

## 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

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

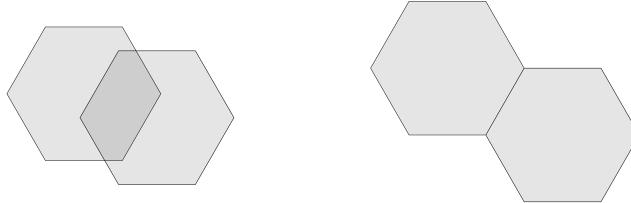


FIGURE 1. Tuiles qui s'intersectent suivant leurs bords ou non

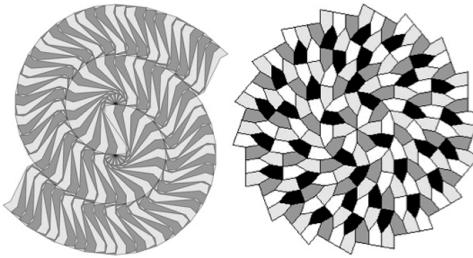


FIGURE 2. Pavages non-reguliers de Voderberg et de Hirschhorn-Hunt  
(source R. Coolman)

ou  $\partial g(\mathbf{T})$  et  $\partial g'(\mathbf{T})$  designent les "bords" de ces tuiles (on verra plus tard une définition précise 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 tuiles ne change pas (et donc que la figure tracée sur le plan par la réunion des bords des différentes 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 manières pour réaliser de tels pavages (si on ne s'inquiète 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 symétrie axiale.*

Pour chaque telle méthode 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 manière continue.

Par contre si on restreint la forme des tuiles aux polygones réguliers (les polygones dont tous les côtés sont de même longueur) on obtient

THÉORÈME 1.2 (Théorème des polygones réguliers pavageurs). *Les seuls polygones réguliers permettant de pavier le plan de manière régulière sont*

- Les triangles équilatéraux
- Les carrés
- Les hexagones réguliers.

Tout ces résultats sont des résultats sur la structure de l'ensemble des isométries (transformations du plan préservant les distances) qui quand on les applique laissent un pavage régulier invariant. Cet ensemble possède une structure algébrique supplémentaire: celle de *groupe*. Cela provient des faits suivants

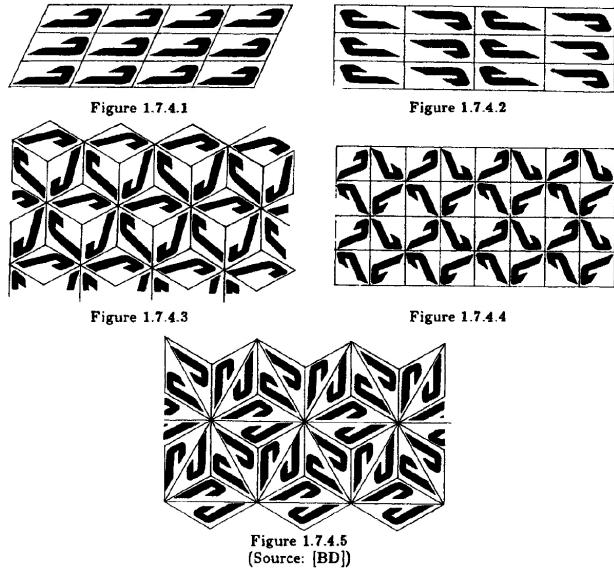


FIGURE 3. Pavages Reguliers sans symetries axiales (source Y. Brossard)

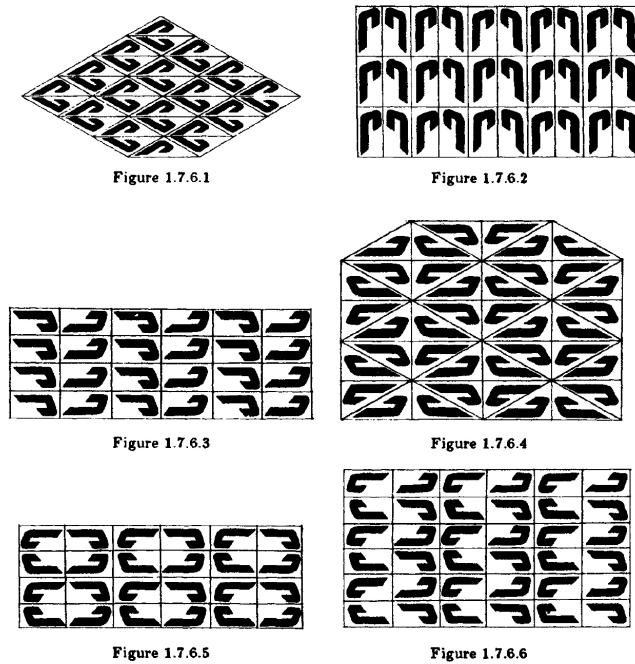


FIGURE 4. Pavages Reguliers avec symetries axiales (source Y. Brossard)

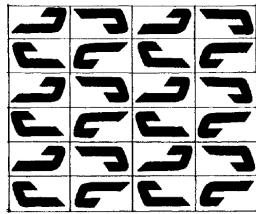


Figure 1.7.6.7

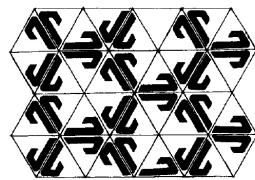


Figure 1.7.6.8

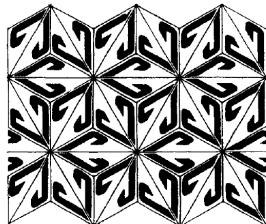


Figure 1.7.6.9

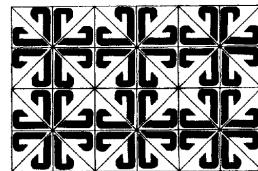


Figure 1.7.6.10

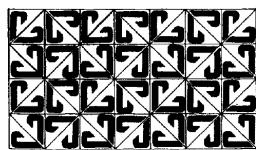


Figure 1.7.6.11

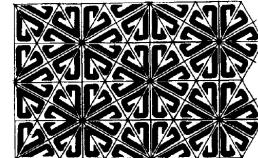


Figure 1.7.6.12

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

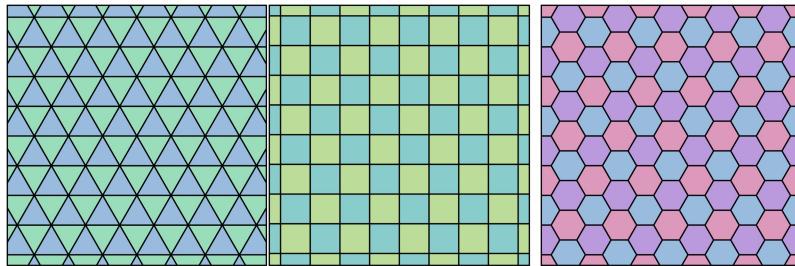


FIGURE 6. Polygones Reguliers paveurs (source wikimedia)

- (1) Si deux isometries laissent un pavage invariant leur composition 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 coordonnee et  $f$  la seconde.

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

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

tel que:

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

ie. l'ensemble des paires contenues dans  $\Gamma_\phi$  dont la premiere coordonnee est  $e$  est reduit a un element. On note la deuxieme coordonnee 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

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

EXERCICE 2.1. Decrire les graphes de ces applications ?

REMARQUE 1.1. Une raison pour la notation  $F^E$  est le fait que si  $E = \{e_1, \dots, e_n\}$  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 et que le nombre de leurs éléments est noté  $|E|$  et  $|F|$  alors  $F^E$  est fini et

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

### 1.1. Composition d'applications.

DÉFINITION 2.3 (Composition). Soit  $\phi : E \rightarrow F$  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 composée définie par

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

La composition défini donc une application de l'ensemble produit  $F^E \times G^F$  vers l'ensemble  $G^E$  notée :

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

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

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

EXERCICE 2.2. Demontrer cette formule.

### 1.2. Image, pre-image, injectivité, surjectivité.

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 donné  $A \subset E$ , l'image de  $A$  par  $\phi$  est le sous-ensemble

$$\phi(A) = \{\phi(e), e \in A\} \subset F.$$

- Etant donné  $B \subset F$ , 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 réduit à un seul élément,

$$\phi^{-1}(\{f\}) = \{e \in E \mid \phi(e) = f\}$$

est l'ensemble des antécédents 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 des antécédents de  $f$ ,  $\phi^{-1}(\{f\})$  a au plus 1 élément (mais peut être l'ensemble vide  $\emptyset$  qui n'a pas d'éléments).
- Surjective: si pour tout  $f \in F$ , l'ensemble  $\phi^{-1}(\{f\})$  a au moins 1 élément.
- Bijective: si pour tout  $f \in F$ ,  $\phi^{-1}(\{f\})$  a exactement 1 élément (i.e. si  $\phi$  est injective et surjective).
- Si  $\phi$  est bijective, on définit son application réciproque  $\phi^{-1} : F \rightarrow E$  comme étant l'application qui à  $f \in F$  associe l'unique élément de l'ensemble  $\phi^{-1}(\{f\}) \subset E$ . L'application  $\phi^{-1} : F \rightarrow E$  est également une bijection et sa réciproque est  $\phi$ :

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

- On a les formules de composition

$$\phi^{-1} \circ \phi = \text{Id}_E, \phi \circ \phi^{-1} = \text{Id}_F.$$

– Une application injective (une injection) sera notée

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

– Une application surjective (une surjection) sera notée

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

– Une application bijective (une bijection) sera notée

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

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 noté

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

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

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

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

### 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 que ces deux ensembles ont le même cardinal. On note cette relation

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

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:

$$|E| = |F| \iff |F| = |E|.$$

On a une notion un peu plus fine pour comparer des cardinaux pas forcément égaux:

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

$$|E| \leq |F|.$$

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

DÉFINITION 2.9. 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 1.4** (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 2.10** (Ensembles denombrables). *Un ensemble infini qui a même cardinal que  $\mathbb{N}$  est dit denombrable.*

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

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

**1.4. Criteres numerique d'injectivite ou de surjectivite 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.

## 2. Groupes

Etant donné un ensemble  $E$  et

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

l'ensemble des bijections de  $E$  sur lui-même. L'ensemble  $\mathfrak{S}_E$  est équipé de structures naturelles (on dit aussi "canoniques") qui méritent d'être isolées:

- (1)  $\mathfrak{S}_E$  possède un élément distingué, l'identité de  $E$ ,  $\text{Id}_E : e \in E \mapsto e \in E$ .
- (2)  $\mathfrak{S}_E$  possède une opération de composition:

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

- (3) Cette opération vérifie une relation d'associativité:

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

- (4) A tout élément  $\phi \in \mathfrak{S}_E$  est associé un élément distingué, la bijection réciproque  $\phi^{-1}$  qui vérifie l'égalité

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

Les mathématiciens ont réalisé que ces structures additionnelles quoique très simples, du fait de leur caractère complètement canonique sont extrêmement importantes et qu'on les retrouve dans de nombreux autres objets mathématiques. Ils ont donc décidé, pour les étudier, de les axiomatiser en une notion abstraite: celle de groupe.

