GROUPES ET SYMÉTRIES

Table des matières

I. Structure des groupes et Groupes Symétriques

1. Introduction et motivations

La notion de groupes a déjà été introduite dans les cours de L1 (algèbre I par exemple) et le cours d'arithmétique de L2.

Cette notion de groupes, c'est à dire de structure multiplicative dont tout élément admet un inverse, a été rencontrée

- surtout dans le *cas commutatif* en particulier en arithmétique où la notion de groupes décrivait les opérations que l'on avait sur les nombres et leurs classes d'équivalence modulo un entier n ;
- mais vous avez aussi rencontré cette notion dans le cadre *non-commutatif* : via le produit de matrices inversibles ($AB \neq BA$ en général) ou la composition d'applications (bijectives).

La notion de "groupe" en mathématiques est l'axiomatisation et l'étude des similitudes entre les propriétés des nombres et congruences en arithmétique, la multiplication matricielle en algèbre linéaire, les compositions de bijection en analyse ou mathématique discrète. Plus généralement, la notion de groupe encode les "transformations" qui agissent sur des ensembles et préservent des structures (de nature géométrique ou algébrique).

Exemple 1.1. La géométrie est une source importante d'exemples de groupes (et vice-versa). En effet, en géométrie on étudie des transformations entre objets géométriques, que ce soit des points, droites, cercles... Par exemple on s'intéresse(ra) aux groupes des translations, rotations, symétries, ou bien aux propriétés remarquables des triangles (intersection des bissectrices, médianes etc...).

D'une manière générale un groupe apparaît souvent comme le groupe des transformations possibles d'une structure ou d'objets géométriques. Autrement dit

la notion de groupe encode les symétries d'un système.

Pour récapituler, les *groupes* apparaissent en

- *arithmétique*,
- *algèbre linéaire*,
- *géométrie*,
- *mathématique discrète et combinatoire*,
- *physique, mécanique et chimie*

Dans les trois derniers cas, les groupes sont vraiment pensés comme encodant des symétries et les transfomations admissibles de ces structures. Ce point de vue existe aussi dans les deux premiers cas, mais de manière plus cachée.

Comme on le voit, la notion de groupes est donc très importante en mathématique et ses applications. Dans ce cours nous allons commencer par étudier cette notion, les propriétés abstraites des groupes et voir comment ils encodent des transformations : ce sera la notion d'action de groupes. Nous étudierons ensuite en détail l'exemple fondamental des groupes symétriques qui interviennent dans de nombreux domaines et applications.

Enfin nous étudierons plus spécifiquement des exemples de groupes en géométrie et vu comme symétries, illustrant ainsi la théorie générale.

Nous laisserons évidemment pour les années et études futures un grand nombre d'aspect de la théorie et de ses applications que nous n'aurons pas le temps d'étudier.

2. Structure de groupe et exemples

2.1. **Définition et exemples fondamentaux de groupes.** Commençons par rappeler la notion de groupes. Tout d'abord une **loi de composition interne** sur un ensemble E est une application $E \times E \to E$. Autrement dit quelque chose qui prend deux éléments de E et les transforme en un troisième. On l'appellera parfois tout simplement multiplication (ou dans de nombreux exemples commutatif, addition).

Définition 2.1. Un groupe est un couple $(G, *)$ où G est un ensemble et $* : G \times G \to G$ est une loi de composition interne vérifiant les propriétés suivantes :

(1) (**associativité**) : pour tout $x, y, z \in G$, on a $(x * y) * z = x * (y * z)$;
(2) (**existence du neutre**) : il existe un élément $e \in G$ qui est neutre, c'est à dire tel que pour tout $g \in G$, on a $e * g = g = g * e$;
(3) (**existence d'inverses)** : pour tout élément $g \in G$, il existe un élément $g^{-1} \in G$ tel que $g * g^{-1} = e = g^{-1} * g$. On appelle g^{-1} l'inverse de g (cet élément est forcément unique, voir 2.3).

Un groupe $(G, *)$ est dit **abélien** (ou **commutatif** selon les auteurs [1]) s'il vérifie la propriété de commutativité usuelle suivante :

$$\text{pour tout } x, y \in G, \text{ on a : } \quad x * y = y * x.$$

La propriété d'associativité dit que l'on a pas besoin de se soucier des parenthèses quand on multiplie des éléments d'un groupe. Autrement dit, on peut oublier les parenthèses sans soucis ! En particulier on peut écrire $x * y * z$ dans un groupe sans ambiguïté puisqu'il n'est pas important de savoir par quel produit on commence.

Si un groupe est commutatif, cela veut dire que l'on peut en plus multiplier les éléments dans la position que l'on veut. Par exemple $x * y * z = z * x * y = x * z * y$.

Notons aussi que dans la définition d'un inverse il faut vérifier deux équations : $g * g^{-1} = e$ et $g^{-1} * g = e$. Elles sont en général indépendantes. Sauf bien-entendu dans un groupe commutatif où elles sont équivalentes et où il suffit donc d'en vérifier une seule.

Remarque 2.2 (Un groupe est la donnée d'une structure sur un ensemble). La donnée de la loi interne $*$ fait partie de la définition d'un groupe. Autrement dit un groupe est un ensemble muni d'une loi précise. En particulier dire qu'un ensemble est un groupe n'a *aucun sens*. Pour parler de groupe il faut préciser l'ensemble **et** la loi interne (voire cependant les conventions 2.7 ci-dessous).

Quelques propriétés 2.3. Explicitons quelques conséquences immédiates des définitions, qui prècise aussi le sens de la définition d'un groupe.

(1) *Si* $(E, *)$ *est un ensemble muni d'une loi de composition interne, il admet* au plus *élément neutre*. Donc en particulier, *un groupe* $(G, *)$ *a un* unique *élément neutre* ; ce qui est heureux sinon la notion d'inverse dans un groupe (la propriété 3 de la définition 2.1 serait un peu ambigüe.

Démonstration : soit e et e' des éléments neutres. Il faut montrer que $e = e'$. Or, par définition, puisque e est neutre $e * e' = e'$. Mais comme e' est lui aussi neutre on a aussi $e * e' = e$. Ainsi $e = e * e' = e'$.

(2) *Un élément* g *dans un groupe* $(G, *)$ *admet un* unique *inverse*. En effet supposons que g^{-1} et h soient des inverses de g. En particulier $h * g = e = g * h$. On a alors

$$g^{-1} = e * g^{-1} = (h * g) * g^{-1} = h * (g * g^{-1}) = h * e = h$$

où on a utilise l'associativité de $*$ au milieu et que e est neutre à la fin et au début. Cette preuve montre qu'en fait, si on a une loi de composition interne $*$ sur un

1. nous utiliserons les deux terminologies pour vous habituer

ensemble E qui admet un élément neutre, alors tout élément admet au plus un inverse.

(3) *L'inverse de g^{-1} est g.* Cela se voit immédiatement de la définition.

(4) *Un groupe $(G, *)$ est non vide.* Il contient forcément un élément neutre par définition.

(5) *Pour tous $g, h \in G$, on a $(g * h)^{-1} = h^{-1} * g^{-1}$.*

Démonstration : par définition de l'inverse, il suffit de vérifier que $(h^{-1} * g^{-1}) * (g * h) = e$ et $e = (g * h) * (h^{-1} * g^{-1})$. Regardons le premier cas, le deuxième se démontrant de la même manière. On a

$$\begin{aligned}(h^{-1} * g^{-1}) * (g * h) &= ((h^{-1} * g^{-1}) * g) * h \text{ (par associativité de } *) \\ &= (h^{-1} * (g^{-1} * g)) * h \text{ (par associativité de } *) \\ &= (h^{-1} * e) * h \text{ (par définition de l'inverse)} \\ &= h^{-1} * h = e \text{ (par définition du neutre puis de l'inverse).}\end{aligned}$$

On prendra garde au fait que le sens du produit est inversé en passant à l'inverse (ceci n'a aucune importance dans un groupe commutatif bien-sûr).

Notation 2.4. On notera en général e le neutre d'un groupe. En présence de plusieurs groupes on notera parfois e_G le neutre d'un groupe $(G, *)$ e_H celui d'un groupe $(H, \cdot)$ lorsque l'on veut les différencier.

Voici quelques exemples standards (à connaître) de groupes commutatifs.

Exemple 2.5.

- Un singleton $\{e\}$ a une structure de groupes unique dont e est l'élément neutre. Autrement dit $e * e = e$. On appelle un tel groupe, le groupe trivial.
- Les entiers relatifs $(\mathbb{Z}, +)$ munis de l'addition sont un groupe abélien dont le neutre est 0 et l'inverse de n est $-n$. En revanche $(\mathbb{N}, +)$ n'est pas un groupe. On a bien 0 qui est neutre et l'associativité, mais par exemple 1 n'a pas d'inverse (pour l'addition).
- Les entiers relatifs $(\mathbb{Z}, \times)$ muni de la multiplication ne forment pas un groupe.
- On a que $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}, +)$ sont des groupes tout comme $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$. De manière générale, dans tout corps $(\mathbb{K}, +, \times)$, $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \times)$ sont des groupes abéliens [2].
- Si E est un espace vectoriel sur un corps $\mathbb{K}$, alors $(E, +)$ est un groupe abélien.
- Comme vue en arithmétique $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien dont la construction sera revue en TD.
- L'ensemble $(\{1, -1\}, \times)$ est un groupe abélien.

Exercice 2.6. Démontrer les affirmations données dans l'exemple (une bonne partie sera (re)vue en TD).

Notations et Conventions 2.7. On a vu ci-dessus que dire qu'un ensemble est un groupe n'a pas de sens. Il arrive cependant parfois que l'on écrive : soit G un groupe. Cela signifie en fait bien sûr que l'on se donne un groupe $(G, *)$ mais qu'on a eu la flemme de préciser la notation pour $*$.

Par ailleurs, il existe plusieurs groupes canoniques où on ne précisera pas la loi ; car elle est sous-entendue. Ainsi quand on parlera du groupe $\mathbb{Z}$ cela sera sous-entendu que l'on parle de $(\mathbb{Z}, +)$ muni de la loi d'addition ; de même pour $\mathbb{R}$ ou $\mathbb{R}^*$ (avec la multiplication pour ce dernier bien-sûr).

Ces raccourcis de langages et notations sont fréquents dans les ouvrages mathématiques et nous les commetront occasionnellement aussi pour vous y habituer et parce qu'ils sont bien pratiques.

2. Ici on utilise la notation standard $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ pour tout corps $\mathbb{K}$

Remarque 2.8 (**Point clé : la simplification dans un groupe)**. Une partie importante de la propriété des groupes généraux qui provient de l'existence d'inverses est que l'on *peut simplifier les équations* dans un groupe. C'est précisément ce que dit le lemme suivant.

Lemme 2.9. *Soit $(G, *)$ un groupe.*

- *Alors*
$$\forall g, h, h' \in G, \quad (g * h = g * h') \iff (h = h')$$
et de même
$$(h * g = h' * g) \iff (h = h').$$
- *De plus, $\forall g, h, h' \in G$, on a les équivalences*
$$(g * h = h' \iff h = g^{-1} * h'), \qquad (h * g = h' \iff h = h' * g^{-1}),$$
$$g = h \iff e = g^{-1} * h \iff g * h^{-1} = e$$

Démonstration. Regardons la première assertion. Le sens $\Leftarrow$ de l'équivalence est facile. Il suffit de multiplier l'équation $h = h'$ à droite ou à gauche par g.

