier si ses cotes sont de même longueur et si les angles formés par deux cotes consécutives orientées  $\overrightarrow{P_i P_{i+1}}$  et  $\overrightarrow{P_{i+1} P_{i+2}}$  sont égaux (pour  $i = n - 1$ , on pose  $P_n = P_0$ ,  $P_{n+1} = P_1$ ).*

## 2. Existence des polygones (generalises) reguliers

THÉORÈME 6.2. Soit  $G^+ \subset \text{Isom}(\mathbb{R}^2)^+$  un groupe fini de rotations d'ordre  $n \geq 3$  et  $r$  un générateur 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 généralisé de sommets

$$P_0 = P, P_1 = r(P), P_2 = r^2(P) = r(P_1), \dots, P_{n-1} = r^{n-1}(P), P_n = r^n(P) = P$$

est régulier; ses sommets sont situés sur le cercle centre en  $P_r$  et de rayon  $d(P_r, P)$  et le barycentre des. Par ailleurs son groupe de symétries est le groupe diédral d'ordre  $2n$

$$G = \langle r, s \rangle$$

engendré par  $r$  et  $s$  où  $s$  est la symétrie axiale d'axe la droite  $(P_r, P)$ .

PREUVE. On a

$$r([P_k, P_{k+1}]) = [r(P_k), r(P_{k+1})] = [P_{k+1}, P_{k+2}]$$

donc la rotation  $r$  envoie un côté sur le côté suivant (car  $P_{n+1} = P$  et  $P_{n+2} = P_1$ ), donc  $r$  préserve  $\mathbf{P}$  et  $r^\mathbb{Z} = G^+$  également.

Soit  $s$  la symétrie d'axe  $(P_r, P)$ . Montrons qu'elle préserve  $\mathbf{P}$ . Puisque cette symétrie préserve  $P_r$ ,  $\text{Ad}(s)(r)$  a également  $P_r$  comme point fixe et si  $r_\alpha$  et  $s_\beta$  désignent les parties linéaires de  $r$  et  $s$  ( $\alpha, \beta \in \mathbb{C}^1$ ), la partie linéaire de  $\text{Ad}(s)(r)$  est égale à

$$s_\beta r_\alpha s_\beta^{-1} : z \mapsto \overline{\beta(\alpha \bar{\beta} z)} = \bar{\alpha} z = \alpha^{-1} z = r_\alpha^{-1}(z).$$

Ainsi comme le centre et les parties linéaires coïncident, on a

$$srs^{-1} = r^{-1} \text{ et donc } sr^k s^{-1} = r^{-k}$$

On a ainsi (car  $s(P) = P$ )

$$s(P_k) = s(r^k(P)) = r^{-k}(s(P)) = r^{-k}(P) = P_{n-k}$$

et donc le segment  $[P_k, P_{k+1}]$  est envoyé sur le segment

$$[P_{n-k-1}, P_{n-k}]$$

et  $s$  préserve donc  $\mathbf{P}$ . Ainsi le groupe  $\langle r, s \rangle$  engendré par  $r$  et  $s$  préserve  $\mathbf{P}$  et c'est un groupe diédral d'ordre  $2n$ .

On sait que  $\text{Isom}(\mathbb{R}^2)_{\mathbf{P}}$  est fini et on a vu qu'il contient le groupe diédral  $\langle r, s \rangle$ . Il suffit de montrer que

$$\text{Isom}(\mathbb{R}^2)_{\mathbf{P}}^+ = G^+.$$

Soit  $r' \in \text{Isom}(\mathbb{R}^2)_{\mathbf{P}}^+$  alors  $r'$  a le même 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'identité et  $r' = r^k$ . On a donc montrer que  $\text{Isom}(\mathbb{R}^2)_{\mathbf{P}} = \langle r, s \rangle = G$ .

Montrons que  $\mathbf{P}$  est régulier.