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

- d'une loi de composition interne

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

- d'une application appelée inversion

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

- d'un élément distingué  $e_G \in G$  appelé "élément neutre" ou "identité"

et qui vérifient:

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

L'élément  $g^{-1}$  est appelé "élément opposé" ou "symétrique" ou "inverse" de  $g$ .

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

- (Unicité de l'élément neutre) Montrer que si  $e'_G \in G$  est tel que  $g \star e'_G = g$  alors  $e'_G = e_G$ .
- (Unicité de l'inverse) Montrer que si  $h$  vérifie  $g \star h = e_G$  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 général 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 2.12 (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 2.13 (Ordre d'un groupe). *Le cardinal  $|G|$  d'un groupe s'appelle aussi l'ordre du groupe. Si  $|G| < \infty$  est fini le groupe est dit fini.*

## 2.1. Exemples.

EXEMPLE 2.1 (Les nombres). Les ensembles des nombres

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

munis de l'addition  $+$ , de l'inversion  $x \mapsto -x$  et de 0 comme 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 2.5. 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 racine  $N$ -ièmes de l'unité muni de la multiplication est un groupe d'élément neutre 1.

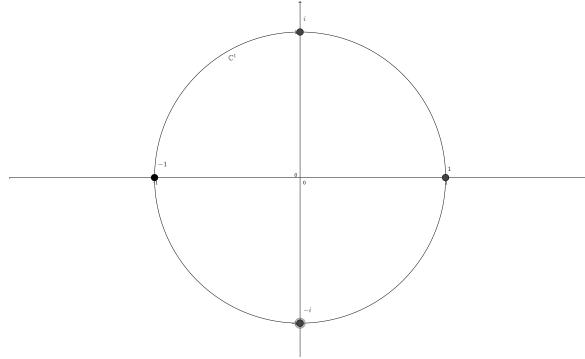


FIGURE 1. Le cercle unité et le groupe  $\mu_4$

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

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

munis de la multiplication  $\times$ , de l'inversion  $x \mapsto 1/x$  et de 1 comme 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 2.6. Si  $E$  est un ensemble fini de cardinal  $|E| = n$ , on a  $|\mathfrak{S}_E| = n!$ .

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

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

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

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

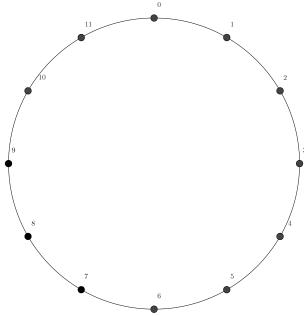


FIGURE 2. Le groupe de l'horloge

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

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

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  $M \cdot M' \in \text{GL}_2(k)$ .
- (3)  $M \cdot \text{Id} = \text{Id} \cdot M = M$
- (4) Si  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{R})$ , alors

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

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

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

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

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

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

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

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

Ainsi equipe,  $\mathbb{N}_{<N}$  forme un groupe commutatif d'element neutre 0; l'inverse de 0 est 0 et de  $n \geq 1$  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 entier  $< 12$  et premiers a 12; on pose

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

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

Plus 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.** 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 conservent la distance: les *isométries* 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 2.14.** 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  $(H, *|_{H \times H})$  (muni de la loi de composition  $*$  restreinte à  $H \times H$  et de l'élément neutre  $e_G$ ) forme un groupe.

**EXEMPLE 2.11.** – 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 2.2** (Critere de sous-groupe). *Un sous-ensemble non-vide  $H$  d'un groupe  $G$  est un sous-groupe (pour  $\star$  et d'element neutre  $e_G$ ) ssi*

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

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

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

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

□

**EXEMPLE 2.12.** Soit  $E$  un ensemble,  $F \subset E$  un sous-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-meme, muni de la composition, de l'identite de  $E$  comme element neutre et de l'application reciproque pour l'inverse). On considere

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

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

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

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

On a

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

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

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

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

**EXERCICE 2.5.** Soit  $N \geq 1$  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.

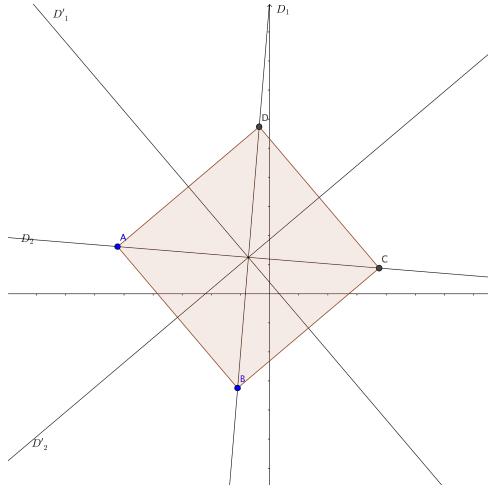


FIGURE 3.

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

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

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

$a \otimes b$	1	5	7	11	$a \oplus b$	(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 2.15. *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 2.16. 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: c'est l'ensemble 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 2.3 (Critère de morphisme). Pour vérifier qu'une application

$$\phi : G \rightarrow H$$

est un morphisme de groupe il suffit de vérifier la deuxième condition de la définition précédente:

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

PREUVE. L'identité ci-dessus est la deuxième condition pour avoir un morphisme; vérifions la première et la troisième. Appliquons l'identité précédente à  $g = g' = e_G$ :

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

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'identité précédente à  $g = g'$ :

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

de sorte que

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

□

EXEMPLE 3.1. Les applications suivantes sont des morphismes de groupes:

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

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

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

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

Quel est le morphisme inverse?

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

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

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

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

est un morphisme de groupes.

PREUVE. Exercice □

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

PROPOSITION 2.5. Soit  $\phi : G \rightarrow H$  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

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

On a

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

et comme  $\phi$  est un morphisme

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

□

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

PREUVE. Exercice □

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

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

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

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

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

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

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

EXERCICE 2.6. Montrer que l'application translation a gauche

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

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

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

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

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

EXERCICE 2.8. Montrer que l'application conjugaison

$$\text{Ad}_{\cdot} : \begin{aligned} G &\mapsto \text{Bij}(G) \\ g &\mapsto \text{Ad}_g \end{aligned}$$

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

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

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

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

On notera respectivement

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

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

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

### 3.6. Noyau, Image.

DÉFINITION 2.17. Soient  $(G, \cdot)$  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 antecedents) de l'element neutre  $e_H$

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

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

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

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

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

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

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

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

car

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

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

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

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

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

**THÉORÈME 2.1.** Soit  $\phi : G \rightarrow H$  un morphisme de groupes. Soit  $h \in H$  alors l'ensemble des solution 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,  $g_0$  designe n'importe quelle solution de l'équation  $E(\phi, h)$ , ie.  $\phi(g_0) = h$ .

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

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

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

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

et

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

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

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

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

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

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)

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

Ainsi  $\mathbf{x}_0$  est notre  $g_0$  et  $\mathbf{x}$  est un 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)

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

ou  $a, b \in \mathbb{R}$ ,  $a \neq 0$ ,  $f : x \mapsto f(x)$  est une fonction de classe  $\mathcal{C}^1$  (dérivable 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

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

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

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

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 définition  $\phi^{-1}(\{e_H\}) = \ker \phi$  possède au plus 1 élément. Comme  $\ker \phi$  contient  $e_G$  (car  $\phi$  est un morphisme), on a  $\ker \phi = \{e_G\}$ .

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

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

mais

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

ne possède qu'un élément. En résumé, tout  $h \in H$  possède au plus un antécédent par  $\phi$ :  $\phi$  est injectif.

□

Le corollaire suivant concerne les groupes finis.

**THÉORÈME 2.3** (Théorème Noyau-Image numérique 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 donc à*

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

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

**REMARQUE 3.2.** ce théorème admet un analogue en algèbre linéaire: si  $k$  est un corps et  $\phi : E \rightarrow F$  est une application linéaire entre deux  $k$ -espaces vectoriels alors le théorème 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 précise du théorème noyau image.

**REMARQUE 3.4.** On va voir un peu plus tard le *Théorème de Lagrange* qui dit que si  $G$  est un groupe fini et  $G' \subset G$  est un sous-groupe ( $G'$  n'est pas forcément 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 antécédents

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

forme une partition de  $G$ : pour  $h \neq h'$  les ensembles  $\phi^{-1}(\{h\})$  et  $\phi^{-1}(\{h'\})$  sont disjoints et  $G$  est la réunion 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 à gauche  $t_{g_0} : k \mapsto g_0 k$  est injective sur  $G$ , ainsi

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

□

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

DÉFINITION 2.18. 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 3.3. 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

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

Multipliant 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. Le Théorème de Lagrange

Le théorème de Lagrange est l'un des résultats les plus importants de la théorie des groupes finis: il illustre le fait qu'en tant qu'espace un groupe est un objet "homogène": il a l'air d'être le même quelque soit l'endroit où l'on se trouve.

THÉORÈME 2.5 (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  $G$ ,  $|G|$ .

PREUVE. Considérons les ensembles translates

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

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

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

donc ces ensembles recouvrent entièrement  $G$ .

On a

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

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

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

échangeant les rôles de  $g$  et  $g'$  on obtient  $gH = g'H$ .

Comme les différents ensembles  $g.H$  sont soit disjoints, soit égaux et que tout élément 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 même cardinal: en effet l'application (de translation par  $g$ )

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

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

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

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

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

et ainsi

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

□

**REMARQUE 4.1.** Le théorème de Lagrange généralise le Théorème noyau-image aux sous-groupes  $H$  qui ne sont pas forcément distingués (par forcement de la forme  $\ker \phi$ .)

**REMARQUE 4.2.** Le quotient  $|G|/|H|$  (qui est entier par le Théorème de Lagrange) a une interprétation concrète: il est égal aux nombres de sous-ensembles distincts de la forme  $g.H$ ,  $g \in G$ .

Cette remarque conduit à la définition un peu plus générale suivante:

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

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

### 5. Groupe engendre par un ensemble

DÉFINITION 2.1. Soit  $(G, \star)$  un groupe et  $A \subset G$  un sous-ensemble de  $G$ . Il existe un sous-groupe de  $G$  contenant  $A$  qui est minimal pour cette 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  $g \cdot g'^{-1} \in \langle A \rangle$ .  $\square$

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

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

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

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 (5.1) montrer que

**PROPOSITION 2.7.** *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 2.8.** *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  $g^{\mathbb{Z}}$ .  $\square$

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

THÉORÈME 2.6. *Soit  $(G, \star)$  un groupe et  $A \subset G$  un sous-ensemble de  $G$ . Le sous-groupe 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 5.1.  $\mathbb{Z}$  et  $\mathbb{Z}/N\mathbb{Z}$  sont engendrés par 1.

EXEMPLE 5.2. 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  $\mathfrak{S}_n$  est engendré par l'ensemble des  $\frac{n(n-1)}{2}$  transpositions

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

(Le vérifier à la main pour  $n = 3$ ).