Dans l'autre sens, c'est là que l'on va utiliser que l'on a des inverses. En effet, si $h * g = h' * g$, alors en multipliant par g^{-1} à droite on obtient l'égalité :

$$\begin{aligned}
(h * g) * g^{-1} &= (h' * g) * g^{-1} \\
h * (g * g^{-1}) &= h' * (g * g^{-1}) \text{ (par associativité de } *) \\
h * e &= h' * e \text{ (par définition de l'inverse)} \\
h &= h' \text{ (par définition de l'élément neutre).}
\end{aligned}$$

Le cas de la simplification à gauche est évidemment similaire.

La deuxième assertion se démontre de la même manière. En effet, si $g * h = h'$, en mutlipliant à gauche par g^{-1}, on a

$$\begin{aligned}
g^{-1} * (g * h) &= g^{-1} * h' \\
(g^{-1} * g) * h &= g^{-1} * h' \text{ (par associativité)} \\
e * h &= g^{-1} * h' \text{ (par définition de l'inverse)} \\
h &= g^{-1} * h' \text{ (par définition de l'élément neutre).}
\end{aligned}$$

L'autre sens se démontre en multipliant par g, et l'autre équivalence est similaire.

Enfin la dernière assertion est une conséqience de la précédente en prenant $g = g$, $h = e$ et $h' = h$: En effet $g = h$ est équivalent à $g * e = h$ par définition du neutre. □

Ce lemme dit qu'on peut simplifier une équation comme on simplifie des équations dans les réels différents de 0 (où on utilise en fait justement que $(\mathbb{R}^*, \times)$ est un groupe sans y penser bien-sûr).

À retenir : dans un groupe on peut donc faire passer un élément de la gauche d'une équation à la droite en le transformant en son inverse !

C'est exactement ce que dit le lemme tout comme la simplification.

Nous avons détaillé dans cette partie comment on utilise les axiomes des groupes dans les preuves du lemme 2.9 ou des propriétés 2.3 précédentes. Nous ne le ferons pas tout le long des notes et il est important d'apprendre à maitriser ces étapes et qu'elles deviennent intuitives et automatiques ! En d'autres termes, entrainez vous absolument à comprendre et démontrer ce genre de résultats et les propriétés 2.3. Ainsi qu'à simplifier et faire passer des éléments d'un groupe d'un côté à l'autre d'une identité comme dans la remarque et le lemme ci-dessus.

Nous allons maintenant donner des exemples de groupes *non*-commutatifs.

Exemple 2.10.
- Soit X un ensemble, alors l'ensemble $(\{f : X \to X,\ f \text{ est bijective}\}, \circ)$ des applications bijectives de X dans X muni de la composition des applications est un groupe, non-commutatif (sauf si $\text{card}(X) \leq 2$ comme on le verra), cf proposition 2.11.
- L'ensemble $(GL(E), \circ)$ des isomorphismes linéaires d'un espace vectoriel muni de la composition est un groupe non-abélien (sauf si $\dim(E) \leq 1$) tout comme $(GL_n(\mathbb{K}), \times)$ les matrices inversibles à coefficient dans un corps $\mathbb{K}$ muni de la multiplication de matrice.
- Le sous-ensemble des applications bijectives de $\mathbb{R}^2$ dans $\mathbb{R}^2$ qui envoie le carré $[-1, 1]^2$ sur lui-même, muni de la composition des applications, est un groupe non-commutatif.

La plupart de ces exemples seront détaillés en TD. Pour le premier exemple, c'est inclus dans la proposition suivante.

Rappelons que pour tout ensemble E, l'application identité, notée $\text{id}_E : E \to E$ ou simplement id (quand E est sous-entendu) est l'application $x \mapsto x$; c'est à dire qui ne fait rien.

Proposition 2.11. *Soit E un ensemble. On note $\text{Hom}(E, E) := \{f : E \to E\}$ l'ensemble des applications de E dans E.*

(1) La composition des applications $(f, g) \mapsto f \circ g$ est une loi de composition interne sur $\text{Hom}(E, E)$ qui est associative.
(2) L'application identité $id_E : E \to E$ est élément neutre pour $\circ$.
(3) Une application $g \in \text{Hom}(E, E)$ admet un inverse si et seulement si elle est bijective. Auquel cas son inverse est l'application réciproque g^{-1}.
(4) Le sous-ensemble $\text{Bij}(E) := \{f : E \to E,\ f \text{ est bijective}\}$ des bijections de E dans E muni de la loi de composition $\circ$ est un groupe.

Démonstration. Le premier point provient simplement du fait que si $X \xrightarrow{f} Y$ et $Y \xrightarrow{g} Z$ sont des applications, alors leur composée est l'application $x \mapsto g(f(x))$ qui est bien définie et va de X dans Z. En prenant $X = Y = Z = E$ on obtient (1) puisque par ailleurs $(f \circ g) \circ h = f \circ (g \circ h)$ pour tout triplet d'applications composables.

Pour (2), on vérifie que quelle que soit $f : E \to E$, on a $f \circ \text{id}_E = f$ et $\text{id}_E \circ f = f$. C'est équivalent à vérifier que pour tout $x \in E$, on a $f \circ \text{id}_E(x) = f(x)$ et $id_E \circ f(x) = f(x)$. Or par définition de la composée, on a

$$f \circ \text{id}_E(x) = f(\text{id}_E(x)) = f(x); \qquad \text{id}_E \circ f(x) = \text{id}_E(f(x)) = f(x)$$

en utilisant la définition de l'application identité.

Le point (3) est le seul non-trivial dans cette proposition. Tout d'abord, si g est bijectve, alors, par définition de sa fonction réciproque, on a bien que $g \circ g^{-1} = \text{id}_E = g^{-1} \circ g$ et celle-ci est bien un inverse de g donc.

Il reste à voir le sens inverse. Soit donc $g : E \to E$ une application inversible pour la loi de composition interne $\circ$. Notons f son inverse : autrement dit $f \circ g = \text{id}_E$ et $g \circ f = \text{id}_E$. Rappelons que la première équation implique que $f \circ g$ est injective car id_E l'est d'où il suit que g est injective aussi (voir les cours des années précédentes). De $g \circ f = \text{id}_E$ on déduit que $g \circ f$ est surjective (car id_E l'est) et ainsi g est surjective. Ainsi g est injective et surjective donc bijective. Comme sa fonction réciproque comme nous l'avons vu est un inverse, par unicité de l'inverse possible (cf 2.3.(2)), nous avons que $f = g^{-1}$.

Pour le point (4), il nous suffit vu (1), (2) et (3) de vérifier que la composée de bijections est une bijection (pour que la loi reste interne dans $\text{Bij}(E)$) et que l'application réciproque d'une bijection est une bijection. Ce dernier point est du cours de L1 [3], ce qui prouve que

3. il s'agit du résultat qui dit qu'une application est bijective (au sens injective et surjective) si et seulement si elle admet une application réciproque

toute bijection a bien un inverse dans les bijections. Enfin si f et g sont des bijections alors $f \circ g$ est injective car composée d'injections et surjective car composée de surjections (on laisse cette affirmation en exercice vu en L1). □

Exemple 2.12. Si $E = \emptyset$ est l'ensemble vide, alors $\mathrm{Hom}(E, E)$ contient une unique application, qui est l'identité et $\mathrm{Bij}(E)$ est le groupe trivial réduit à un élément.

Si $E = \{e\}$ est un singleton alors $\mathrm{Hom}(E, E) = \{\mathrm{id}_E\}$ et on a encore un groupe trivial.

Si $E = \{a, b\}$, alors, $\mathrm{Hom}(E, E)$ contient 4 applications et deux seulement sont des bijections : l'identité et l'application qui permute a et b (appelée transposition) : $\tau : \{a, b\} \to \{a, b\}$ définie par $\tau(a) = b$ et $\tau(b) = a$. Il est facile de voir que $\tau \circ \tau = \mathrm{id}_E$ ce qui décrit toute la structure du groupe $\mathrm{Bij}(\{a, b\})$. Tous ces exemples sont abéliens. On verra que ce n'est plus le cas si $\mathrm{card}(E) \geq 3$.

2.2. **Comment comparer des groupes : sous-groupes et morphismes de groupes.** On va s'intéresser maintenant à comparer des groupes. Comme on l'a dit un groupe est plus qu'un ensemble. Il vient avec une multiplication (la loi de composition interne). Pour comparer des groupes on va donc comparer les ensembles via des applications mais on va demander que ces applications soient compatibles avec les multiplications (et donc comparent ces multiplications) car sinon cela revient à oublier la structure des groupes. C'est le sens de la définition suivante

Définition 2.13. Soit $(G, *)$, $(H, \cdot)$ deux groupes. Un morphisme de groupes de $(G, *)$ vers $(H, \cdot)$ est une application $f : G \to H$ qui vérifie que

$$\forall g_1, g_2 \in G, \text{ on a } f(g_1 * g_2) = f(g_1) \cdot f(g_2).$$

Un morphisme de groupes $f : (G, *) \to (H, \cdot)$ est un *isomorphisme* de groupes s'il est en plus bijectif.

Un morphisme de groupes est souvent appelé *homomorphisme* (de groupes) dans la littérature mathématique. J'ai choisi d'utiliser la notation raccourcie [4]. En général, par abus de notation on écrira simplement que f est un morphisme de groupes de G vers H (ou que $f : G \to H$ est un morphisme de groupes) lorsque les lois de groupes sur G et H sont sous-entendues (ou génériques).

Lemme 2.14. *Soit $f : (G, *) \to (H, \cdot)$ un morphisme de groupes. Alors on a $f(e_G) = e_H$*
De plus pour tout $g \in G$, on a $f(g^{-1}) = f(g)^{-1}$.

Autrement dit un morphisme de groupe envoie automatiquement l'élément neutre sur l'élément neutre et l'inverse sur l'inverse.

Démonstration. On va utiliser que l'on peut simplifier dans un groupe. Montrons la première propriété. Par définition du neutre on a $e_G = e_G * e_G$ et donc

$$f(e_G) = f(e_G * e_G) = f(e_G) \cdot f(e_G) \text{ (car } f \text{ et un morphisme de groupes).}$$

On simplifie $f(e_G) = f(e_G) \cdot f(e_G)$ par $f(e_G)$ comme dans la dernière équivalence du lemme 2.9. Cela donne $e_H = f(e_G)$ comme énoncé.