Soit

$$r' = t_{-P_r} \circ r \circ t_{P_r}$$

le conjugué de  $r$  par la translation  $t_{P_r}$ . La rotation  $r'$  est linéaire et engendre le groupe conjugué de rotations linéaire  $G'^+ = \text{Ad}(t_{-P_r})(G^+)$ . soit  $P' = t_{-P_r}(P) = P - P_r$  le translate de  $P$  alors le polygone  $\mathbf{P}'$  de sommets

$$P'_0 = P', P'_1 = r'(P'), P'_2 = r'^2(P') = r'(P'_1), \dots, P'_{n-1} = r'^{n-1}(P'), P'_n = r'^n(P') = P'$$

est le translate

$$\mathbf{P}' = -P_r + \mathbf{P}.$$

Quitte à remplacer  $\mathbf{P}$  par  $\mathbf{P}'$  on peut supposer que  $G^+$  est un groupe de rotations linéaires et que  $r = r_\alpha$  est linéaire de paramètre complexe  $\alpha \in \mathbb{C}^1$ . Alors  $\alpha$  est un générateur du groupe des racines  $n$ -ièmes de l'unité  $\mu_n$ .

Soit  $z \in \mathbb{C}$  correspondant à  $P$  alors  $z \neq 0$  et les complexes correspondant aux sommets de  $\mathbf{P}$  sont

$$P_0 = z, P_1 = \alpha z, \dots, P_{n-1} = \alpha^{n-1} z$$

et les cotes consécutifs  $\overrightarrow{P_k P_{k+1}}$ ,  $k \geq 0$  sont données par les différences  $\alpha^{k+1} z - \alpha^k z = \alpha^k (\alpha - 1) z$ ,  $k \geq 0$ .

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

$$\vec{P}_{k+1} P_k = \alpha^k (1 - \alpha) z, \quad \vec{P}_{k+1} \vec{P}_{k+2} = \alpha^{k+1} (\alpha - 1) z = -\alpha \cdot \alpha^k (1 - \alpha) z$$

et l'angle entre ces deux vecteurs (de même longueur) est le quotient de ces deux nombres complexes

$$\widehat{P_k P_{k+1} P_{k+2}} = \frac{-\alpha \cdot \alpha^k (1 - \alpha) z}{\alpha^k (1 - \alpha) z} = -\alpha$$

qui est constant.

□

**THÉORÈME 6.3.** *Reciproquement tout polygone généralisé régulier est obtenu de cette manière.*

On déduit de ce résultat et du Théorème précédent

**COROLLAIRE 6.1.** *Le groupe d'isométries d'un polygone généralisé régulier  $\mathbf{P}$  à  $n$  cotés est diédral d'ordre  $2n$ , engendré par une rotation centrale au barycentre de  $\mathbf{P}$  d'ordre  $n$  et par la symétrie axiale passant par un sommet de  $\mathbf{P}$  et le barycentre.*

**Preuve:** Soit

$$\mathbf{P} = [P_0, \dots, P_{n-1}, P_n = P_0] \subset \mathbb{C}$$

un polygone généralisé régulier,  $\{z_0, \dots, z_{n-1}\}$  les  $n$  nombres complexes distincts correspondants aux sommets de  $\mathbf{P}$  et (posant  $z_n = z_0$ ,  $z_{n+1} = z_1$ ) soient

$$\{\omega_k = z_{k+1} - z_k, k = 0 \dots n-1\}$$

les nombres complexes correspondant aux cotés

$$\{\overrightarrow{P_k P_{k+1}}, k = 0, \dots, n-1\};$$

par définition, l'angle  $\widehat{P_k P_{k+1} P_{k+2}}$  est constant: notons le  $-\alpha \in \mathbb{C}^1$ . 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

$$z'_k = z_k - b, \quad k = 0 \dots n$$

on voit que

$$z'_k = \alpha^k z'_0 = r_{\alpha,0}(z'_0)$$

est obtenu en appliquant à  $z'_0$  la rotation centree en 0 d'angle  $\alpha$   $k$ -fois; ainsi le polygone  $\mathbf{P}' = [z'_0, \dots, z'_{n-1}]$  est de la forme requise et  $\mathbf{P}$  est son translate par  $b$  et ses sommets sont obtenu en appliquant les rotations centrees en  $b$  et d'angles  $\alpha^k$ . □