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

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

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

**5.3. Notation additive.** La notation exponentielle est utilisée pour un groupe général. Si le groupe est commutatif il peut être commode d'utiliser la notation additive: si la loi de groupe commutatif est notée  $\oplus$ , l'élément neutre  $\mathbf{0}_G$  et l'opposé d'un élément  $g$  est noté  $\ominus g$ , on a donc

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

On pose alors

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

et pour  $n \geq 1$  un entier,

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

et on pose

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

et on a

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

Un élément de la forme  $n.g$  sera appellé un multiple de  $g$  et on notera

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

l'ensemble des multiples de  $g$ .

#### 5.4. Ordre d'un élément.

DÉFINITION 2.20. Soit  $g \in G$  et

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

le sous-groupe engendré par  $G$ .

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

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

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

Il résulte de cette définition et du théorème de Lagrange que

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

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

La proposition suivante est également très utile.

PROPOSITION 2.10. Si  $\text{ord}(g) < \infty$  est fini alors  $\text{ord}(g)$  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  $\text{ord}(g)$ .

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

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

donc  $n - kN = 0$  car il est  $\geq 0$  et  $< N$  et ne peut être non-nul par minimilité de  $N$ . Montrons que  $N \leq \text{ord}(g) = |g^{\mathbb{Z}}|$ : il suffit de montrer que

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

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

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

alors

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

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

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

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

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

□

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

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

**Preuve:** Exercice. □

### 5.5. Groupes cycliques.

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

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

*est dit cyclique.*

PROPOSITION 2.11. *Soit  $G$  un groupe cyclique alors ou bien  $G$  est infini et il est isomorphe 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. Considerons le morphisme

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

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

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

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

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

Considerons 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  $g^n = e_G$  donc si  $g^r \neq e_G$  et si  $0 \leq r < N$  cela force  $r = 0$ , on a donc  $\ker \exp_{g,N} = \{0\}$ . Le morphisme est injectif et surjectif car les deux groupes ont le même nombre d'éléments et c'est donc un isomorphisme. □

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

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

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

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

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

Le nombre de ces générateurs est noté  $\varphi(N)$  et vaut

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

est appellée la fonction d'Euler de  $N$ .

PREUVE. Montrons que

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

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

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

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

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

et donc

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

on a donc l'inclusion inverse

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

et donc égalité

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

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

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

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

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

En particulier, on a

$$\text{ord}(g^n) = 1 \iff (n, N) = 1.$$

Les générateurs de  $G$  sont donc exactement les éléments de la forme  $g^n$  avec  $(n, N) = 1$ . L'élément  $g^n$  engendre  $G$ ; reciprocement si  $g^n = G$  alors

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

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

COROLLAIRE 2.3. Soit  $G$  cyclique d'ordre  $N$  et engendré par  $g$ . L'application

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

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

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

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

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

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

Montrons qu'elle est surjective.

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

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

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

Deux éléments de même ordre engendrent des sous-groupes de même ordre; notons  $N/d$  cet ordre (il divise  $N$  donc peut s'écrire sous cette forme). Les deux groupes sont égaux et correspondent à  $d$  par la bijection précédente.  $\square$

### 5.6. Le cas des racines de l'unité.

Soient  $N \geq 1$  un entier et

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

l'ensemble des racines  $N$ -ièmes de l'unité (l'ensemble des racines du polynôme  $X^N - 1$  dans le corps des nombres complexes  $\mathbb{C}$ ).

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

**PREUVE.** L'application

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

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

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

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

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

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

$\square$  On redémontrera plus tard (sans supposer l'existence de l'exponentielle complexe) que ce groupe est cyclique comme conséquence d'un résultat général sur les corps.

Rappelons également que  $\mu_N$  est contenu dans le cercle unité, ie l'ensemble des nombres complexes de module 1:

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

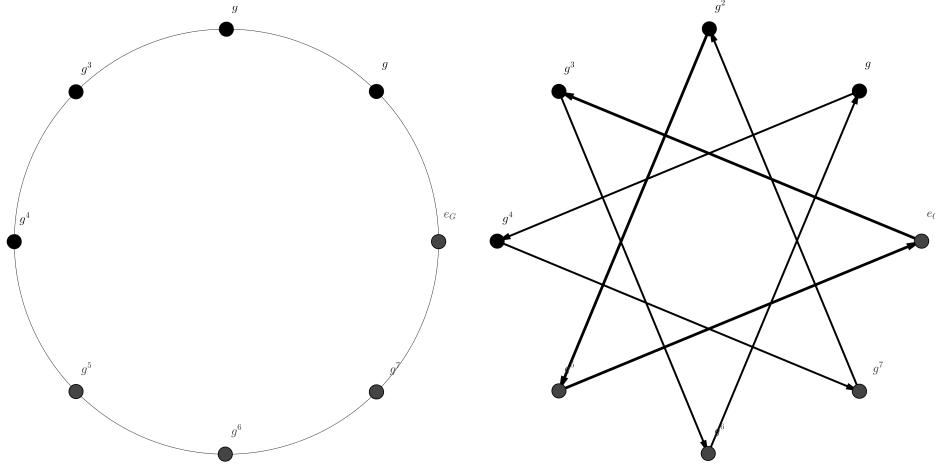
En effet

$$\forall z \in \mu_N, 1 = |z^N| = |z|^N \implies |z| = 1.$$

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

Ainsi pour  $N = 8$  la figure 5.6 est une représentation graphique d'un groupe cyclique à 8 éléments

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

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

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

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

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



## CHAPITRE 3

### Isometries du plan

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

Le plan 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  $\mathbf{0}$  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  $\mathbf{0}$ ; avec la multiplication par les scalaires définie par

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

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 2.6 du chapitre précédent. Par le critère 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 appellé 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 réaliser comme un sous-groupe de transformations du plan. C'est en fait un cas particulier d'un phénomène complètement général: tout groupe peut être réalisé comme un sous-groupe de son groupe de bijections. C'est l'*action* d'un groupe sur lui-même par translations (cf. le chapitre sur les actions de groupes).

On a la proposition élémentaire 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'élément  $(u, v)$  recherché est donné par

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

□

La proposition précédente s'exprime de manière un peu pédante en disant que  $\mathbb{R}^2$  est un espace principal homogène sous l'action de  $\mathbb{R}^2$  par translations. Ce type de vocabulaire n'est pas très 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 manières: soit comme un ensemble (un espace homogène 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 translations agissant sur l'ensemble  $\mathbb{R}^2$ .

Ainsi notera les éléments de  $\mathbb{R}^2$  soit, sous forme de points  $P = (x_P, y_P)$  (si on veut mettre en avant l'aspect espace homogène), 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  $\mathbf{0}\vec{P}$  sous forme vectorielle. Cette distinction de points de vue est assez subtile et pas indispensable pour la suite: dans la pratique on utilisera l'une ou l'autre des deux notations de manière interchangeable.

## 1.2. Droites affines et vectorielles.

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

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

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

*C'est un groupe (et même un sous-espace vectoriel de dimension 1) de  $\mathbb{R}^2$ . C'est la droite vectorielle de direction  $\vec{v}$ .*

- Une droite affine  $D$  est l'ensemble des images d'un point  $P$  par les translations d'une droite vectorielle: c'est un sous-ensemble de  $\mathbb{R}^2$  de la forme

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

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

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

- Soit forme paramétrique 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 équation cartésienne:  $D = \mathcal{D}(P, \vec{v})$  est l'ensemble des solutions  $(x, y)$  de l'équation

$$ax + by = c$$

avec

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

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

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

Rappelons également les définitions et résultats de base concernant les droites

PROPOSITION 3.3. *Etant données 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 données deux droites  $D = \mathcal{D}(P, \vec{v}), D' = \mathcal{D}(P', \vec{v}')$  alors l'intersection  $D \cap D'$  est*

- soit réduite à un point,
- soit l'ensemble vide,
- soit égale à  $D = D'$ .

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 parallèles et dans le troisième elles sont confondues.

**DÉFINITION 3.4.** Trois points  $P, Q, R \in \mathbb{R}^2$  sont alignés si ils font partie d'une même droite affine ou de manière équivalente si  $\vec{PQ}$  et  $\vec{QR}$  font partie de la même 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

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

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

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

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

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

$$\|\vec{u}\| = 0 \iff \vec{u} = \mathbf{0}, \quad d_2(P, Q) = 0 \iff P = Q.$$

- Symétrie: pour tout  $\vec{u} \in \mathbb{R}^2$ ,  $P, Q \in \mathbb{R}^2$

- 

$$\|-\vec{u}\| = \{\vec{u}\}, \quad d_2(P, Q) = d_2(Q, P).$$

- Inégalité du triangle: pour tout  $\vec{u}, \vec{v} \in \mathbb{R}^2$ ,  $P, Q, R \in \mathbb{R}^2$

$$\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|, \quad d_2(P, R) \leq d_2(P, Q) + d_2(Q, R)$$

avec égalité si et seulement si  $\vec{u}$  et  $\vec{v}$  sont proportionnels et que le facteur de proportionnalité est  $\geq 0$ /ssi  $P, Q, R$  sont alignés (cad  $\vec{PQ}$  et  $\vec{PR}$  sont proportionnels) et  $Q$  est "entre"  $P$  et  $R$ .

- Homogénéité:

$$\|\lambda \vec{u}\| = |\lambda| \|\vec{u}\|, \quad d_2(\lambda \cdot P, \lambda \cdot Q) = |\lambda| d_2(P, Q)$$

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

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

Les trois premières propriétés sont constitutives de ce qu'on appelle une distance:

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

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

qui vérifie les propriétés suivantes

- Separation des points: pour tout  $P, Q \in X$ ,

$$d(P, Q) = 0 \iff P = Q.$$

- Symétrie: pour tout  $P, Q \in X$ ,

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

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

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

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

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

Elle permet seulement de mesurer si deux éléments sont égaux ou pas.

REMARQUE 1.3. La notion générale de distance est très importante: elle permet de mesurer si deux éléments d'un ensemble sont "proches" l'un de l'autre ou non; elle est utilisée pour des ensembles très généraux: ainsi on peut définir une notion de distance sur des espaces de fonctions abstraits. Dans ce cours on ne parlera que de la distance euclidienne.

Cette notion permet d'introduire de nouveaux lieux géométriques:

DÉFINITION 3.7. *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

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

On a donc

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

Rappelons que

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

– symétrique:

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

– bilinéaire:

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

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

– 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-evident est l'inegalite du triangle. Elle provient de la proposition suivante

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

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

avec egalite 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 colineaire a  $\vec{v}$ ).