Soit maintenant $g \in G$. On a $g * g^{-1} = e_G$ En appliquant f et en utilisant que c'est un morphisme de groupes, on a

$$f(g) \cdot f(g^{-1}) = f(g * g^{-1}) = f(e_G) = e_H$$

par ce que l'on vient de démontrer. De même on montre que $f(g^{-1}) \cdot f(g) = f(g^{-1} * g) = f(e_G) = e_H$. Il suit que $f(g^{-1})$ est bien l'inverse de $f(g)$ par définition (et unicité) de l'inverse dans un groupe. □

4. qui est aussi plus en phase avec la théorie des catégories

Remarque 2.15. On notera que la preuve du lemme utilise que tout élément est inversible. Ce n'est effectivement pas vrai que tout morphisme vérifiant $f(xy) = f(x)f(y)$ dans un anneau, par exemple, envoie 1 (le neutre pour la multiplication) sur 1 ; précisément car les éléments d'un anneau ne sont pas forcément inversibles. En particulier une application f entre monoide [5] qui vérifie $f(x * y) = f(x) \cdot f(y)$ n'envoie pas forcément le neutre sur le neutre.

Lemme 2.16. *Soit f un* isomorphisme *de groupes. Alors l'application réciproque f^{-1} est aussi un morphisme de groupes.*

Autrement dit, on aurait pu définir de manière équivalente un isomorphisme de groupes comme un morphisme de groupes qui admet un inverse qui est aussi un morphisme de groupes [6].

Démonstration. L'idée est une technique qui revient souvent avec les applications bijectives. C'est bien de la comprendre.

On doit montrer que pour tout $h_1, h_2 \in H$, on a $f^{-1}(h_1 \cdot h_2) = f^{-1}(h_1) * f^{-1}(h_2)$ (dans G). Par bijectivité de f, on a des g_1, g_2 (uniques) tels que $f(g_1) = h_1$, $f(g_2) = h_2$ (et $f^{-1}(h_i) = g_i$, $i = 1, 2$). On en déduit d'une part que

$$f^{-1}(h_1) * f^{-1}(h_2) = f^{-1}(f(g_1)) * f^{-1}(f(g_2) = g_1 * g_2)$$

et d'autre part, en utilisant que f est un morphisme de groupes, on a que

$$f^{-1}(h_1 \cdot h_2) = f^{-1}(f(g_1) \cdot f(g_2)) = f^{-1}(f(g_1 * g_2)) = g_1 * g_2.$$

Ces deux égalités nous donnent donc bien $f^{-1}(h_1 \cdot h_2) = f^{-1}(h_1) * f^{-1}(h_2)$. □

Voyons quelques exemples classiques, détaillés notamment en TDs

Exemple 2.17.

- Quel que soit G un groupe, l'identité $\mathrm{id} : G \to G$ est un morphisme de groupes.
- Quel que soient G, H des groupes, l'application constante $g \mapsto e_H$ est un morphisme de groupes. En revanche, pour tout $h_0 \neq e_H$, l'application constante $g \mapsto h_0$ n'est pas un morphisme de groupes.
- Pour tout groupe trivial $\{e\}$ et tout groupe G, l'application $e \mapsto e_G$ est un morphisme de groupes. Qui n'est un isomorphisme que si G est aussi trivial.
- L'application $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$, $x \mapsto \exp(x)$ est un morphisme de groupes car $\exp(a + b) = \exp(a)\exp(b)$. Ce n'est *pas* un isomorphisme. En revanche sa restriction (à son image) $\exp : (\mathbb{R}, +) \to (]0, +\infty[, \times)$ est un isomorphisme de groupes d'inverse $\ln :]0, +\infty[, \times) \to (\mathbb{R}, +)$.
- Toute application linéaire $f : E \to F$ entre espaces vectoriels est un morphisme de groupes $(E, +) \to (F, +)$ et c'est un isomorphisme de groupes si f est un isomorphisme linéaire.
- L'application quotient $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \overline{k}^n$ est un morphisme de groupes (pour les structures additives bien-sûr).
- Pour tout corps $\mathbb{F}$, l'application $\det : GL_n(\mathbb{F}) \to (\mathbb{F}^*, \times)$ est un morphisme de groupes.

5. un ensemble muni d'une loi de composition interne associative admettant un élément neutre

6. cette dernière est la bonne notion d'isomorphisme en général. Il se trouve que pour les groupes, c'est équivalent à être simplement bijectif et un morphisme de groupes. Mais ce n'est pas le cas pour toutes les structures mathématiques

- Pour tout groupe $(G, *)$ et tout élément $g \in G$, les puissances entières forment un morphisme de groupes. Plus précisément, notons pour tout entier $n \in \mathbb{Z}$,

$$g^{*n} := \begin{cases} \overbrace{g * \cdots * g}^{n \text{ termes}} & \text{si } n > 0 \\ e_G & \text{si } n = 0 \\ \underbrace{g^{-1} * \cdots * g^{-1}}_{-n \text{ termes}} & \text{si } n < 0. \end{cases} \tag{1}$$

  L'application $n \mapsto g^{*n}$ est un morphisme de groupes $(\mathbb{Z}, +) \to (G, *)$: autrement dit pour tout $i, j \in \mathbb{Z}$, on a

$$g^{*i} * g^{*j} = g^{*i+j}. \tag{2}$$

  On notera souvent simplement g^n pour simplifier la notation.
- L'application $\theta \mapsto \exp(i\theta)$ est un morphisme de groupes de $(\mathbb{R}, +) \to (\mathbb{C}^*, \times)$

Exercice 2.18. Démontrer les assertions données en exemple.

Exemple 2.19. Soit $\mathscr{B} = \{e_1, \ldots, e_n\}$ une base d'un $\mathbb{R}$-espace vectoriel E de dimension n. Rappelons que $(GL(E), \circ)$ est le groupe des automorphismes linéaires de E.

L'application $\varphi_{\mathscr{B}} : GL(E) \mapsto GL_n(\mathbb{R})$ qui à une application linéaire associe sa matrice dans la base $\mathscr{B}$ est un isomorphisme de groupes.

Exercice 2.20. Démontrer ce qui est affirmé dans cet exemple.

Définition 2.21. Le noyau d'un morphisme de groupes $f : (G, *) \to (H, \cdot)$ est $\ker(f) := \{g \in G,\ f(g) = e_H\}$. Son image est l'image de l'application f, notée $\mathrm{Im}(f)$.

Le lemme suivant simplifie la vérification qu'un morphisme de groupes est injectif. Et est complétement analogue au cas des applications linéaires.

Lemme 2.22. *Un morphisme de groupes $f : (G, *) \to (H, \cdot)$ est injectif si et seulement si* $\ker(f) = \{e_G\}$.

Démonstration. L'injectivité implique que le noyau est réduit à e_G puisque on sait déjà que l'image de e_G est e_H et que par injectivité c'est donc le seule élément possible.

Réciproquement, supposons que $f(x) = f(y)$. Alors par simplification dans H, on obtient $f(x) \cdot f(y)^{-1} = e_H$ et comme f est un morphisme de groupes cela est équivalent à

$$e_H = f(x) \cdot f(y^{-1}) = f(x * y^{-1}).$$

D'où $x * y^{-1} \in \ker(f)$ et donc $x * y^{-1} = e_G$ par hypothèse. Par simplification encore, on obtient $x = y$ ce qui prouve l'injectivité. □

Exemple 2.23. Le noyau du morphisme de groupes $\theta \mapsto \exp(i\theta)$ de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$ est le sous-groupe $2\pi\mathbb{Z}$ de $\mathbb{R}$. Son image est l'ensemble $S^1 = \{z, \in \mathbb{C},\ |z| = 1\}$ des nombres complexes de module 1 ; c'est à dire le cercle unité.

Remarque 2.24 (**Que veut dire que deux groupes sont les-mêmes ?**). La notion d'égalité en mathématique est en général utilisée pour des éléments ou des sous-ensembles d'un ensemble. Dans cette optique, que deux groupes sont égaux voudraient dire qu'ils ont exactement le même ensemble sous-jacent et la même loi de composition interne.

Cette notion d'égalité n'est pas une notion très raisonnable pour des structures mathématiques abstraites (comme les groupes, espaces vectoriels etc...). En effet si je prends deux singletons $\{a\}$ et $\{b\}$ dans un même ensemble (ou même des ensembles différents), ils ne sont pas égaux bien qu'ils aient tous les deux une structure de groupe trivial et complètement analogues. Ils sont en revanche effectivement isomorphes : via la bijection $a \mapsto b$ dont on laisse exercice de vérifier que c'est bien un isomorphisme de groupes.

De même, $\mathbb{R}$ et $M_1(\mathbb{R})$ sont deux espaces vectoriels réels qui ne sont pas égaux, bien qu'ils se ressemblent beaucoup. En fait ils sont canoniquement isomorphes en tant que $\mathbb{R}$-espace vectoriels. Et de manière générale tout $\mathbb{R}$-espace vectoriel de dimension n est isomorphe à $\mathbb{R}^n$ mais ne lui est essentiellement jamais égal. Et cette question d'égalité est peu pertinente.

En fait la bonne notion d'égalité que l'on considère pour des structures de groupes abstraites est celle d'isomorphisme de groupes. On considérera que deux groupes sont "la même structure" si ils sont *isomorphes* en tant que groupes. Donc une phrase du genre déterminer tous les groupes G vérifiant *Blaah* signifiera déterminer, à isomorphisme près, tous les groupes vérifiant la propriété *Blaah*.

Notons que si les groupes formaient un ensemble [7], alors on pourrait voir la notion d'être isomorphe comme une relation d'équivalence que l'on substitue à celle d'égalité.

Remarque 2.25 (Retour sur le fait qu'un *groupe est une structure*). Tout ensemble peut être muni d'une structure de groupes (et en général de plusieurs non-isomorphes). Par exemple, si X est un ensemble de cardinal n. Alors il existe une bijection $\varphi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} X$ puisqu'ils ont même cardinaux. On note $\overline{+}$ la structure additive dans $\mathbb{Z}/n\mathbb{Z}$. Alors $* : (x, y) \mapsto f\big(f^{-1}(x)\overline{+}f^{-1}(y)\big)$ est une loi de composition interne sur X qui fait de $(X, *)$ un groupe commutatif [8].

L'application $f : (\mathbb{Z}/n\mathbb{Z}, \overline{+}) \to (X, \star)$ est un isomorphisme de groupes. Mais cette structure n'est pas canonique. On peut faire des raisonnement similaires pour un ensemble dénombrable ou en bijection avec $\mathbb{R}$ en utilisant $(\mathbb{Z}, +)$ ou $(\mathbb{R}, +)$ à la place de $\mathbb{Z}/n\mathbb{Z}$. En particulier on peut trouver une structure de groupe sur $GL_n(\mathbb{R})$ qui soit isomorphe à $(\mathbb{R}, +)$ mais qui est évidemment très différente de celle donnée par la multiplication de matrices.

De même si X est un ensemble à 6 éléments, par la même méthode on peut lui donner une structure de groupe isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou bien au groupe symétrique S_3 (voir 4) qui est non-commutatif et en particulier *pas* isomorphe à $\mathbb{Z}/6\mathbb{Z}$. En d'autres termes, on voit qu'un ensemble n'a en général aucune structure de groupe naturelle.

Passons maintenant à la notion de sous-groupes.

Définition 2.26. Soit $(G, *)$ un groupe. Un sous-ensemble $H \subset G$ de G est un *sous-groupe* si il vérifie les trois conditions suivantes :

(1) H contient l'élément neutre : $e_G \in H$;
(2) H est stable par multiplication : pour tout $h_1, h_2 \in H$, on a $h_1 * h_2 \in H$;
(3) H est stable par inverse : pour tout $h \in H$, $h^{-1} \in H$.