**REMARQUE 2.1.** Supposons (quitte à faire une translation et une rotation) que  $\mathbf{P}$  a pour barycentre l'origine et que  $P$  correspond à  $x$  un nombre réel  $> 0$ . Avec les notation précédentes  $r = r_\alpha$  avec  $\alpha \in \mu_n$  un generateur et  $s = s_1$ . Notons que les isométries préservant  $\mathbf{P}$  sont les rotations

$$r_1 = \text{Id}_{\mathbb{R}^2}, \quad r_\alpha, \dots, r_{\alpha n-1}$$

et les symétries

$$s_1, \quad r_\alpha s_1, \dots, r_{\alpha n-1} s_1.$$

On a

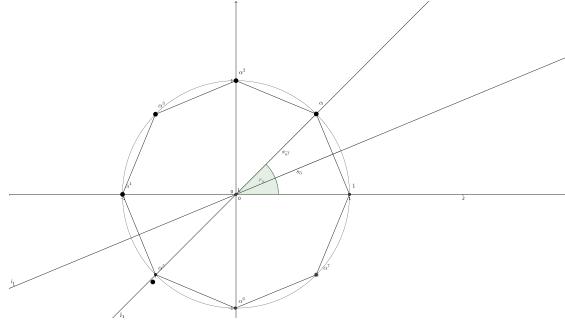
$$r_{\alpha^k} s_1 = s_{\alpha^{-k}}$$

et la symétrie  $s_{\alpha^{-k}}$  est la symétrie par rapport à la droite  $\mathbb{R}\beta^k$  avec  $\beta$  vérifiant

$$\beta^2 = \alpha.$$

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.

FIGURE 2. La rotation  $r_\alpha$  et les symétries  $s_{\bar{\alpha}}$  et  $s_{\bar{\alpha}^2}$ .

### 3. Polygones constructibles à la règle et au compas

On sait depuis la petite enfance construire sur une feuille, plusieurs polygones réguliers comme le triangle équilatéral, le carré, l'hexagone voire, (si on a été assidu) le pentagone, l'octogone (8 cotés), le décagone (10 cotés) et même le dodécagone (12 cotés). En revanche, même les enfants très assidus n'ont jamais appris construire un heptagone (7 cotés), ni un enneagone (9 cotés) ou un triskaïdecagone (13 cotés). On va expliquer pourquoi.

Cette question est également intimement liée au fait qu'en trigonométrie 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 éventuellement 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** (Constructibilité à la règle et au compas). *Soit  $P_0 = (0, 0)$  et  $P_1 = (1, 0)$ . Un point  $P$  du plan est constructible à la règle et au compas à partir d'un ensemble fini de points  $\mathcal{P}_n = \{P_0, P_1, \dots, P_n\}$  contenant  $P_0$  et  $P_1$  si  $P$  est obtenu soit*

- comme l'intersection de deux droites passant chacune par deux points distincts de  $\{P_0, P_1, \dots, P_n\}$
- de l'intersection d'une droite passant par deux points distincts de  $\{P_0, \dots, P_n\}$  et d'un cercle dont le centre est contenu dans  $\{P_0, P_1, \dots, P_n\}$  et le rayon est égal à la distance  $|P_i P_j|$  pour  $0 \leq i, j \leq n$ .
- de l'intersection de deux cercles centres en des éléments de  $\mathcal{P}_n$  et de rayons  $|P_i P_j|$  et  $|P_k P_l|$ .
- Un point  $P$  est constructible à la règle et au compas si il existe un ensemble de points  $\{P_0, P_1, \dots, P_n, P_{n+1}\}$  avec  $P_{n+1} = P$  tel que pour tout  $i \geq 2$ ,  $P_i$  soit constructible à la règle et au compas à partir de  $\{P_0, P_1, \dots, P_{i-1}\}$ .