**PREUVE.** On peut supposer  $\vec{v} \neq 0$  (sinon on a  $0 = 0$ ). Pour  $\lambda \in \mathbb{R}$  considerons 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 polynome a coefficients reels de degree  $\leq 2$  et a valeurs positives ou nulles. La derivee 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'inegalite. 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'inegalite du triangle): soient  $\vec{u}, \vec{v} \in \mathbb{R}^2$ , on a par l'inegalite de Cauchy-Schwarz

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

□

#### 1.4. Decomposition dans une base orthogonale.

**DÉFINITION 3.8.** *Etant donne  $\vec{u}, \vec{v} \in \mathbb{R}^2$ , si  $\langle \vec{u}, \vec{v} \rangle = 0$ , on dit que  $\vec{u}$  et  $\vec{v}$  sont orthogonaux ou perpendiculaires*

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

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

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

**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 3.9.** 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

$$\begin{aligned}\vec{w} &= \frac{\langle \vec{w}, \vec{u} \rangle}{\|\vec{u}\|^2} \vec{u} + \frac{\langle \vec{w}, \vec{v} \rangle}{\|\vec{v}\|^2} \vec{v} \quad \text{si } (\vec{u}, \vec{v}) \text{ est orthogonale et} \\ (1.3) \quad \vec{w} &= \langle \vec{w}, \vec{u} \rangle \vec{u} + \langle \vec{w}, \vec{v} \rangle \vec{v} \quad \text{si } (\vec{u}, \vec{v}) \text{ est orthonormee.}\end{aligned}$$

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 1.2.** 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 isométries et on va les déterminer toutes. Pour cela on introduit le sous-ensemble

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

des isométries 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 distingué 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 isométrie  $\phi$  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'isométrie  $\phi_0$  s'appelle la partie linéaire de l'isométrie  $\phi$ .

La preuve commence par le résultat non moins important suivant.

**THÉORÈME 3.3.** *Soit  $\phi$  une isométrie 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 réciproque  $\phi^{-1}$  est une isométrie 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 3.10.** *L'ensemble  $\text{Isom}(\mathbb{R}^2)_{\mathbf{0}}$  s'appelle l'ensemble des isométries linéaires du plan. Par opposition un élément général de  $\text{Isom}(\mathbb{R}^2)$  sera parfois appellé "isométrie affine".*

La preuve de ce théorème repose sur la

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

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

**PREUVE.** Soit  $\phi \in \text{Isom}_{\mathbf{0}}(\mathbb{R}^2)$ , et  $\vec{v} = \overrightarrow{\mathbf{0}P}$  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  $\vec{w} = \overrightarrow{\mathbf{0}Q}$

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

□

**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.

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

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

et

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

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

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

□

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

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

- (1) Montrer que si  $\phi$  preserve la longueur ( $\forall \vec{u} \in \mathbb{R}^2, \|\phi(\vec{u})\| = \|\vec{u}\|$ ) alors  $\phi$  est une isometrie.

---

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

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

### 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  $\text{Isom}(\mathbb{R}^2)$ ,  $\text{Isom}(\mathbb{R}^2)_0$  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. Considerons  $\phi_0 = t_{-\phi(\mathbf{0})} \circ \phi$  est une isometrie et comme

$$\phi_0(\mathbf{0}) = t_{-\phi(\mathbf{0})}(\phi(\mathbf{0})) = \phi(\mathbf{0}) - \phi(\mathbf{0}) = \mathbf{0}$$

elle est lineaire et en particulier est bijective. De plus

$$\phi = t_{\phi(\mathbf{0})} \circ \phi_0$$

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  $\text{Isom}(\mathbb{R}^2)_0$  et  $T(\mathbb{R}^2)$  sont des sous-groupes.

- Montrons que la decomposition translation/isometrie lineaire

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

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

$$\phi = t \circ \phi_0 = t' \circ \phi'_0.$$

On a alors

$$t'^{-1} \circ t = \phi'_0 \circ \phi_0^{-1}$$

et donc l'element  $\psi_0 = t'^{-1} \circ t = \phi'_0 \circ \phi_0^{-1}$  appartient a la fois a  $T(\mathbb{R}^2)$  et a  $\text{Isom}(\mathbb{R}^2)_0$  : on a  $\psi_0 = t_{\vec{u}}$  pour un certain vecteur  $\vec{u} \in \mathbb{R}^2$  et donc

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

Il en resulte que

$$t = t', \phi_0 = \phi'_0.$$

- Le sous-groupe  $T(\mathbb{R}^2)$  est distingué:  $T(\mathbb{R}^2)$  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 precisement

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

On commence par supposer que  $\phi = \phi_0 \in \text{Isom}(\mathbb{R}^2)_0$ . Par linearite 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 general:  $\phi = t \circ \phi_0$ , 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 deduit de cette decomposition le corollaire suivant qui sera tres utile:

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

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

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

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

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

On a

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

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

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

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

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

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

□

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

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

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

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 equipe 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 lineaire.** 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

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

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

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

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

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

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

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

On rappelle la

**DÉFINITION 3.11.** Soit  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $a, b, c, d \in \mathbb{R}$  une matrice quelconque (pas forcement associee a une isometrie lineaire), son determinant  $\det M$  est defini par

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

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

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

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

$$(2.3) \quad a^2 + c^2 = b^2 + d^2 = a^2 + b^2 = c^2 + d^2 = 1, \quad ab + cd = ac + bd = 0$$

$$(2.4) \quad \det(M_\phi) = ad - bc = \pm 1.$$

**Preuve:** Les coefficients de  $M_{\phi^{-1}} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$  sont les coefficients de  $\mathbf{e}'_1 = \phi^{-1}(\mathbf{e}_1)$ ,  $\mathbf{e}'_2 = \phi^{-1}(\mathbf{e}_2)$  dans la base  $\mathcal{B}_0$ . Comme  $\mathcal{B}_0$  est orthonormee, on a par (1.3) les formules

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

Comme  $\varphi$  est une isometrie on a

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

en appliquant à nouveau (1.3). De même on trouve que

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

et également

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

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

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

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

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

Enfin pour (2.4), on a

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

□

**DÉFINITION 3.12.** Une matrice  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  est dite orthogonale si c'est la matrice associée à une isométrie linéaire. Une matrice orthogonale est dite spéciale si son déterminant vaut +1 et elle est dite non-spéciale si son déterminant vaut -1. On note respectivement  $O_2(\mathbb{R})$ ,  $O_2(\mathbb{R})^+ = SO_2(\mathbb{R})$ ,  $O_2(\mathbb{R})^-$  l'ensemble des matrices orthogonales, orthogonales spéciales, orthogonales non-spéciales. On a donc

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

**DÉFINITION 3.13.** Soit

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

Une matrice  $2 \times 2$ . La transposee de  $M$  notée  ${}^t M$  est la matrice obtenue en échangeant les coefficients de part et d'autre de la diagonale:

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

On a donc montrer que

**PROPOSITION 3.8.** Une matrice orthogonale est inversible et son inverse est donnée par la matrice transposee  ${}^t M$ .

On va expliciter la forme des matrices orthogonales.

**PROPOSITION 3.9.** Une matrice  $M$  est orthogonale si et seulement si il existe  $c, s \in \mathbb{R}$  vérifiant  $c^2 + s^2 = 1$  tel que  $M$  est de l'une des deux formes suivante

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

et  $M$  est spéciale ou bien

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

et  $M$  est non-spéciale.

– Si  $M$  est speciale son inverse est égale à sa transposee

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

et est encore speciale.

– Si  $M$  est non-speciale son inverse est égale à sa transposee et est égale à  $M$ ; en d'autres termes  $M$  est d'ordre 2 exactement

$$M^{-1} = {}^t M = M = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}, \quad M^2 = \text{Id} \text{ et } M \neq \text{Id}.$$

**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  $c^2 + s^2 = 1$  et donc  $(c, s) \neq (0, 0)$ , les solution  $(b, d)$  du système linéaire ci-dessus sont toutes de la forme

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

On a

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

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

Réiproquement soit  $M$  de l'une des deux formes ci-dessus et  $\phi$  l'application linéaire définie par

$$\phi(x, y) = (ax + by, cx + dy).$$

La matrice associée à  $\phi$  est  $M$  et si  $\mathbf{e}_1 = (1, 0)$  et  $\mathbf{e}_2 = (0, 1)$  on a

$$\langle \phi(1, 0), \phi(1, 0) \rangle = a^2 + c^2 = c^2 + s^2 = 1, \quad \langle \phi(0, 1), \phi(0, 1) \rangle = b^2 + d^2 = s^2 + c^2 = 1,$$

$$\langle \phi(1, 0), \phi(0, 1) \rangle = ab + cd = \pm(cs - sc) = 0$$

donc  $\phi$  transforme une base orthonormée en une base orthonormée, c'est donc une isométrie.

Soit  $M$  une matrice spéciale, son inverse est égale à sa transposee qui vaut  $\begin{pmatrix} c & s \\ -s & c \end{pmatrix}$  qui est encore une matrice spéciale.

Soit  $M = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}$  une matrice non-spéciale alors  $M \neq \text{Id}$  car on aurait  $s = 0$  et les coordonnées sur la diagonale sont différentes. Son inverse est égale à sa transposee qui vaut

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

On a donc  $M \cdot M = \text{Id}_2$ . □

**2.2. Applications linéaires et matrices.** On a associé à chaque isométrie linéaire  $\phi$  une certaine matrice  $M_\phi$  dont les coefficients sont les coefficients des images  $\phi(\mathbf{e}_1), \phi(\mathbf{e}_2)$  des deux vecteurs de la base canonique  $\mathbf{e}_1, \mathbf{e}_2$  dans la base canonique. Pour faire cette association il suffit juste que  $\phi$  soit linéaire et on va donner des précisions supplémentaires quand à cette association:

### 2.2.1. L'algèbre des applications linéaires.

DÉFINITION 3.14. Une application  $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  est  $\mathbb{R}$ -linéaire si

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

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

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

- Une loi d'addition: si  $\phi, \psi$  sont linéaires alors l'application  $\phi + \psi$  définie par

$$(\phi + \psi)(\vec{v}) = \phi(\vec{v}) + \psi(\vec{v})$$

est linéaire.

- La loi de composition des applications: si  $\phi, \psi$  sont linéaires alors l'application composée  $\phi \circ \psi$  définie par

$$(\phi \circ \psi)(\vec{v}) = \phi(\psi(\vec{v})).$$

- Un loi de multiplication par les scalaires: pour  $\phi$  linéaire et  $\lambda \in \mathbb{R}$ , l'application  $\lambda.\phi$  définie par

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

est linéaire.