Exercice 2.27. Démontrer que l'on peut remplacer la condition (1) par H est non-vide.

Démontrer que l'on peut remplacer (2) et (3) (sachant (1)) par, pour tout $h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$.

Le premier lemme trivial est

Lemme 2.28. *Si H est un sous-groupe de $(G, *)$ alors $(H, *)$ est un groupe et l'inclusion $H \hookrightarrow G$, $h \mapsto h$ est un morphisme de groupes injectif.*

Le lemme justifie que l'on a pas parlé de la loi de H dans la définition de sous-groupe, car elle est canonique : c'est celle donnée par G (qui elle a été fixé au début).

Exercice 2.29. Démontrer le lemme.

Voici quelques exemples élémentaires à toujours garder en tête :

7. et nous ne rentrerons pas dans les subtilités de théorie des catégories ou de logique rendant le reste de la phrase mathématiquement bien définie

8. Démontrer le ; c'est assez similaire à la preuve du lemme 2.16

Exemple 2.30.
- Il y a deux sous-groupes triviaux dans un groupe G : le singleton $\{e_G\}$ et G lui même sont des sous-groupes de G. Notons que $\{e_G\}$ est l'unique singleton de G qui soit un sous-groupe.
- $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$ mais aussi de $\mathbb{R}$ et $\mathbb{C}$.
- Le cercle unité $S^1 := \{z \in \mathbb{C}, |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$. En effet 1 est bien dans S^1 et comme $|z \times z| = |z| \times |z'|$ on vérifie facilement que S^1 est stable par produit et par inverse.
- De même $]0, +\infty[$ est un sous-groupe de $(\mathbb{R}^*, \times)$. En revanche $]-\infty, 0[$ n'est évidemment pas un sous-groupe de $\mathbb{R}^*$.
- $\{-1, 1\}$ est un sous-groupe de $\mathbb{R}^*$.
- Soit $E = \{a, b, c\}$ un ensemble à 3 éléments. Le sous-ensemble des bijections $\mathrm{Bij}(E)$ qui vérifient $f(a) = a$ est un sous-groupe de $\mathrm{Bij}(E)$. Ce n'est pas le cas pour le sous-ensemble des bijections qui vérifient $f(a) = b$.
- Si H est un sous-groupe de G et K un sous-groupe de H, alors K est un sous-groupe de G (la démonstration est laissée en exercice).

On peut construire des sous-groupes nouveaux à partir d'autres sous-groupes comme nous le dit le lemme suivant.

Lemme 2.31. *Soit $(H_i)_{i\in I}$ une famille quelconque de sous-groupes de G. Alors l'intersection $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. Cette preuve a été vue en TD. □

Le lemme suivant donne beaucoup d'exemples.

Lemme 2.32. *Si $f : G \to H$ est un morphisme de groupes, alors* $\ker(f)$ *est un sous-groupe de G et* $\mathrm{Im}(f)$ *un sous-groupe de H.*

Démonstration. Par le lemme 2.14 on sait déjà que $e_G \in \ker(f)$. Si $g_1, g_2 \in \ker(f)$, montrer que $g_1 * g_2 \in \ker(f)$ revient à motnrer que $f(g_1 * g_2) = e_H$. Or

$$f(g_1 * g_2) = f(g_1) \cdot f(g_2) = e_H \cdot e_H = e_H$$

car f est un morphisme de groupes et que $g_1, g_2 \in \ker(f)$. On montre de même que $\ker(f)$ est stable par passage à l'inverse en utilsiant que $f(g^{-1}) = f(g)^{-1}$ et $e_H^{-1} = e_H$.

De même, $f(e_G) = e_H$ implique que $e_H \in \mathrm{Im}(f)$. Et si $x, y \in \mathrm{Im}(f)$ on montre que $x \cdot y \in \mathrm{Im}(f)$ en écrivant simplement, que, par définition, $x = f(g)$, $y = f(g')$ puisque ils sont dans l'image (g, g' ne sont pas forcément uniques). Ainsi

$$x \cdot y = f(g) \cdot f(g') = f(g * g') \in \mathrm{Im}(f).$$

On a bien montré la stabilité par produit et celle par inverse est encore similaire. □

Exemple 2.33. Le sous-ensemble $SL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}),\ \det(M) = 1$ est un sous-groupe de $GL_n(\mathbb{R})$ car l'application déterminant est un morphisme de groupes.

Lemme 2.34. *Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $d\mathbb{Z}$ où d est un entier quelconque.*

Démonstration. La preuve a été vue en DM (et cours d'arithmétique). □

Exemple 2.35. Soit $g \in G$, alors l'image par le morphisme $n \mapsto g^{*n}$ de $\mathbb{Z}$ est un sous-groupe de G, dont on verra plus loin que c'est le sous-groupe engendré par g.

Remarque 2.36. On a vu que la notion d'égalité de groupes n'avait pas grand sens. En revanche la notion d'égalités de sous-groupes d'un groupe G fixé a un sens très clair et est pertinente dans de nombreuses situations. Elle ne l'est pas spécialement si on s'intéresse aux sous-groupes en tant que groupes abstraits (c'est à dire sans se soucier de où ils vivent) mais elle le devient si on voit les sous-groupes comme vivant dans G.

3. Actions de groupes

Les actions de groupes sont au cœur de l'interaction entre groupes et géométrie ou combinatoire. C'est via leur intermédiaire que les groupes ont été découverts-et utilisés-longtemps avant que la notion ne soit formalisée. D'un point de vue heuristique : un groupe a pour vocation d'agir sur des ensembles, incarnant ainsi des symétries.

3.1. **Définitions et exemples.**

Définition 3.1. Soit $(G, *)$ un groupe et X un ensemble. Une action à gauche de G sur X est la donnée d'une application $\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$ satisfaisant les deux propriétés suivantes :

(1) $\forall g_1, g_2 \in G$ et $\forall x \in X$, on a $g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x$;
(2) $\forall x \in X$, on a $e \cdot x = x$.

Symétriquement, une action à droite de G sur X est la donnée d'une application $\begin{array}{ccc} X \times G & \to & X \\ (x, g) & \mapsto & x \cdot g \end{array}$ satisfaisant les deux propriétés suivantes :

(1) $\forall g_1, g_2 \in G$ et $\forall x \in X$, on a $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 * g_2)$;
(2) $\forall x \in X$, on a $x \cdot e = x$.

On dira souvent simplement que G agit sur X (à gauche ou à droite) pour dire que l'on se donne une action (à gauche ou à droite) de G sur X.

La condition (1) est une condition d'associativité et compatibilité de l'action avec la structure du groupe. La condition (2) signifie que le neutre agit trivialement.

Notation 3.2. On notera souvent ${}^g x$ pour $g \cdot x$ et x^g pour une action à droite. C'est à dire comme des opérations puissances. Il y a beaucoup de notations différentes standards pour les actions dans la littérature. Il faut donc savoir être souple. Notamment,il faut faire attention, dans les propriétés ci-dessus de ne pas confondre $*$ (la multiplication du groupe) avec $\cdot$, l'action sur X. Les notations pour l'action et la multiplication variants tout le temps, certains préfèrent les notations puissances qui sont moins ambigües. Cela dit, il faut s'habituer à toutes les notations fréquentes.

Remarque 3.3 (Pourquoi des actions à gauche et à droite ?). Les actions à gauche et à droite se ressemblent, mais ne sont pas équivalentes si le groupe n'est pas abélien en raison de l'ordre des opérations. Nous verrons en TD des exemples qui font apparaître des actions dans un sens mais pas dans l'autre.

Notons cependant deux points :

- Si un groupe est abélien, une action à droite et une action à gauche sont la même chose. Donc on ne s'en préoccupera pas dans ce cas.
- Si un groupe G agit à gauche sur X, alors on a automatiquement une action à droite sur X donnée par la formule $x^g = {}^{g^{-1}} x$. En effet on a que $e^{-1} = e$ ce qui assure que $x^e = x$ et $(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$ permet de vérifier que
$$x^{g_1 * g_2} = {}^{(g_1 * g_2)^{-1}} x = {}^{g_2^{-1} * g_1^{-1}} x = {}^{g_2^{-1}}({}^{g_1^{-1}}(x)) = {}^{g_2^{-1}}(x^{g_1}) = (x^{g_1})^{g_2}.$$

Remarque 3.4. Notons que si la condition (2) est vraie, alors la condition (1) est automatiquement vérifiée dans le cas $g_1 = e$ ou $g_2 = e$. (mais pas pour g_1, g_2 quelconques bien sûr !). En effet, dans ce cas là, si par exemple $g_1 = e$, alors $g_1 * g_2 = e = g_2 = g_2$ ce qui donne $(g_1 * g_2) \cdot x = g_2 \cdot x$. D'autre part $g_1 \cdot (g_2 \cdot x) = e \cdot (g_2 \cdot x) = g_2 \cdot x$ par la condition (2) ce qui prouve le résultat. L'autre cas de figure est similaire.

Remarque 3.5. Une action à gauche associe donc à tout élément g de G une transformation de X, c'est à dire une application $\rho_g : X \to X$ définie par $\rho_g(x) = g \cdot x$. L'axiome (2) se traduit par $\rho_e = \mathrm{id}_X$. On a évidemment la même chose pour une action à droite. La propriété (1) nous dit que,

Lemme 3.6. *Pour tout $g, h \in G$, on a*

$$\rho_g \circ \rho_h = \begin{cases} \rho_{g*h} & \text{si l'action est à gauche} \\ \rho_{h*g} & \text{si l'action est à droite.} \end{cases} \tag{3}$$

Démonstration. Pour une action à gauche, on a pour tout $x \in X$, que

$$\rho_g \circ \rho_h(x) = \rho_g(\rho_h(x)) = \rho_g(h \cdot x) = g \cdot (h \cdot x) = (g * h) \cdot x = \rho_{g*h}(x)$$

où on a utilisé la définition de ρ pour les premières égalités, puis la condition (1) et enfin la définition de ρ_{g*h}.

De même pour une action à droite, on a

$$\rho_g \circ \rho_h(x) = \rho_g(\rho_h(x)) = \rho_g(x \cdot h) = (x \cdot h) \cdot g = x \cdot (h * g) = \rho_{h*g}(x).$$

□

La propriété suivante est très importante :

Proposition 3.7. *Soit G un groupe agissant sur un ensemble X. Pour tout $g \in G$, l'application* $\begin{array}{ccc} X & \xrightarrow{\rho_g} & X \\ x & \longmapsto & g \cdot x \end{array}$ *est une bijection.*

Démonstration. L'idée de cette preuve revient très fréquemment en théorie des groupes et géométrie. Cette idée est d'utiliser l'inverse de g pour exhiber une application réciproque à ρ_g. Le candidat naturel est $\rho_{g^{-1}}$. Vérifions qu'il marche. On a, pour tout $x \in X$, en utilisant (3), que

$$\rho_{g^{-1}} \circ \rho_g(x) = \rho_{g^{-1}*g}(x) = \rho_e(x)e \cdot x = x$$

où la dernière égalité provient de la condition (2) d'une action : à savoir que le neutre agit trivialement. Conclusion $\rho_{g^{-1}} \circ \rho_g = \mathrm{id}_X$. On démontre de même que $\rho_g \circ \rho_{g^{-1}} = \mathrm{id}_X$ et donc ρ_g est bijective, d'application réciproque $\rho_{g^{-1}}$. □

Remarque 3.8. La proposition et le lemme précédent sont équivalent à dire que l'application $\rho : g \mapsto \rho_g$ est un morphisme de groupe de G vers $(\mathrm{Bij}(X), \circ)$. Réciproquement, on peut montrer qu'un tel morphisme de groupes définit une action de G sur X par la formule $g \cdot x = \rho_g(x)$.