Identifiant le plan  $\mathbb{R}^2$  à  $\mathbb{C}$ , on a

**DÉFINITION 6.5.** *Un nombre complexe  $z = x + iy$  est constructible à la règle et au compas si et seulement si le point  $P = (x, y)$  l'est.*

Notons que

- Tout entier relatif est constructible,
- tout nombre rationnel est constructible (Théorème de Thales -cf. ci-dessous)
- $\sqrt{2}$  et plus généralement toute racine carrée d'un nombre rationnel est constructible.

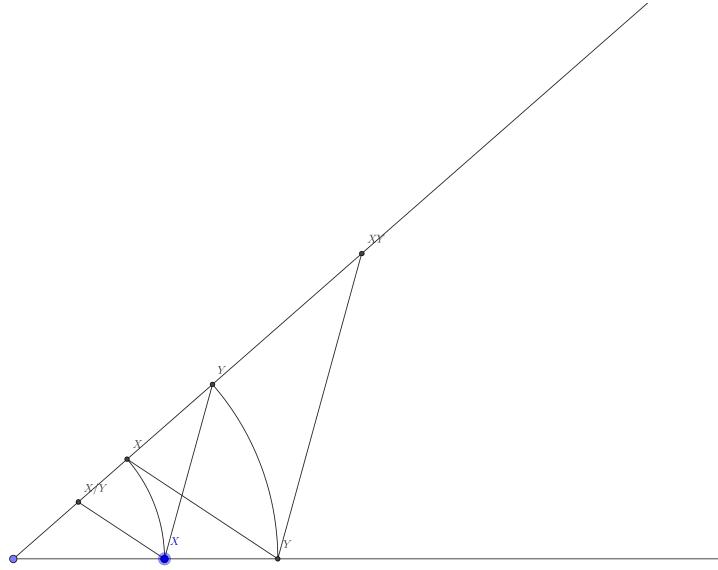


FIGURE 3. Par Thales  $XY$  et  $X/Y$  sont constructibles si  $X$  et  $Y$  le sont.

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

$$z = x + iy \in \mathbb{C} \text{ est constructible si et seulement si } x \text{ et } y \text{ le sont.}$$

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:  $\square$

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

- (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*

$$n = 2^k \prod_i p_i$$

ou les  $p_i$  sont des nombres premiers distincts de la forme  $p_i = 2^{2^{k_i}} + 1$  avec  $k_i \geq 0$  un entier (un tel premier est dit "de Fermat").

**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:  $6 = 2 \times 3$ .
- 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

$$2 = 1 + 2^0, \quad 3 = 1 + 2^1, \quad 5 = 1 + 2^2, \quad 17 = 1 + 2^4, \quad 257 = 1 + 2^8, \quad 65537 = 1 + 2^{16}.$$

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).

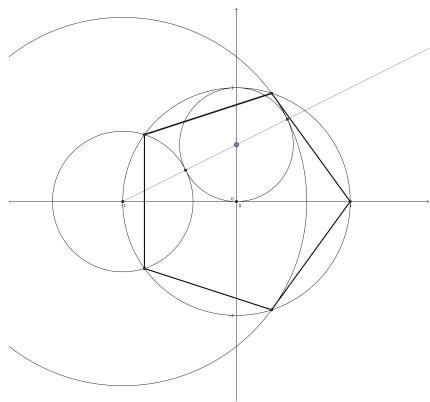


FIGURE 4. Construction de Duerer du pentagone regulier.

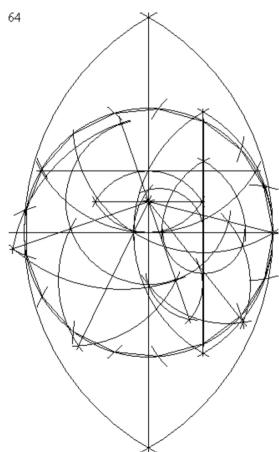


FIGURE 5. Construction de Gauss du polygone regulier a 17 cotes (source Wikipedia)