De plus

- L'addition est commutative et associative

$$\phi + \psi = \psi + \phi.$$

- La composition est associative:

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

- La composition est distributive par rapport à l'addition:

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

- La multiplication est distributive par rapport à l'addition:

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

Enfin  $\text{End}_{\mathbb{R}}(\mathbb{R}^2)$  possède deux éléments distingués

- L'application constante égale à  $0_{\mathbb{R}^2} = (0, 0)$

$$0_{\mathbb{R}^2} : \vec{v} \rightarrow 0_{\mathbb{R}^2}$$

qui est l'élément neutre de  $\text{End}_{\mathbb{R}}(\mathbb{R}^2)$  pour l'addition:

$$\forall \varphi \in \text{End}_{\mathbb{R}}(\mathbb{R}^2), \varphi + 0_{\mathbb{R}^2} = \varphi.$$

- L'application identité

$$\text{Id}_{\mathbb{R}^2} : \vec{v} \rightarrow \vec{v}$$

qui est l'élément neutre de  $\text{End}_{\mathbb{R}}(\mathbb{R}^2)$  pour la composition:

$$\forall \varphi \in \text{End}_{\mathbb{R}}(\mathbb{R}^2), \varphi \circ \text{Id}_{\mathbb{R}^2} = \text{Id}_{\mathbb{R}^2} \circ \varphi = \varphi.$$

### 2.2.2. L'algèbre des matrices $2 \times 2$ .

DÉFINITION 3.15. Une matrice réelle  $2 \times 2$  est un tableau carré à 4 entrées réelles

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{R}.$$

On note  $M_2(\mathbb{R})$  l'ensemble des matrices  $2 \times 2$

L'ensemble  $M_2(\mathbb{R})$  est munis de structures supplémentaires

- Une loi d'addition: si  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$  sont des matrices on définit la matrice  $M + M'$  par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}.$$

- Une loi de multiplication matricielle: si  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$  sont des matrices on définit la matrice produit  $M.M'$  par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

- Un loi de multiplication par les scalaires: pour  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  une matrice et  $\lambda \in \mathbb{R}$ , la matrice  $\lambda.M$  est définie par

$$\lambda \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}.$$

De plus

- L'addition est commutative

$$M + M' = M' + M.$$

- La multiplication matricielle est distributive par rapport à l'addition:

$$\forall M, M', M'', \quad M.(M' + M'') = M.M' + M.M'', \quad (M' + M'').M = M'.M + M''.M.$$

- La multiplication par les scalaires est distributive par rapport à l'addition:

$$\forall M, M', \quad \lambda.(M + M') = \lambda.M + \lambda.M'.$$

Enfin  $M_2(\mathbb{R})$  possède deux éléments distingués

- La matrice nulle

$$\mathbf{0}_{M_2(\mathbb{R})} = 0_2 := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

qui est l'élément neutre de  $M_2(\mathbb{R})$  pour l'addition:

$$\forall M, \quad M + 0_2 = M.$$

- La matrice identité

$$\text{Id}_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

qui est l'élément neutre de  $M_2(\mathbb{R}^2)$  pour la multiplication matricielle:

$$\forall M, \quad M.\text{Id}_2 = \text{Id}_2.M = M.$$

Des ensembles tels que l'ensemble des endomorphismes ou celui des matrices munis des structures supplémentaires  $(\text{End}_{\mathbb{R}}(\mathbb{R}^2), +, \circ, 0_{\mathbb{R}^2}, \text{Id}_{\mathbb{R}^2})$ ,  $(M_2(\mathbb{R}^2), +, ., 0_2, \text{Id}_2)$  sont appelés de  $\mathbb{R}$ -algèbres.

Soit  $\phi$  une application linéaire, on lui associe la matrice

$$M_\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ avec } \phi(\mathbf{e}_1) = (a, c), \phi(\mathbf{e}_2) = (b, d).$$

L'intérêt de définir la multiplication des matrices telle qu'on l'a définie est la suivante

**THÉORÈME 3.6.** *L'application*

$$\begin{aligned} M_\cdot : \text{End}(\mathbb{R}^2) &\mapsto M_2(\mathbb{R}) \\ \phi &\mapsto M_\phi \end{aligned}$$

est un isomorphisme de  $\mathbb{R}$ -algèbres, i.e. une bijection compatible avec les structures d'algèbres et qui vérifie notamment

$$M_{\phi+\psi} = M_\phi + M_\psi, \quad M_{\phi \circ \psi} = M_\phi \cdot M_\psi, \quad M_{\lambda \cdot \phi} = \lambda \cdot M_\phi$$

ainsi que

$$M_{0_{\mathbb{R}^2}} = \mathbf{0}_{M_2(\mathbb{R})}, \quad M_{\text{Id}_{\mathbb{R}^2}} = \text{Id}_2.$$

### 2.2.3. Isomorphismes linéaires et matrices inversibles.

**DÉFINITION 3.16.** Un isomorphisme linéaire de  $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ , ou encore un automorphisme linéaire, est une application linéaire qui est bijective. Sa réciproque  $\phi^{-1}$  est alors automatiquement linéaire. On dit également que  $\phi$  est inversible. On note

$$\text{Aut}_{\mathbb{R}}(\mathbb{R}^2) = \text{GL}(\mathbb{R}^2) = \text{End}_{\mathbb{R}}(\mathbb{R}^2) \cap \text{Bij}(\mathbb{R}^2)$$

l'ensemble des isomorphismes linéaires. L'ensemble  $(\text{GL}(\mathbb{R}^2), \circ)$  est un sous-groupe de  $(\text{Bij}(\mathbb{R}^2), \circ)$  appellé le groupe linéaire de  $\mathbb{R}^2$ .

Rappelons comment on montre que  $\phi^{-1}$  est linéaire: on a

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

et

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

et donc comme  $\phi$  est injective

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

**DÉFINITION 3.17.** L'image par l'application "matrice dans la base canonique" du groupe des applications linéaires inversibles de  $\mathbb{R}^2$  est l'ensemble des matrices inversibles:

$$\text{GL}_2(\mathbb{R}) = \{M \in M_2(\mathbb{R}), \exists M^{-1} \in M_2(\mathbb{R}) \text{ tel que } M \cdot M^{-1} = M^{-1} \cdot M = \text{Id}_2\}.$$

Si  $M = M_\phi$  alors

$$M^{-1} = M_{\phi^{-1}}.$$

cette matrice est donc unique: c'est inverse de  $M$ .

**DÉFINITION 3.18.** L'ensemble des matrices inversibles est noté  $\text{GL}(\mathbb{R}^2)$ . C'est un groupe pour la multiplication des matrices (isomorphe au groupe  $\text{GL}(\mathbb{R}^2)$ ). On l'appelle le groupe linéaire (des matrices  $2 \times 2$ .)

2.2.4. *Le determinant et l'inversion des matrices.*

DÉFINITION 3.19. *Le determinant est la fonction  $\det : M_2(\mathbb{R}^2) \rightarrow \mathbb{R}$  définie par*

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc.$$

Elle permet entre-autres de détecter si une matrice est inversible.

PROPOSITION 3.10. *Le determinant a les propriétés suivantes:*

(1) *Il est multiplicatif:*

$$\det(M \cdot M') = \det(M) \cdot \det(M') \quad \det(\text{Id}_2) = 1.$$

(2) *Une matrice  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  est inversiblessi  $\det M \neq 0$  et alors*

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

2.2.5. *La transposition.* La première partie de la définition suivante a déjà été vue:

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*

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

*est l'application de transposition.*

PROPOSITION 3.11. *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:*

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

(3) *La transposition est multiplicativa:*

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

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

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

**Preuve:** Exercice. □

PROPOSITION 3.12. *Une matrice  $M$  est orthogonale si et seulement si elle vérifie*

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

*Elle vérifie alors également*

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

**Preuve:** Supposons que  ${}^t M \cdot M = \text{Id}_2$ , cela s'écrit

$${}^t M \cdot M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & bc + ad \\ ab + cd & b^2 + d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ce qui montre que les vecteurs  $(a, c), (b, d)$  forment une base orthonormée. Ainsi  $\phi$  l'application linéaire associée à  $M$  transforme la base canonique en une base orthonormée. C'est donc une isométrie.  $\square$

### 2.3. Le groupe des matrices orthogonales.

THÉORÈME 3.7. *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 orthogonale s'écrit comme produit de une matrice non-spéciale (si la matrice est non-spéciale) ou de deux matrices non-spéciales (si la matrice est spéciale). En particulier le groupe  $O_2(\mathbb{R})$  est engendré par  $O_2(\mathbb{R})^-$ , l'ensemble des matrices orthogonales non-spéciales.*

**PREUVE.** Les matrices orthogonales sont exactement les matrices associées à des isométries linéaires dans la base canonique et le produit de deux telles matrices est la matrice associée à la composition de ces isométries. Comme l'ensemble des isométries linéaires forme un groupe, la composition est encore une isométrie linéaire et donc le produit des deux matrices orthogonales est encore orthogonale. Pour la même raison, une matrice orthogonale  $M$  correspondant à  $\phi \in \text{Isom}(\mathbb{R}^2)_0$  est inversible et son inverse  $M^{-1}$  est orthogonale car c'est la matrice associée à  $\phi^{-1}$ . Cela montre que  $O_2(\mathbb{R})$  est un sous-groupe du groupe des matrices inversibles  $GL_2(\mathbb{R})$ .

Pour voir que  $O_2(\mathbb{R})^+$  est un sous-groupe, on a deux possibilités.

La première est de vérifier par un calcul explicite que si  $M, M' \in O_2(\mathbb{R})^+$ ,  $M \cdot M'$  appartient à  $O_2(\mathbb{R})^+$ :

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

$$M \cdot M' = \begin{pmatrix} cc' - ss' & -cs' - sc' \\ sc' + cs' & -ss' + cc' \end{pmatrix} = \begin{pmatrix} c'' & -s'' \\ s'' & c'' \end{pmatrix}$$

avec

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

La matrice appartient à  $O_2(\mathbb{R})$  et donc à  $O_2(\mathbb{R})^+$  puisqu'elle est de la bonne forme.

Ainsi  $O_2(\mathbb{R})^+$  est stable par multiplication et comme il est stable par inversion c'est un sous-groupe de  $GL_2(\mathbb{R})$ . On remarque que les coordonnées de  $M \cdot M'$  ne changent pas si on échange  $c \leftrightarrow c'$  et  $s \leftrightarrow s'$  donc

$$M \cdot M' = M' \cdot M$$

Le groupe  $O_2(\mathbb{R})^+$  est commutatif.

Rappelons la réunion disjointe

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

– Soit  $M^- \in O_2(\mathbb{R})^-$  et  $M^+ \in O_2(\mathbb{R})^+$  alors  $M^+ \cdot M^-$  et  $M^- \cdot M^+$  sont dans  $O_2(\mathbb{R})$  mais ne peuvent appartenir à  $O_2(\mathbb{R})^+$  car cela impliquerait (en multipliant par  $(M^+)^{-1}$ ) que  $M^- \in O_2(\mathbb{R})^+$  car  $O_2(\mathbb{R})^+$  est un groupe. Ainsi

$$M^- \cdot O_2(\mathbb{R})^+, \quad O_2(\mathbb{R})^+ \cdot M^- \subset O_2(\mathbb{R})^-.$$

Montrons l'inclusion inverse: soit  $M \in O_2(\mathbb{R})^-$  alors  $M \cdot M^- \in O_2(\mathbb{R})$  et

$$M \cdot M^- = \begin{pmatrix} c & s \\ s & -c \end{pmatrix} \cdot \begin{pmatrix} c' & s' \\ s' & -c' \end{pmatrix} = \begin{pmatrix} cc' + ss' & cs' - sc' \\ -(cs' - sc') & cc' + ss' \end{pmatrix} \in O_2(\mathbb{R})^+$$

car elle n'est pas non-spéciale. Cela montre que

$$O_2(\mathbb{R})^- \cdot M^- \subset O_2(\mathbb{R})^+ \implies O_2(\mathbb{R})^- \subset O_2(\mathbb{R})^+ \cdot (M^-)^{-1} = O_2(\mathbb{R})^+ \cdot M^-$$

(car  $(M^-)^{-1} = M^-$ ) et donc

$$O_2(\mathbb{R})^- = O_2(\mathbb{R})^+ \cdot M^- \text{ et on a de même } O_2(\mathbb{R})^- = M^- \cdot O_2(\mathbb{R})^+.$$

Ainsi pour  $M \in O_2(\mathbb{R})^-$ , il existe  $M^+ \in O_2(\mathbb{R})^+$  tel que  $M = M^+ \cdot M^-$ . L'élément  $M^+$  est unique car égal à  $M \cdot M^{-1}$ .