Exemple 3.9. La conjugaison des nombres complexes définit une action du groupe $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{C}$ via la formule $\overline{0} \cdot z = z$ et $\overline{1} \cdot z = \overline{z}$.

En effet, la condition (2) est satisfaite puisque $\overline{0}$ est le neutre de $\mathbb{Z}/2\mathbb{Z}$. Il reste à voir la condition (1). Par la remarque 3.4, il suffit de vérifier que $\overline{1} \cdot (\overline{1} \cdot z) = (\overline{1+1}) \cdot z$ pour tout complexe z. Or $\overline{1+1} = \overline{0}$ dans $\mathbb{Z}/2\mathbb{Z}$. Donc $(\overline{1+1}) \cdot z = z$. D'un autre côté $\overline{1} \cdot (\overline{1} \cdot z) = \overline{1}(\overline{z}) = \overline{\overline{z}} = z$ ce qui conclut.

Exactement la même preuve permet de montrer que la transposition dans $M_n(\mathbb{R})$ induit une action de $\mathbb{Z}/2\mathbb{Z}$ sur $M_n(\mathbb{R})$.

Plus généralement, on a en fait montré

Lemme 3.10. *Une action de $\mathbb{Z}/2\mathbb{Z}$ sur un ensemble X est équivalente à la donnée d'une involution $\tau : X \to X$. C'est à dire une application vérifiant $\tau \circ \tau = id_X$.*

La ***règle 2.9 de simplification*** dans un groupe se transmet aux actions. Et il faut la maîtriser au même titre que dans les groupes car elle est très utile et a de nombreuses conséquences.

Lemme 3.11 (Règle de simplification)**.** *Soit G un groupe agissant sur X à gauche. Alors pour tout $g \in G$, $x, y \in X$, on a*

$$g \cdot x = y \iff x = g^{-1} \cdot y.$$

On a le même résultat pour les actions à droite.

Démonstration. On part de $g \cdot x = y$. En faisant agir g^{-1} sur chaque membre de l'égalité, on obtient : $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$. Mais on a aussi par propriétés (1) et (2) d'une action que $g^{-1} \cdot (g \cdot x) = (g^{-1} * g) \cdot x = e \cdot x = x$. On a donc bien prouvé que $g^{-1} \cdot y = x$.

L'implication réciproque se fait de manière similaire. De même que le cas des actions à droite. □

Une fois que l'on a une action, on peut définir certains sous-ensembles importants de X et de G.

Définition 3.12. Soit G un groupe agissant sur X (à gauche).

- Pour tout $x \in X$, on appelle *stabilisateur* de x, le sous-ensemble $\mathrm{stab}_x = \{g \in G,\ g \cdot x = x\ \}$ des éléments de G qui laisent x stable.
- Pour tout $x \in X$, on appelle *orbite* de x ou classe de x le sous-ensemble $C_x = \{g \cdot x,\ g \in G\}$, c'est à dire tous les points que l'on obtient à partir de x en faisant agir les éléments de G.
- Pour tout g, le sous-ensemble $\mathrm{Fix}(g) = \{x \in X,\ g \cdot x = x)$ des points de X sur lesquels g agit trivialement.

On notera souvent G_x pour stab_x et X^g pour $\mathrm{Fix}(g)$.

Remarque 3.13. Plus généralement, pour un sous-ensemble H, on appellera *points fixes* de H les éléments de $\mathrm{Fix}(H) = \{x \in X,\ \forall h \in H, {}^h x = x\}$ que l'on notera souvent X^H pour simplifier la notation.

De même pour un sous-ensemble Y de X, on appellera stabilisateur de Y, le sous-ensemble $\mathrm{stab}_Y = \{g \in G,\ \forall y \in Y,\ g \cdot y = y\} = \bigcup_{y \in Y} \mathrm{Fix}_y$. Il sera parfois noté G_Y.

Lemme 3.14. *Quel que soit $x \in X$, on a que stab_x est un sous-groupe de G.*

Démonstration. On a que $e \in \mathrm{stab}_x$ car $e \cdot x = x$ par définition d'une action. Si $g, h \in \mathrm{stab}_x$, alors

$$(g * h) \cdot x = g \cdot (h \cdot x) = g \cdot x \ (\text{car } h \in \mathrm{stab}_x) \ = x \ (\text{car } g \in \mathrm{stab}_x).$$

Ceci nous donne bien que $g * h \in \mathrm{stab}_x$. Si $g \in \mathrm{stab}_x$, nous devons prouver que $g^{-1} \cdot x = x$.

Nous allons encore utiliser que l'on peut simplifier dans un groupe. Plus précisément, le lemme 3.11 nous dit que $g \cdot x = x$ est équivalent à $x = g^{-1} \cdot x$ ce qui prouve que $g^{-1} \in \mathrm{stab}_x$. □

Voici quelques exemples standards à connaître d'actions de groupes.

Exemple 3.15.

- Commençons par *l'action triviale* : pour tout groupe G et tout ensemble X, l'application $G \times X \ni (g, x) \mapsto x$ est une action à gauche. Dîte action triviale à gauche. De même l'application $X \times G \ni (x, g) \mapsto x$ est une action à droite appelée action triviale à droite. Le mot trivial vient du fait que tout élément g agit comme le neutre e_G et que donc l'action ne transforme aucun point de X en un autre point. Ce qui fait que cette action est rarement très intéressante à considérer (à part pour la comparer à une autre action).
- Le groupe $GL_n(\mathbb{R})$ agit sur $\mathbb{R}^n$ via $(M, X) \mapsto MX$. C'est à dire par multiplication d'une matrice avec un vecteur colonne.

  On a $C_0 = \{0\}$ et si $X \neq 0$, $C_X = \mathbb{R}^n \setminus \{0\}$ car on peut toujours trouver une matrice inversible qui envoie un vecteur non-nul sur tout autre vecteur non-nul (par théorème de choix de complémentaires des vecteurs non-nuls). Par ailleurs, si $X \neq 0$, alors stab_X est le sous-ensemble des matrices inversibles dont X est vecteur propre associé à la valeur propre 1. Évidemment, $\mathrm{stab}_0 = GL_n(\mathbb{R})$.
- Le groupe $GL_n(\mathbb{R})$ agit aussi sur l'ensemble B des bases de $\mathbb{R}^n$ par

$$(M, \{E_1, \ldots, E_n\}) \mapsto \{ME_1, \ldots, ME_n\}.$$

On a que pour toute base $\{E_1, \dots, E_n\}$, $\text{stab}_{\{E_1,\dots,E_n\}} = \{I_n\}$. En revanche $C_{\{E_1,\dots,E_n\}} = B$. En effet, on peut toujours passer d'une base à une autre via une matrice inversible.

- Un groupe $(G, *)$ agit à gauche sur lui-même par *conjugaison*[9] : via l'application $G \times G \to G$ définie par $(g, x) \mapsto g * x * g^{-1}$.

  Quel est stab_x pour cette action ? Par définition, il s'agit de tous les éléments $g \in G$ tels que $gxg^{-1} = x$ ce qui est équivalent (par règle de simplification) à $gx = xg$. Autrement dit, il s'agit précisément des éléments g dans G qui commutent avec x. En particulier, si x est dans le centre de G (voir définition 3.71), alors $\text{stab}_x = G$ et $\text{stab}_G = Z(G)$ est le centre de G.

Exercice 3.16. Démontrer les affirmations données dans cet exemple.

Nous allons maintenant donner un exemple **fondamental** d'action. Il s'agit de *l'action canonique* d'un sous-groupe sur un groupe.

Soit donc G un groupe et H un sous-groupe de G. Précisons que nous noterons la multiplication de x et y dans G simplement xy dans la suite de cette partie.

Définition 3.17 (Actions canoniques d'un sous-groupe sur un groupe)**.** L'action par multiplication à droite par H est l'application $\begin{array}{ccc} G \times H & \longrightarrow & G \\ (g, h) & \longmapsto & gh. \end{array}$

L'action par multiplication à gauche par H est l'application $\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg. \end{array}$

Lemme 3.18. *La multiplication à droite (resp. à gauche) est une action à droite (resp. à gauche) de H sur G.*

Remarque 3.19. Dans cette action, on voit donc G comme un ensemble et c'est pour H que l'on utilise la structure du groupe.

Démonstration. Il suffit de vérifier les axiomes. Les deux cas sont similaires, faisons le pour l'action à droite. *La propriété (1) de l'action se traduit simplement par l'associativité de la multiplication* dans cet exemple comme nous allons le voir. Notons g^h la multiplication à droite de g par h (donné par la définition 3.17), en oubliant pour le moment la formule histoire de se rappeler précisément de ce que l'on doit montrer. On doit montrer pour tout $g \in G$, $h_1, h_2 \in H$ que

$$g^{h_1 h_2} = (g^{h_1})^{h_2}.$$

En appliquant maintenant la formule donnée pour g^h, on a

$$g^{h_1 h_2} = g(h_1 h_2) = (gh_1)h_2 = (g^{h_1})^{h_2}$$

où la deuxième égalité est donnée par l'associativité de la loi de groupe de G (et les autres égalités sont simplement la définition de l'action).

Pour le deuxième point on a que $g^e = ge = g$ par définition du neutre. □

Remarquons que pour cette action, nous avons que quel que soit $x \in G$, on a $\text{stab}_x = \{e\}$. En effet, par définition de l'action, $x^h = x \Leftrightarrow xh = x$ ce qui est équivalent à $h = e$ par simplification par x (ce qu'on peut faire puisque G est un groupe).

Cette action est très très importante ; nous allons le voir en étudiant la relation d'équivalence qui lui est associée dans la prochaine partie.

9. notion que l'on va voir réapparaître souvent

3.2. **Relation d'équivalence associée à une action de groupe et cas de l'action d'un sous-groupe.** Un point **fondamental** d'une action de groupe est qu'elle définit *une relation d'équivalence* sur l'ensemble sur lequel elle agit.

Définition 3.20. Soit G un groupe agissant à gauche sur un ensemble X. On définit la relation ${}_{G,X}\mathscr{R}$ sur X par $x\,{}_{G,X}\mathscr{R}y$ si il existe $g \in G$ tel que $y = g \cdot x$.

De même si G agit à droite sur X, $\mathscr{R}_{G,X}$ sur X par $x\mathscr{R}_{G,X}\,y$ si il existe $g \in G$ tel que $y = x \cdot g$.