– Montrons que le groupe  $O_2(\mathbb{R})^+$  est distingué:

$$\forall M \in O_2(\mathbb{R}), \text{ ad}(M)(O_2(\mathbb{R})^+) = MO_2(\mathbb{R})^+M^{-1} = O_2(\mathbb{R})^+.$$

Si  $M \in O_2(\mathbb{R})^+$  c'est évident. Si  $M \in O_2(\mathbb{R})^-$  on a

$$MO_2(\mathbb{R})^+M^{-1} = O_2(\mathbb{R})^-M^{-1} = O_2(\mathbb{R})^+ \cdot M \cdot M^{-1} = O_2(\mathbb{R})^+.$$

Soit  $M$  une matrice orthogonale; si  $M$  est non-spéciale est le produit d'une matrice non-spéciale: elle-même. Si  $M$  est orthogonale, soit  $M^-$  une matrice non-spéciale fixée quelconque alors

$$M^- \cdot O_2(\mathbb{R})^- = M^- \cdot M^- \cdot O_2(\mathbb{R})^+ = O_2(\mathbb{R})^+ \ni M$$

Ainsi  $M$  s'écrit sous la forme  $M^- \cdot M'$  avec  $M' \in O_2(\mathbb{R})^-$  et c'est donc bien le produit de deux matrices non-spéciales. □

**Preuve:** (alternative) Toute matrice de  $O_2(\mathbb{R})$  est inversible et son inverse est sa transposee  $'M$  qui appartient à  $O_2(\mathbb{R})$ ; donc  $O_2(\mathbb{R}) \subset GL_2(\mathbb{R})$  et est stable par inversion.

– Si  $M, N \in O_2(\mathbb{R})$ , alors

$$(M \cdot N)^t(M \cdot N) = M \cdot N \cdot {}^tN \cdot {}^tM = M \cdot \text{Id}_2 \cdot {}^tM = M \cdot {}^tM = \text{Id}_2$$

donc l'inverse de  $M \cdot N$  est sa transposee ce qui implique que  $M \cdot N$  est orthogonale. 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

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

En d'autre terme c'est un morphisme du groupe  $(\mathrm{GL}_2(\mathbb{R}), \times)$  vers le groupe multiplicatif  $(\mathbb{R}^\times, \times)$ . En particulier la restriction de  $\det$  au sous-groupe  $O_2(\mathbb{R})$  est un morphisme de groupes (dont image est le sous-groupe d'ordre 2  $\{\pm 1\}$ ). L'ensemble des matrices speciales orthogonales

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

est le noyau de ce morphisme (restreint au sous-groupe  $O_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$ ), c'est donc un sous-groupe qui est de plus distingue.

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

□

### 3. Classification des isometries lineaires

On a vu que l'application

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

qui a une isometrie lineaire associe sa matrice (dans la base  $(e_1, e_2)$ ) est une bijection. On defini alors les isometries lineaires speciales ou non-speciales comme etant celles donc la matrice associee est speciale ou non:

DÉFINITION 3.2. *On notera*

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

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

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

On deduit du Theoreme ?? le

THÉORÈME 3.8. *On a les proprietes suivantes*

- (1) *L'ensemble des isometries lineaires speciales  $\mathrm{Isom}(\mathbb{R}^2)_0^+$  est un sous-groupe distingué du groupe  $\mathrm{Isom}(\mathbb{R}^2)_0$  des isometries lineaires.*
- (2) *Le groupe  $\mathrm{Isom}(\mathbb{R}^2)_0^+$  est commutatif.*
- (3) *L'ensemble des isometries lineaires non-speciales  $\mathrm{Isom}(\mathbb{R}^2)_0^-$  est le translate pour le composition (a gauche ou a droite) de  $\mathrm{Isom}(\mathbb{R}^2)_0^+$  par n'importe quelle isometrie lineaire non-speciale :*

$$\forall \phi^- \in \mathrm{Isom}(\mathbb{R}^2)_0^-, \text{ on a } \mathrm{Isom}(\mathbb{R}^2)_0^- = \phi^- \circ \mathrm{Isom}(\mathbb{R}^2)_0^+ = \mathrm{Isom}(\mathbb{R}^2)_0^+ \cdot \phi^-.$$

*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  $\mathrm{Isom}(\mathbb{R}^2)_0^+$ .*

(4) Une isometrie lineaire non-speciale est d'ordre 2:  $\forall \phi \in \text{Isom}(\mathbb{R}^2)^-, \text{ on a}$

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

(5) Toute isometrie lineaire s'ecrit comme produit de une ou deux isometries lineaires non-speciales. En particulier le groupe  $\text{Isom}(\mathbb{R}^2)_0$  est engendre par  $\text{Isom}(\mathbb{R}^2)_0^-$ .

**3.1. Point fixes des isometries lineaires.** On va maintenant classifier les differentes isometries lineaires. On effectue cette classification a l'aide de leurs points fixes.

DÉFINITION 3.20. 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 3.13. 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

$$\text{Fix}(\phi) = \ker(\phi - \text{Id}_{\mathbb{R}^2})$$

: c'est donc un sous-espace vectoriel de  $\mathbb{R}^2$  et sa dimension est 0, 1 ou 2.  $\square$

PROPOSITION 3.14. Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_0$  une isometrie lineaire alors un et un seul des cas suivant se presente

- $\phi = \text{Id}$  et  $\text{Fix}(\phi) = \mathbb{R}^2$ ,
- $\phi \in \text{Isom}(\mathbb{R}^2)_0^+$  et  $\text{Fix}(\phi) = \{\mathbf{0}\}$ ,
- $\phi \in \text{Isom}(\mathbb{R}^2)_0^+$  et  $\text{Fix}(\phi) = \mathbb{R}.\vec{u}$  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 ( $c^2 + s^2 = 1$ )

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

et le determinant de ce systeme vaut

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

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

- Supposons  $\phi$  non-speciale, le systeme devient ( $c^2 + s^2 = 1$ )

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

et le determinant de ce systeme vaut

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

Le systeme est degener (les deux lignes sont proportionnelles) mais le systeme est non-trivial (si  $s = 0$  alors  $c - 1$  ou  $c + 1$  est non-nul) et donc le systeme est equivalent a une de ses lignes (une de celles qui est non-nulle). L'ensemble des solutions est donc de la forme  $\mathbb{R}\vec{u}$  avec  $\nu = (-s, c - 1)$  si  $(c, s) \neq (1, 0)$  et  $\vec{u} = (1, 0)$  si  $(c, s) = (1, 0)$ .  $\square$

**3.2. Les symetries.** On etudie le cas ou  $\phi$  est non-speciale.

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 elements de  $\vec{u}^\perp$  sont les vecteurs  $\vec{v} = (x, y)$  verifiant le systeme lineaire

$$ax + by = 0$$

c'est a dire l'ensemble

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

$\square$

THÉORÈME 3.9. Soit  $\phi \in \text{Isom}(\mathbb{R}^2)_0^-$  et  $\text{Fix}(\phi) = \mathbb{R}\vec{u}$  la droite de ces points fixes. Soit  $\vec{v}$  un vecteur non-nul perpendiculaire a  $\vec{u}$  alors on a pour tout  $\vec{w} \in \mathbb{R}^2$

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

En particulier

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

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

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

est une isometrie lineaire non-speciale.

**Preuve:** Considerons  $\phi(\vec{v})$ : on a

$$\langle \phi(\vec{v}), \vec{u} \rangle = \langle \phi(\vec{v}), \phi(\vec{u}) \rangle = \langle \vec{v}, \vec{u} \rangle = 0$$

donc  $\phi(\vec{v}) \in \vec{u}^\perp$  et donc

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

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 a  $\vec{u}$ . On a donc demonstre (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 lineaire (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 3.3.** Une isométrie linéaire non-spéciale dont l'ensemble des points fixes est la droite  $\mathbb{R}\vec{u}$  ( $\vec{u} \neq \mathbf{0}$ ) sera appelée la symétrie orthogonale d'axe  $\mathbb{R}\vec{u}$ .

Les isométries linéaires non-spéciales sont appelées symétries et les matrices non-spéciales, matrices de symétrie.

### 3.3. Explication des symétries.

On a le formulaire suivant

THÉORÈME 3.10. 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

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

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 données 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  $\langle \vec{u}, \vec{v} \rangle = 0$ .  $\square$

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

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

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

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

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

$\square$

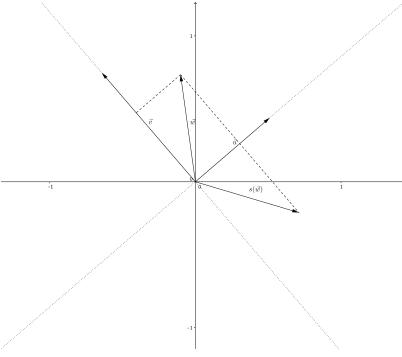


FIGURE 1. Exemple de symetrie lineaire.

**3.4. Rotations.** On considere maintenant le cas des isometries speciales

DÉFINITION 3.4. Une isometrie linéaire spéciale  $\phi$  sera appellée rotation de centre  $\mathbf{0}$ . On dira également que sa matrice est une matrice de rotation. Le groupe  $\text{Isom}(\mathbb{R}^2)_{\mathbf{0}}^+$  des isometries spéciales est encore appelle le groupe des rotations de centre  $\mathbf{0}$ .

Le groupe des rotations a la propriété fondamentale suivante:

THÉORÈME 3.11. 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  $P \in \mathbf{C}^1$  (par exemple  $P = \mathbf{e}_1 = (1, 0)$ ) 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 point  $Q$  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.

### 3.4.1. Angle de deux vecteurs.

DÉFINITION 3.5. *L'angle*

- de deux vecteurs unitaires  $\vec{u}, \vec{v} \in \mathbf{C}^1$  (de longueur 1) est l'unique rotation  $r_{\vec{u}, \vec{v}}$  qui envoie  $\vec{u}$  sur  $\vec{v}$ .
- de deux vecteurs non-nuls,  $\vec{u}, \vec{v}$ , est l'unique rotation  $r_{\vec{u}, \vec{v}}$  qui envoie  $\vec{u}/\|\vec{u}\|$  sur  $\vec{v}/\|\vec{v}\|$ .
- de deux demi-droites  $\mathbb{R}_{\geq 0}\vec{u}$  et  $\mathbb{R}_{\geq 0}\vec{v}$  est la rotation  $r_{\vec{u}, \vec{v}}$  qui envoie  $\vec{u}/\|\vec{u}\|$  sur  $\vec{v}/\|\vec{v}\|$  et donc  $\mathbb{R}_{\geq 0}\vec{u}$  sur  $\mathbb{R}_{\geq 0}\vec{v}$ . On note cet angle

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

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

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

- de deux droites passant par l'origine  $\mathbb{R}\vec{u}, \mathbb{R}\vec{v}$  est l'ensemble des deux rotations<sup>2</sup>  $\{r_{\vec{u}, \vec{v}}, -r_{\vec{u}, \vec{v}}\}$  qui envoient la droite  $\mathbb{R}\vec{u}$  sur la droite  $\mathbb{R}\vec{v}$ .

On fait également les définitions suivantes

- Un angle entre vecteurs ou deux demi-droites sera aussi appellé "angle orienté". Un angle entre deux droites (ie. un ensemble de deux angles orientés) sera appellé "angle non-orienté".
- L'ensemble des angles (orientés) est l'ensemble des rotations  $\text{Isom}(\mathbb{R}^2)_0^+$ ; c'est donc un groupe abélien et étant donné  $r, r'$  deux angles, la "somme" de ces angles est la rotation composée  $r \circ r' = r' \circ r$ .
- On définit de même la somme de deux angles non-orientés comme la paire  $\{r \circ r', -r \circ r'\}$ .
- On peut identifier une rotation  $r$  (donc un angle) avec sa matrice  $M_r = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}$  et donc représenter un angle par le vecteur de  $\mathbf{C}^1$ ,  $(c, s)$ . Le nombre  $c$  s'appelle le cosinus de l'angle  $r$  et le nombre  $s$  s'appelle son sinus. Avec cette représentation la "somme" des deux angles  $(c, s)$  et  $(c', s')$  est l'angle

$$(c'', s'') = (cc' - ss', sc' + cs').$$

EXERCICE 3.2. 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.

### 3.4.2. 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...".

---

<sup>2</sup>Si  $r$  est une rotation de matrice  $M$ ,  $-r$  est la rotation de matrice  $-M$

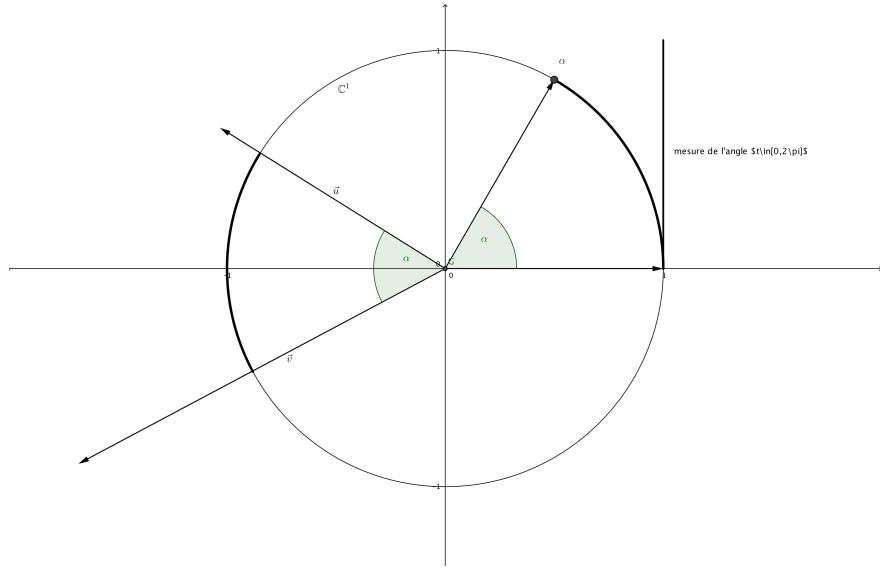


FIGURE 2. Deux paires de vecteurs representant le meme angle

- "parcouru dans le sens inverse des aiguilles d'une montre"

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

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

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

Alors

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

est un groupe abelien en bijection avec  $C^1$  et  $\text{Isom}(\mathbb{R}^2)_0^+$ .

**3.5. Classification des isometries affines.** On classifie maintenant les isometrie affines generales composees d'une translation et d'une isometrie lineaire:

$$\phi = t_{\phi(\mathbf{0})} \circ \phi_0.$$

On defini d'abord les notion d'isometries affines speciales et non-speciales

DÉFINITION 3.8. 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 (à gauche ou à droite) de  $\text{Isom}(\mathbb{R}^2)^+$  par un élément quelconque de  $\text{Isom}(\mathbb{R}^2)^-$ : pour toute symétrie affine  $s \in \text{Isom}(\mathbb{R}^2)^-$ , on a*

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

**Preuve:** Exercice; Indication: utiliser le théorème de structure du groupe des isométries directes et la fait que l'application partie linéaire  $\text{lin}: \text{Isom}(\mathbb{R}^2) \rightarrow \text{Isom}(\mathbb{R}^2)_0$  est un morphisme de groupe surjectif.  $\square$

REMARQUE 3.1. 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.*

*– Si la partie linéaire de  $r$  est l'identité  $r$  est une translation et  $\text{Fix}(r) = \emptyset$  sauf si le vecteur de translation est le vecteur nul: on a alors  $r = \text{Id}_{\mathbb{R}^2}$  et  $\text{Fix}(r) = \mathbb{R}^2$ .*

*– Si la partie linéaire de  $r$  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 3.15.** *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  $\text{Isom}(\mathbb{R}^2)_0^+$  (en particulier ils sont isomorphes.)*

**Preuve:** Exercice; considérer la conjugaison par la translation qui envoie  $\mathbf{0}$  sur  $P$ .  $\square$

**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

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

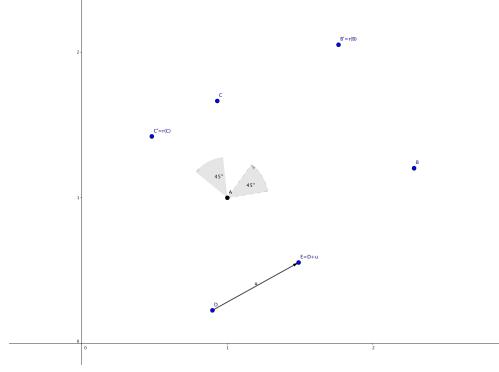


FIGURE 3. Exemple de translation, rotation ...

parallele 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 3.9. 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))

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

Resolvons 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

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

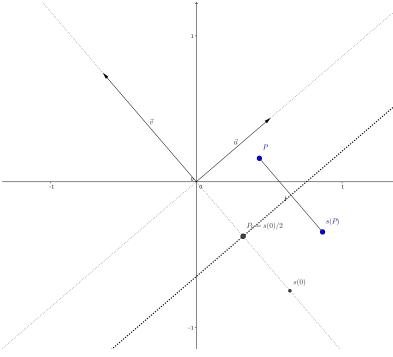
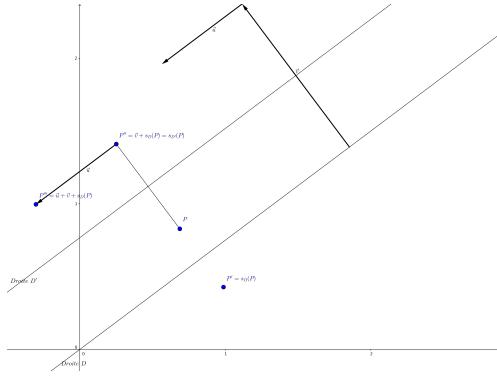


FIGURE 4. Exemple de symetrie affine axiale.

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

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

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

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 symetrie affine  $s$  se decompose sous la forme suivante:*

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

ou  $t' = t_{\vec{u}'}$  est une translation de vecteur  $\vec{u}'$  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:

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

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

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

Ainsi les matrices associes sont donnees par

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

avec

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

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

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

Soit  $P$  l'intersection des deux droites, alors  $P$  est un point fixe pour  $s_1$  et  $s_2$  et donc pour  $s_1 \circ s_2$  c'est donc le centre de  $r_3$ . On resoud donc le systeme

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

et on trouve

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

#### 4. Conclusion

Pour resumer, les isometries du plan sont constituees des

- **translations:** les elements de  $T(\mathbb{R}^2)$ ; elles appartiennent a  $\text{Isom}(\mathbb{R}^2)^+$  et ce sont les rotations dont la partie lineaire est l'identite. Elles n'ont aucun point fixe sauf la translation par le vecteur nul  $\mathbf{0}$  (c'est l'identite) et alors l'ensemble de ses points fixes est  $\mathbb{R}^2$  tout entier.
- **les rotations:** ce sont les elements de  $\text{Isom}(\mathbb{R}^2)^+$ ; elles sont composees d'une translation et d'une rotation lineaire; et si leur partie lineaire n'est pas l'identite (si ce ne sont pas des translations), elles ont exactement un point fixe, le centre de la rotation.
- **les symetries axiales:** elles appartiennent a  $\text{Isom}(\mathbb{R}^2)^-$  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 points fixes est la droite parallele a l'axe de la symetrie lineaire et passant par le milieu du segment de translation. Elles sont d'ordre 2.
- **les symetries glissees:** elles appartiennent a  $\text{Isom}(\mathbb{R}^2)^-$  et sont composees d'une translation et d'une symetrie lineaire telle que le vecteur de la translation n'est pas perpendiculaire au vecteur directeur de l'axe de la symetrie. Elles sont d'ordre infini (leur carre est une translation par un vecteur non-nul) et n'ont pas de point fixe.



## CHAPITRE 4

### Isometries et nombres complexes

Nous commençons par rappeler la construction des nombres complexes.

#### 1. Construction des nombres complexes

L'ensemble des nombres complexes  $\mathbb{C}$  s'obtient "concrètement", comme un sous-anneau de l'anneau des matrices  $2 \times 2$ : posont

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

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  $Z \in \mathbb{C}$  dans la base  $(\text{Id}, I)$  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

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

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  $Z, Z' \in \mathbb{C}$

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

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

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

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. De plus pour  $Z \neq 0$  son inverse est donnée par la formule usuelle

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

et

$${}^t Z = x\text{Id} - yI \in \mathbb{C}$$

donc

$$Z^{-1} \in \mathbb{C},$$

en d'autre termes  $\mathbb{C}$  est un corps.