Notation 3.21. *On notera en général* $X_G := X/_{G,X}\mathscr{R}$ *le quotient de* X *par la relation d'équivalence* (qu'elle soit à droite ou à gauche)

Notation 3.22. Pour l'action par multiplication à droite d'un sous-groupe H sur G, on notera simplement $\mathscr{R}_H$ cette relation $\mathscr{R}_{H,G}$.

Proposition 3.23. *On a que les relations* ${}_{G,X}\mathscr{R}$ *(dans le cas d'une action à gauche) et* $\mathscr{R}_{G,X}$ *(dans le cas d'une action à droite) sont des relations d'équivalence sur* X*.*

Démonstration. Nous la faisons dans le cas à droite. La preuve est formellement la même dans les deux cas. Tout d'abord, comme $x \cdot e = x$ on a que $x\mathscr{R}_{H,G}x$ et donc la relation est réflexive.

La symétrie va être une conséquence de la règle de simplification du lemme 3.11 : Si $x\mathscr{R}_{H,G}y$, alors il existe $g \in G$ tel que $y = x \cdot g$ ce qui est équivalent par division par g à $y \cdot g^{-1} = x$. Or $g^{-1} \in G$, donc $y\mathscr{R}_{H,G}x$.

La transitivité est une conséquence de la propriété (1) d'une action. Supposons que $x\mathscr{R}_{H,G}y$ et $y\mathscr{R}_{H,G}z$; alors on a $g_1, g_2 \in G$ tels que $y = x \cdot g_1$ et $z = y \cdot g_2$. D'où

$$z = (x \cdot g_1) \cdot g_2 = x \cdot (g_1 * g_2)$$

et donc comme $g_1 * g_2 \in G$, on a $x\mathscr{R}_{H,G}z$. □

Remarque 3.24 (**Rappels sur les classes d'équivalence.**). On renvoie aux cours d'algèbre 1 et d'arithmétique pour les détails sur les relations d'équivalence, classes d'équivalences et quotients.

Rappelons que à tout élément x de X, on associe sa classe d'équivalence

$$\overline{x} := \{y \in X \text{ tel que } y\mathscr{R}x\}.$$

Notation 3.25. On trouvera souvent les notation $[x]$ ou C_x à la place de $\overline{x}$ dans la littérature. Ce sont les notations standards qu'il vaut mieux connaître. On les utilisera donc pour vous y habituer.

Un point clé des classes d'équivalence est la proposition suivante.

Proposition 3.26. *Pour tout* $x, y \in X$*, on a soit* $\overline{x} = \overline{y}$ *soit* $\overline{x} \cap \overline{y} = \emptyset$*.*

Autrement dit deux classes d'équivalences sont égales ou sont disjointes. En particulier, elles forment une **partition**[10] **de** X. La proposition suivante précise un peu plus la précédente.

Proposition 3.27. *Soit* $\mathscr{R}$ *une relation d'équivalence sur un ensemble* X*. Alors, quels que soient* $x, y \in X$*, on a que les propriétés suivantes sont équivalentes*

- $x\mathscr{R}y$
- $\overline{x} = \overline{y}$
- $y \in \overline{x}$

10. autrement dit une décomposition de X en sous-ensembles 2 à 2 disjoints, et qui recouvrent X

Terminologie 3.28. **L'ensemble quotient de X par $\mathscr{R}$** est par définition l'ensemble des classes d'équivalence (qui est un sous-ensemble de $P(X)$ les parties de X) On le note $X_{/\mathscr{R}}$.

On dispose d'une application (dite canonique) $X \to X_{/\mathscr{R}}$ définie par $x \mapsto \overline{x}$ qui est surjective mais en général pas injective.

Étudions, maintenant ces rappels effectués, le cas spécifique de l'action d'un sous-groupe H sur G. On regardera celle par multiplication à droite, mais il y a bien-sûr des résultats complètement analogues pour l'action à gauche.

Notation 3.29. On notera G/H l'ensemble quotient $G/\mathscr{R}_H$ donné par la relation d'équivalence associée à la multiplication à droite par G. Cette notation est standard dans tous les textes mathématiques.

Comme l'ensemble sur lequel on agit a une structure de groupe, on peut réécrire la relation d'équivalence comme suit.

Lemme 3.30. *On a que $x\mathscr{R}_H y$ si et seulement si $x^{-1}y \in H$ ce qui est aussi équivalent à $y^{-1}x \in H$.*

Démonstration. La définition de $x\mathscr{R}_H y$ est que il existe $h \in H$ tel que $y = xh$ ce qui est équivalent par simplification par x à la condition $x^{-1}y \in H$. Cela donne la première équivalence. Comme H est un sous-groupe, on a que $x^{-1}y \in H$ si et seulement si $(x^{-1}y)^{-1} \in H$. Or $(x^{-1}y)^{-1} = y^{-1}x$ ce qui conclut. □

Décrivons maintenant les classes pour cette action par multiplication à droite.

Lemme 3.31. *Soit H un sous-groupe de G que l'on fait agir par multiplication à droite. Alors pour tout $g \in G$, sa classe d'équivalence est*

$$C_g = gH.$$

Rappelons que gH est le sous-ensemble $gH = \{gh,\, h \in H\}$ (et que C_g se note aussi $[g]$ ou $\overline{g}$).

Terminologie 3.32. Le sous-ensemble gH est appelé ***coensemble***[11] *à gauche* associé à g. On appelle coensemble (à gauche) tout ensemble de la forme gH. On trouve également la terminologie classe à gauche de g pour gH.

De même un coensemble à droite est un sous-ensemble de g qui s'écrit Hg. Il s'agit bien entendu exactement de la classe d'équivalence de g pour l'action à gauche de H.

Remarque 3.33 (Coensemble à gauche alors que l'action est à droite ?). Et bien oui. En fait quand on écrit coensemble ou classe à gauche de g, cela fait référence au fait que g est à gauche. Et c'est d'ailleurs pour cela que le groupe H agit à droite. Ce sont des terminologies standards qui viennent aussi de l'exemple 3.39 qui établit que G agit à gauche (par multiplication) sur le quotient G/H.

La proposition 3.27 a pour corollaire immédiat :

Corollaire 3.34. *On a les équivalences $gH = g'H \Leftrightarrow \overline{g} = \overline{g'} \Leftrightarrow (g')^{-1}g \in H \Leftrightarrow g' \in gH$.*

Exercice 3.35. Démontrer le corollaire.

L'ensemble quotient G/H est donc par définition l'ensemble[12] $\{gH, g \in G\}$ des coensembles à droite de G et le corollaire dit que $gH = g'H$ si et seulement si $(g')^{-1}g \in H$.

Notons que H lui même est un coensemble. C'est la classe de e et plus généralement, $\overline{h} = H$ pour tout $h \in H$. En revanche si $g \notin H$, alors $gH \cap H = \emptyset$ d'après la proposition 3.26.

Enfin, comme les classes forment une partition de G on a le corollaire suivant de la proposition 3.26.

11. coset en anglais, terminologie que beaucoup de francophones utilisent sans états d'âmes
12. que l'on peut voir comme un sous-ensemble de $P(G)$ les parties de G

Corollaire 3.36. *Soit H un sous-groupe de G, alors on a une partition $G = \coprod_{\overline{g} \in G/H} gH$*

Notation 3.37. La notation $E = \coprod_{i \in I} U_i$ signifiera dans ce cours que l'ensemble E est la réunion des ensembles U_i et que pour $i \neq j$ on a $U_i \cap U_j = \emptyset$. Autrement dit, cela veut exactement dire que les U_i forment une partition de E

Exemple 3.38. Vous avez déjà rencontré un exemple très important de cette construction. Il s'agit de $\mathbb{Z}/n\mathbb{Z}$ qui est bien le quotient du groupe $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

Notons que $\mathbb{Z}/n\mathbb{Z}$ est plus qu'un ensemble. Il hérite d'une structure de groupes provenant de $\mathbb{Z}$. Ceci n'est *pas* vrai pour le quotient G/H d'un groupe quelconque par un sous-groupe. On verra que le groupe H doit être normal pour que cela soit vrai (condition toujours satisfaite lorsque G est abélien).

Exemple 3.39 (On peut multiplier des deux côtés en même temps !). Le groupe G (et donc tout sous-groupe K) agit par multiplication à gauche sur lui même (c'est un cas particulier de l'action générale à gauche d'un sous-groupe). Notons que pour l'action à droite d'un sous-groupe H, on a la relation de compatibilité suivante entre les actions : $\forall k \in K$, $x \in G$, $h \in H$, on a

$$^k(x^h) = kxh = (^k x)^h.$$

Autrement dit agir d'abord à gauche(par k) puis à droite (par h) et la même chose que d'abord agir à droite (par h) puis à gauche (par k). On a en fait que K agit à gauche sur les coensembles : $g \cdot xH = (gx)H$ et donc sur l'ensemble quotient G/H. On peut donc considérer un double quotient $K\backslash G/H$ des doubles coensembles. Nous ne nous en servirons cependant pas dans la suite.

3.3. **Théorème de Lagrange et cardinal des sous-groupes.** Nous allons énoncer et démontrer un premier théorème important permettant d'étudier et comprendre les groupes. La démonstration utilisera de manière cruciale l'action par multiplication d'un sous-groupe sur un groupe.

Commençons par une remarque. Si G est un groupe fini, alors tout sous-groupe H est aussi fini. On peut noter que son cardinal est le même que celui de tout coensemble gH.

Lemme 3.40. *Si G est fini, alors pour tout $x \in G$, on a* $\mathrm{card}(xH) = \mathrm{card}(H)$.

Remarque 3.41. La preuve du lemme ci-dessous suit une idée standard et très fructueuse en théorie des groupes. Il faut la comprendre et s'en souvenir. Elle est basée sur un principe fondamental de la théorie des groupes

La multiplication par un élément $x \in G$ est une bijection.

Démonstration du lemme 3.40. On applique le principe juste énoncé comme suit. Notons $\ell_x : \begin{array}{ccc} G & \to & G \\ g & \mapsto & xg \end{array}$. Alors cette application est bijective. En effet, suivant un principe de preuve déjà vu, elle a un inverse qui est précisément l'application $\ell_{x^{-1}}$: pour tout $g \in G$, on a

$$\ell_{x^{-1}}(\ell_x(g)) = \ell_{x^{-1}}(xg) = x^{-1}xg = eg = g.$$

Donc $\ell_{x^{-1}} \circ \ell_x = \mathrm{id}_G$. De même on montre que $\ell_x \circ \ell_{x^{-1}} = \mathrm{id}_G$.

Maintenant que l'on sait que cette application est injective, on en déduit que $\mathrm{card}(\ell_x(H) = \mathrm{card}(H)$ pour tout sous-ensemble H de G (en particulier pour tout sous-groupe). □

Remarque 3.42. La preuve montre même plus généralement, que quel que soit le cardinal de G et H, et $x \in G$, on a une bijection entre xH et H

Théorème 3.43 (de Lagrange)**.** *Soit G un groupe fini. Alors*

$$\mathrm{card}(G) = \mathrm{card}(H) \times \mathrm{card}(G/H).$$

Le théorème de Lagrange relie donc le cardinal du groupe, du sous-groupe et celui du quotient de manière précise. Il a de nombreuses conséquences, comme nous allons le voir tout au long du cours et du TD.

Terminologie 3.44. Le cardinal de G/H s'appelle *l'indice* de H dans G. Il se note souvent $[G : H]$. Par ailleurs on appelle parfois ordre de H le cardinal de H. C'est en référence à l'ordre d'un élément (voir la partie 3.4).

Démonstration du théorème de Lagrange. Cela va être un corollaire direct de notre étude de l'action par multiplication à droite de H et du lemme précédent. En effet, par le corollaire 3.36, on a une décomposition de G en réunion de coensembles à gauche : $G = \coprod_{\overline{x} \in G/H} xH$. La réunion étant disjointe, on a que

$$\begin{aligned} \operatorname{card}(G) = \sum_{\overline{x} \in G/H} \operatorname{card}(xH) &= \sum_{\overline{x} \in G/H} \operatorname{card}(H) \text{ (par le lemme 3.40)} \\ &= \operatorname{card}(G/H) \times \operatorname{card}(H) \end{aligned}$$

ce qui conclut. □

La première importante conséquence est la suivante.

Corollaire 3.45 (Lagrange)**.** *Soit G est un groupe fini. Pour tout sous-groupe H de G,* $\operatorname{card}(H)$ *divise* $\operatorname{card}(G)$*.*

Démonstration. Le théorème de Lagrange donne précisément ce résultat puisque le cardinal du quotient G/H est un nombre fini (car G est fini et que ce quotient est de cardinal plus petit que celui de G). □

Exemple 3.46. Soit p un nombre premier. Alors $\mathbb{Z}/p\mathbb{Z}$ n'a pas de sous-groupes non-triviaux, c'est à dire différent de lui-même et de $\{\overline{0}\}$. En effet d'après le corollaire de Lagrange, comme p est premier, tout sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ est de cardinal 1 ou p. Si c'est 1, puisqu'il contient $\{0\}$, c'est que c'est le groupe trivial $\{\overline{0}\}$. Si c'est p alors c'est un sous-groupe de même cardinal que $\mathbb{Z}/p\mathbb{Z}$. Il lui est donc égal.

Remarque 3.47. On prendra garde qu'il peut exister, selon le groupe, des diviseurs qui ne correspondent au cardinal d'aucun sous-groupe. Ce n'est pas tout à fait évident à voir. Mais, pour $n \geq 5$, par exemple le groupe A_n (voir pour les TDs ou le chapitre 4) n'a pas de sous-groupes de cardinal $\dfrac{n!}{4}$ qui est un diviseur de son cardinal $\dfrac{n!}{2}$ (ceci n'est pas évident, mais découle par exemple du fait que ces groupes n'ont pas de sous-groupes normaux non-triviaux).

3.4. **Ordre d'un groupe, groupe engendré par un élément et groupes cycliques.** On va s'intéresser au plus petit sous-groupe contenant un élément fixé g et à son cardinal. Ces notions sont les premier outils pour étudier et différencier des groupes ! Avant cela faisons une digression un peu générale sur la notion de sous-groupe engendré par des éléments.

Soit S une partie d'un groupe G. Alors il existe évidemment un sous-groupe qui contient S. Par exemple G lui-même. Ce qui est un peu moins évident, mais vrai, est qu'il existe ***un plus petit sous-groupe de*** G *contenant* S. C'est le contenu du lemme suivant.

Lemme 3.48. *Soit S une partie d'un groupe G, il existe un unique sous-groupe, noté $\langle S \rangle$, de G contenant S et tel que tout sous-groupe de G contenant S, contient aussi $\langle S \rangle$.*

On appelle souvent $\langle S \rangle$ *le sous-groupe engendré par* S.

Démonstration. La preuve la plus rapide est la suivante. On regarde la famille $\mathscr{F}$ de tous les sous-groupes contenant S. Alors, par le lemme 2.31, on a que l'intersection $\bigcap_{H_i \in \mathscr{F}} H_i$ est un sous-groupe de G, et contient S puisque chaque H_i contient S.

Par définition, il est inclus dans chaque H_i. Il vérifie donc les deux propriétés demandées. Par ailleurs si un autre sous-groupe K vérifie les mêmes propriétés, alors, on a que d'une part $K \subset \bigcap_{H_i \in \mathscr{F}} H_i$ puisque ce dernier contient S mais aussi $\bigcap_{H_i \in \mathscr{F}} H_i \subset K$ puisque K contient S. Ainsi ces deux groupes sont égaux ce qui prouve l'unicité. □

Remarque 3.49 (A quoi ressemble $\langle S \rangle$?). La démonstration donnée est rapide et efficace, mais elle ne décrit pas vraiment $\langle S \rangle$. Il est en fait assez facile de comprendre qui est $\langle S \rangle$. En effet, un sous-groupe contenant S, doit contenir tout élément $s \in S$, évidemment, mais aussi, puisque c'est un sous-groupe, tous les s^{-1} (avec $s \in S$), mais aussi tous les produits finis de ces éléments : c'est à dire tous les éléments de la forme

$$s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k} \text{ avec, pour tout } i,\ s_i \in S \text{ et } n_i \in \mathbb{Z}$$

On a repris ici la notation (1) pour $s_i^{n_i}$.

Autrement dit, un sous-groupe contenant S contient tous les mots finis écrits sur l'alphabet $S \cup S^{-1}$, en interprétant la concaténation des mots comme un produit dans G. Il suffit alors de montrer que l'ensemble de ces mots est un sous-groupe pour conclure que $\langle S \rangle$ existe et est donné par le sous-ensembe

$$\{s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k},\ k \in \mathbb{N}, s_i \in S, n_i \in \mathbb{Z}\} \subset G.$$

On va voir explicitement en détail le cas où S est un singleton ci-dessous (dans le point clé de la preuve de la proposition 3.53). Notons qu'évidemment il y a des répétitions dans l'écriture ci-dessus (par exemple $s^3 s^{-2} = s$, mais en général il y a des choses beaucoup plus subtiles aussi), répétitions que l'on appelle *relation* en language mathématique. Bien que cette écriture soit explicite, pour des S généraux, il n'est pas toujours facile de comprendre $\langle S \rangle$. On verra en TD un cas explicite (celui de Q_8) de sous-groupe engendré par 2 éléments.

Ce préliminaire effectué, passons à notre exemple phare.

Définition 3.50 (Ordre d'un élément)**.** Soit $g \in G$ un groupe. On note $\langle g \rangle$ le sous-groupe engendré [13] par l'élément g, c'est à dire le plus petit sous-groupe contenant g.

On appelle **ordre** de g le cardinal de $\langle g \rangle$. On le notera $\mathrm{ord}(g)$.

Notons que l'ordre peut donc être infini. La propriété suivante est fondamentale

Corollaire 3.51. *Soit $g \in G$.*

(1) L'ordre de g divise le cardinal de G.
(2) On a $\mathrm{ord}(g) = 1$ si et seulement si $g = e$.

Démonstration. Le premier point est une conséquence immédiate du Théorème de Lagrange. En effet, l'ordre de g est le cardinal de $\langle g \rangle$ qui est un sous-groupe de G.

Le deuxième point vient du fait que si $\mathrm{card}(\langle g \rangle) = 1$, alors ce sous-groupe ne contient qu'un seul élément et donc cet élément est e puisque c'est un sous-groupe. Comme il contient aussi g par définition, on a $g = e$. Réciproquement, si $g = e$, $\{e\}$ est un sous-groupe contenant g et comme tout sous-groupe contient e, c'est forcément le plus petit sous-groupe possible. □

Exemple 3.52. Regardons quelques exemples.

- Soit $n \neq 0 \in \mathbb{Z}$, alors $\mathrm{ord}(n) = \infty$. En effet, $n\mathbb{Z} = \langle n \rangle$ est de cardinal infini.

13. c'est à dire $\langle \{g\} \rangle$ dans les notations du lemme 3.48

- Soit $\overline{2}^4 \in \mathbb{Z}/4\mathbb{Z}$. Remarquons que $\overline{2}^4 + \overline{2}^4 = \overline{4}^4 = 0$ dans $\mathbb{Z}/4\mathbb{Z}$. Il suit que $\overline{2}^4$ est son propre inverse dans $\mathbb{Z}/4\mathbb{Z}$ et on a donc que $\{\overline{0}^4, \overline{2}^4\}$ est un sous-groupe de cardinal 2 de $\mathbb{Z}/4\mathbb{Z}$ qui contient $\overline{2}^4$. C'est forcément le plus petit puisque tout sous-groupe doit contenir ces deux éléments. Il suit que $\mathrm{ord}(\overline{2}^4) = 2$.
- Considérons maintenant $\overline{2}^5 \in \mathbb{Z}/5\mathbb{Z}$. Alors tout sous-groupe contenant $\overline{2}^5$ doit contenir aussi $\overline{2}^5 + \overline{2}^5 = \overline{4}^5 = -\overline{1}^5$. Il doit aussi contenir $\overline{2}^5 + \overline{2}^5 + \overline{2}^5 = \overline{6}^5 = \overline{1}^5$. Puis il doit aussi contenir $\overline{1}^5 + \overline{2}^5 = \overline{3}^5$, encore et toujours par stabilité d'un sous-groupe par addition. Enfin il doit contenir $\overline{3}^5 + \overline{2}^5 = \overline{0}^5$. Finalement, on vit qu'un tel sous-groupe contient tous les éléments de $\mathbb{Z}/5\mathbb{Z}$. Donc $\langle \overline{2}^5 \rangle = \mathbb{Z}/5\mathbb{Z}$ et il suit que $\mathrm{ord}(\overline{2}^5) = 5$.

L'ordre d'un groupe peut aussi être défini en utilisant le point (1) de la proposition suivante qui est une caractérisation équivalente. Rappelons la notation $g^{*n} = \underbrace{g * \cdots * g}_{n\text{-termes}}$ pour un entier $n \in \mathbb{N}$.

Proposition 3.53. *Soit $(G, *)$ un groupe et $g \in G$.*

(1) L'ordre de g est le plus petit entier $n > 0$ tel que $g^{*n} = e$ s'il existe et l'infini sinon.
(2) Si $\mathrm{ord}(g) = \infty$, pour tout $n \in \mathbb{Z} \setminus \{0\}$, on a $g^{*n} \neq e$.
(3) Si $n = \mathrm{ord}(g)$, le sous-groupe $\langle g \rangle$ est égal *au sous-groupe $\{e, g, g^{*2}, \cdots, g^{*(n-1)}\}$ de $(G, *)$.*

Remarque 3.54 (*Commentaire sur la proposition).* Avant de démontrer cette proposition, commentons l'assertion (3). Nous avons déjà vu que les deux premiers points sont une caractérisation équivalente de l'ordre (définition 3.50).

Le troisième point dit que le groupe $\langle g \rangle$ est égal au sous-ensemble $\{e, g, g^{*2}, \cdots, g^{*(n-1)}\}$ muni de la multiplication de G. Comme ce groupe est de cardinal n par hypothèse, cela veut dire que tous les termes g^{*i} pour $i \in \{0, 1, \ldots, n-1\}$ sont 2 à 2 distincts.