1.0.5. *Conjugaison complexe.* On a vu que pour  $Z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathbb{C}$  la matrice 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  $\mathbb{C}$  (de reciproque la transposee). On l'appelle la conjugaison complexe et on la note*

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

On a

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

et

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

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

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

La quantité

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

s'appelle le module de  $Z$  et on a donc la formule

$$Z \cdot \bar{Z} = |Z|^2 \text{Id}.$$

1.0.6. *Structure euclidienne.* L'ensemble des nombres complexes est muni d'un produit scalaire (bilineaire, symétrique, défini positif) donné par

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

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 réelles 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 isométrie 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 nombres reels  $\mathbb{R}$  s'identifie donc a un sous-corps du corps des nombres complexes.

On simplifiera les notations en notant 1 a la place de l'identité et  $i$  a la place de la matrice  $I$ : ainsi un nombre complexe s'ecrira sous la forme

$$z = x + iy.$$

Avec ces notations on a donc

$$z + z' = (x + x') + i(y + y'), \quad z.\bar{z} = x^2 + y^2 = |z|^2, \quad z^{-1} = \bar{z}/|z|^2$$

## 2. Interpretation des isometries en termes de nombres complexes

L'isomorphisme (1.1) identifie le corps des complexes  $\mathbb{C}$  avec le plan reel  $\mathbb{R}^2$ . On va voir que plusieurs transformations du plan (notamment les isometries) admettent une interpretation simple en terme de nombres complexes.

-*Translations.* Soit  $\vec{u} = (u, v) \in \mathbb{R}^2$ , la translation  $t_{\vec{u}}$  est la transformation

$$t_{\vec{u}} : \vec{x} = (x, y) \in \mathbb{R}^2 \mapsto \vec{u} + \vec{x} = (u, v) + (x, y) = (x + u, y + v).$$

Il lui correspond la translation dans le corps des complexes: pour  $\nu = u + iv \in \mathbb{C}$

$$t_{\nu} : z \in \mathbb{C} \mapsto z + \nu \in \mathbb{C}.$$

-*Rotations lineaires.* Soit  $\rho = c + is \in \mathbb{C}$ , 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  $\{1, i\}$  s'ecrit

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

(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

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

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*

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

est un isomorphisme de groupes. En particulier (car  $\rho^{-1} = \overline{\rho}$  pour  $\rho \in \mathbb{C}^1$ )

$$r_\rho^{-1} = r_{\rho^{-1}} = r_{\bar{\rho}}.$$

– *Symétries linéaires.* La conjugaison complexe est définie (en notation simplifiée) est définie par

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

Elle vérifie

– Linearité:

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

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

– Multiplicativité:

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

– 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 noté  $|z|$ . Il vérifie

$$|z.z'| = |z||z'|.$$

– 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

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

– Caractérisation des nombres réels 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 linéaire dans la base  $(1, i)$  est

$$M_{\bar{z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Cette application  $z \mapsto \bar{z}$  correspond donc à la symétrie 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 symétrique de  $(x, y)$  par rapport à l'axe des  $x$ .

Plus généralement, on a vu que toute symétrie linéaire  $s$  se décompose en la composition d'une rotation et d'une symétrie fixée (ou de manière équivalente la matrice associée se décompose en produit d'une matrice de rotation et d'une matrice de symétrie). Prenant comme symétrie la symétrie  $s_{\mathbf{e}_1}$  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

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

REMARQUE 2.1. Notons egalement que

$$\overline{\rho.z} = \overline{\rho}.\overline{z}$$

ainsi la symetrie

$$s_\rho = s_{\mathbf{e}_1} \circ r_\rho$$

s'ecrit egalement comme la composee

$$s_\rho = r_{\overline{\rho}} \circ s_{\mathbf{e}_1} = r_\rho^{-1} \circ s_{\mathbf{e}_1}.$$

On retrouve ainsi un cas particulier du fait que si  $r$  est une rotation lineaire et  $s$  une symetrie lineaire

$$r \circ s = s \circ r^{-1}.$$

*Homotheties.* Soit  $\lambda \in \mathbb{R}^\times$ , la multiplication

$$[\times \lambda] : \begin{array}{ccc} \mathbb{C} & \mapsto & \mathbb{C} \\ z & \mapsto & \lambda z \end{array}$$

correspond a l'application lineaire

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

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

*Homotheties affines.*

DÉFINITION 4.4. *Etant donne  $\vec{u} \in \mathbb{R}^2$ , une application de la forme*

$$h_{\lambda, \vec{u}} := t_{\vec{u}} \circ h_{\lambda, 0}$$

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

REMARQUE 2.2. C'est une application affine, bijective et telle que  $\text{Fix}(h_{\lambda, \vec{u}})$  est reduit a un point sauf si  $\lambda = 1$ ; dans ce dernier cas  $\text{Fix}(h_{1, \vec{u}}) = \mathbb{R}^2$  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 homothetie affine correspond a la transformation de  $\mathbb{C}$  donnee par

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

### Isometries generales.

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

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

avec

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

La partie lineaire  $\varphi_0$  est donnee par

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

et leur matrices sont donnees 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  $\varphi \in \text{Isom}(\mathbb{R}^2)^-$ . Les nombres complexes  $(\rho, \nu)$  associes a  $r_{\rho, \nu}$  et  $s_{\rho, \nu}$  (ou bien seulement  $\rho$  si on considere les isometries lineaires  $r_\rho$  et  $s_\rho$ ) sont appeles parametres complexes des ces isometries.

### 2.1. Angle et nombre complexes.

**2.2. Mesure d'un angle.** Un angle correspond donc a une rotation et donc a un nombre complex de module 1,  $\alpha$ , ou encore un point sur le cercle unité. Pour des raisons pratiques, on preferera souvent representer un angle par un nombre reel: pour cela on mesure la longueur de l'arc du cercle unite  $\mathbb{C}^1$  compris entre 1 et  $\alpha$  (ou encore la longueur de l'arc de cercle unite determine par les deux vecteurs  $\vec{u}, \vec{v}$ : cela necessite de definir rigoureusement ce qu'est la longueur d'un arc de cercle ce qui implique la notion d'integrale le long de courbe; cela sera defini rigoureusement au semestre de printemps).

Au lieu de cela, on admettra le resultat suivant de nature algebrique/analytique

THÉORÈME 4.2. *Il existe un morphisme de groupe non-trivial*

$$\phi_1 : (\mathbb{R}, +) \mapsto (\mathbb{C}^1, \times)$$

*qui est derivable (la fonction  $t \mapsto \phi_1(t) = x_1(t) + iy_1(t)$  est derivable) et tel que  $\phi'_1(0) = i$ . Ce morphisme est surjectif et on a*

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

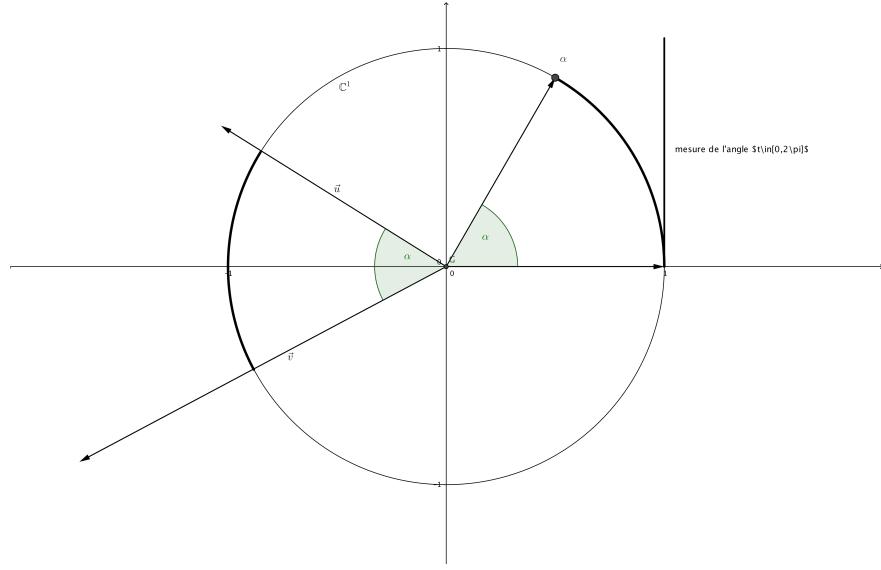


FIGURE 1. Deux paires de vecteurs representant le meme angle

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

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

Les derivees ens sont donc egales: on obtient alors  $\forall s, t \in \mathbb{R}$

$$\phi'(s+t) = \phi'(s)\phi(t)$$

et

$$-\phi'(-s) = \overline{\phi'(s)}.$$

En  $s = 0$  on obtient que

$$\phi'(t) = \phi'(0)\phi(t)$$

et

$$-\phi'(0) = \overline{\phi'(0)} \Rightarrow \phi'(0) = \lambda i \in i\mathbb{R}.$$

Notons que  $\lambda \neq 0$  car sinon

$$\forall t, \phi'(t) = 0$$

et  $\phi$  serait constant. On a

$$\phi'(t) = \phi'(0)\phi(t)$$

de sorte que

$$\forall t, |\phi'(t)| = |\lambda|.$$

Ce qui s'interprete en disant que  $\phi(t)$  parcours le cercle  $\mathbb{C}^1$  a vitesse constante.

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

Soit  $\psi : (\mathbb{R}, +) \rightarrow \mathbb{C}^1$  un autre morphisme derivable  $\psi'(0) = i\mu$  alors

$$\varphi : t \mapsto \psi(t/\mu)\phi_1(t)^{-1} = \psi(t/\mu)\phi_1(-t)$$

est un morphisme de groupe derivable tel que

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

Ce morphisme est donc constant egal a 1. □

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

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

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

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

( 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 appelle l'argument de  $z$  et est note  $\arg(z)$ .

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

Ainsi dans ce language on a le resultat tautologique suivant:

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

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

- 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 parametrisation est importante car elle permet d'ordonner les angles par l'ordre naturel de l'intervalle  $[0, 2\pi[$ : on dira qu'un angle est plus petit qu'un autre si son parametre reel dans  $[0, 2\pi[$  est plus petit que celui de l'autre angle; on peut egalement parler de secteur angulaire par rapport a un segment oriente  $[P, Q]$  associe a un intervalle  $I \subset [0, 2\pi[$  comme etant l'ensemble des points  $R$  du plan tel que le parametre reel associe a l'angle  $\widehat{QPR}$  appartienne a l'intervalle  $I$ .

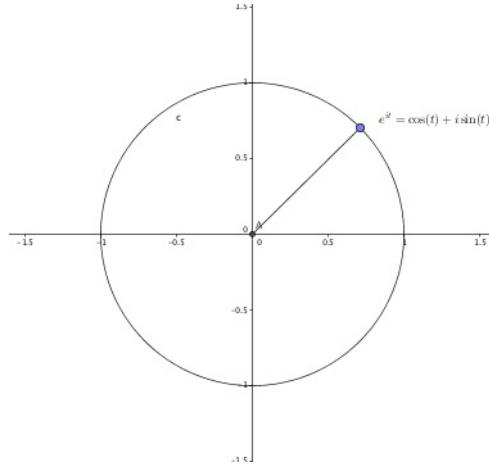


FIGURE 2. Le cercle trigonométrique

2.2.1. *Trigonometrie.* On peut également en déduire 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 dérivable 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.*