Enfin dire que la multiplication est celle de g signifie que $g * g = g^{*2}$ et que pour tout $0 \leq i, j \leq n-1$, on a $g^{*i} * g^{*j} = g^{*(i+j)}$ et que ce dernier terme correspond à un unique entier $r_{i+j} \in \{0, \ldots, n-1\}$. Ceci peut vous faire penser très fortement à ce qui se passe dans $\mathbb{Z}/n\mathbb{Z}$. Et pour cause nous allons préciser ce nombre r_{i+j} et la relation avec $\mathbb{Z}/n\mathbb{Z}$ dans le corollaire 3.55 ci-dessous.

Démonstration de la Proposition 3.53. Nous avons énoncé les points (1) et (2) séparément pour faire ressortir les énoncés. Mais on va les démontrer simultanément car ils sont étroitement reliés.

Première remarque clé : montrons d'abord que

$$\textit{le sous-ensemble } \{g^{*i},\ i \in \mathbb{Z}\} \textit{ est égal à } \langle g \rangle$$

(avec la notation (1)). À l'évidence si H est un sous-groupe contenant g, il contient (par stabilité par inverse) g^{-1} et toutes les puissances entières de g et g^{-1} (par stabilité par produit). Ainsi il contient tous les g^{*i} et donc $\{g^{*i},\ i \in \mathbb{Z}\}$. Pour conclure que ce sous-ensemble est $\langle g \rangle$, il suffit maintenant de prouver que ce sous-ensemble est un sous-groupe. Mais c'est assez facile (on ne lui a guère laisser le choix comme on va le voir) : il contient $e = g^{*0}$, il est stable par produit car $g^{*i} * g^{*j} = g^{*i+j}$ et il contient l'inverse g^{*-i} de tout élément g^{*i}. L'affirmation est donc démontrée.

Le reste de la preuve consiste maintenant à étudier cet ensemble des puissances de g : $\{g^{*n}, n \in \mathbb{N}\}$. On va considérer *les deux cas de figure : soit il existe $0 \leq i < j$ tels que $g^{*i} = g^{*j}$ soit pour tout $i \neq j \in \mathbb{N}$, on a $g^{*i} \neq g^{*j}$.*

- Considérons d'abord le premier cas. Alors par simplification dans un groupe (lemme 2.9) on a que $g^{*(j-i)} = e$ d'où il suit qu'il existe un entier $k > 0$ tel que $g^{*k} = e$. Par

suite il existe un plus petit entier naturel > 0 qui vérifie cette propriété. Notons le n. On veut montrer que $n = \mathrm{ord}(g)$. Pour cela on va directement établir le point (3) dans ce cas. Déjà notons que les éléments $e, g, \ldots, g^{*(n-1)}$ sont 2 à 2 distincts. En effet sinon, il existerait $0 \leq p < q \leq n-1$ tels que $g^{*p} = g^{*q} \Leftrightarrow g^{*(q-p)} = e$. Or $0 < q - p < n$ par hypothèse sur p, q. Ceci contredit la minimalité de n et donc ce cas de figure est impossible. On sait donc que l'ensemble $\{e, g, g^{*2}, \cdots, g^{*(n-1)}\}$ est de cardinal (les éléments sont tous distincts) et il est inclus dans $\langle g \rangle$ d'après notre remarque clé ci-dessus. Montrons l'inclusion réciproque.

Soit $i \in \mathbb{Z}$. Effectuons la division euclidienne de i par n : $i = q_i n + r_i$ (avec $r_i \in \{0, 1, \ldots, n-1\}$. Alors on a

$$g^{*i} = g^{q_i n + r_i} = (g^{*n})^{*q_i} * g^{*r_i} = e^{*q_i} * g^{*r_i} = g^{*r_i} \tag{4}$$

Ainsi $g^{*i} \in \{e, g, g^{*2}, \cdots, g^{*(n-1)}\}$. On a prouvé l'inclusion inverse et on a donc que $\langle g \rangle = \{e, g, g^{*2}, \cdots, g^{*(n-1)}\}$ et ce groupe est de cardinal n. Ce qui prouve (1) et (3) du moins dans le premier cas que nous avons regardé.

- Regardons maintenant le deuxième cas. On suppose donc $g^{*i} \neq g^{*j}$ pour des entiers naturels distincts $i \neq j$. Le sous-ensemble $\{g^{*i},\ i \in \mathbb{N}\}$ est donc infini et comme il est inclus dans $\langle g \rangle$ par notre remarque clé, on a que $\mathrm{ord}(g) = \infty$. Enfin, par hypothèse on a déjà que $g^{*i} \neq 0$ si i est un entier > 0. Si $i < 0$, alors $g^{*i} = e \Leftrightarrow e = g^{*-i}$ (par simplification par g^{*i}) ce qui est exclu car $-i > 0$. On a donc bien démontré (2). Pour finir de montrer (1), il reste à montrer que si $g^{*n} \neq e$ pour $n > 0$, alors $g^{*i} \neq g^{*j}$ pour tout $0 \leq i < j$. C'est immédiat car sinon $g^{*(j-i)} = e$ et contredit notre hypothèse puisque $j - i > 0$.

□

Notons tout de suite trois conséquences très utiles de la proposition et de sa preuve

Corollaire 3.55. *Soit $(G, *)$ un groupe et $g \in G$.*

(1) Pour tout $m \in \mathbb{Z}$, si $g^{*m} = e$, alors $\mathrm{ord}(g)$ divise m (autrement dit m est un multiple de $\mathrm{ord}(g)$).
(2) Si g est d'ordre n, alors pour tout $i \in \mathbb{Z}$, on a que $g^{*i} = g^{*r_i}$ où r_i est le reste dans la division euclidienne de i par n.
(3) Si g est d'ordre n, l'application $\langle g \rangle = \{g^{*i},\ i = 0 \cdots n-1\} \to \mathbb{Z}/n\mathbb{Z}$ définie par $g^{*i} \mapsto \overline{i}$ est un isomorphisme de groupes. Si g est d'ordre infini, alors $g^{*i} \mapsto i$ est un isomorphisme entre $\langle g \rangle$ et $\mathbb{Z}$.

Démonstration. On peut remarquer que l'on a déjà démontré (2) dans la preuve de la proposition 3.53. C'est précisément la formule (4).

Utilisons cette formule pour démontrer (1) : on a pour tout entier relatif m que

$$g^{*m} = g^{*r_m},$$

avec $r_m \in \{0, \ldots, \mathrm{ord}(g) - 1\}$. Or on a vu dans la proposition 3.53 que $g^{r_m} \neq e$ si $r_m \neq 0$. La réciproque $g^{*0} = e$ est vraie par définition. Conclusion : $g^{*m} = e$ est équivalent à $r_m = 0$ ce qui est équivalent à m est divisible par ordre de g.

Il reste à montrer (3). L'application est définie sans ambiguïté puisque les g^{*i} sont tous distincts pour $i \in \{0, \ldots, n-1\}$. Il reste à vérifier que c'est un morphisme de groupes. Notons $\psi : g^{*i} \mapsto \overline{i}$ cette application. On doit vérifier que

$$\psi(g^{*i} * g^{*j}) = \psi(g^{*i}) \overline{+} \psi(g^{*j}) = \overline{i} + \overline{j}.$$

Or $\psi(g^{*i} * g^{*j}) = \psi(g^{*(i+j)})$. Pour déterminer son image, on doit utiliser la propriété (2) (car ψ n'est défini qu'en écrivant un élément sous sa forme g^{*k} avec $k \in \{0, \ldots, n-1\}$). On a alors que

$$\psi(g^{*i} * g^{*j}) = \psi(g^{*(i+j)}) = \psi(g^{r_{i+j}}) = \overline{r_{i+j}} = \overline{i+j}$$

puisque par définition $i+j \equiv r_{i+j}$ modulo n. On a bien montré la formule cherchée ! Dans le cas d'ordre infini, la première partie de la définition nous donne déjà que l'application est un morphisme de groupes (le seul point à vérifier étant que les g^{*i} sont tous distincts ce que l'on a par la proposition 3.53).

Il reste à voir que ces morphismes sont des isomorphismes. Dans le cas fini, par égalité des cardinaux, il suffit de vérifier que ce morphismes est injectif, ce qui est trivial ici. Pour le deuxième cas, il est également facile de vérifier qu'il est injectif et surjectif. □

En particulier le corollaire nous dit que

le groupe engendré par un élément est soit isomorphe à $\mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$,
soit isomorphe à $\mathbb{Z}$ *si* $\mathrm{ord}(g) = \infty$.

Remarque 3.56. Les inverses des isomorphismes donnés par (3) sont évidemment les morphismes $n \mapsto g^{*n}$ dans le cas d'ordre infini. Et dans le cas fini, c'est le morphisme $\overline{i} \mapsto g^{*i}$ (la preuve du corollaire nous assurant que ce morphisme est bien défini).

Le corollaire suivant est aussi très utile.

Corollaire 3.57. *Si G est un groupe fini, alors, pour tout $g \in G$, on a $g^{\mathrm{card}(G)} = e$. En particulier* $\mathrm{ord}(g)$ *divise* $\mathrm{card}(G)$.

Démonstration. Si G est de cardinal fini, alors tout sous-groupe est de cardinal fini, donc $\langle g \rangle$ est fini et par le Théorème de Lagrange son cardinal divise $\mathrm{card}(G)$ ce qui conclut pour le premier point. Le deuxième a été vu dans le corollaire précédent. □

Exemple 3.58. Soit p un nombre premier.

- Dans $\mathbb{Z}/p\mathbb{Z}$, tout élément non nul est d'ordre p car p est premier.
- Dans $\mathbb{Z}/p^2\mathbb{Z}$, tout élément est d'ordre $1, p, p^2$. On trouve facilement que les éléments d'ordre p sont $\{p, 2p, \cdots, (p-1)p\}$.

Définition 3.59. Un groupe G est dit ***cyclique* fini** si il existe un élément g d'ordre fini tel que $G = \langle g \rangle$.

Un groupe G est dit ***cyclique* infini** si il existe un élément g d'ordre infini tel que $G = \langle g \rangle$.

Un élément g vérifiant les conditions ci-dessus s'appelle un **générateur** de G.

Terminologie 3.60. On trouvera aussi la terminologie monogène à la place de cyclique dans la littérature. Par ailleurs le plus souvent le mot cyclique tout seul sous-entend fini dans la littérature.

On dira aussi dans le cas ci-dessus que G est **engendré par** g (si g est un élément vérifiant que $\langle g \rangle = G$).

Plus généralement une famille $S \subset G$ est appelée une *famille génératrice*, ou un ensemble de générateurs, d'un groupe G si $\langle S \rangle = G$.

Remarque 3.61 (Un groupe cyclique est abélien, isomorphe à $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}$). Le corollaire 3.55 nous dit qu'un groupe cyclique fini est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$ et qu'un groupe cyclique infini est isomorphe à $\mathbb{Z}$. Et il est abélien puisque isomorphe à un groupe abélien. On peut aussi utiliser directement qu'il est de la forme $\{g^{*i}\}$ et que les puissances de g commutent tout le temps entre elles !

Exemple 3.62.

- Le groupe $\mathbb{Z}$ est cyclique infini (on peut prendre $g = \pm 1$ et uniquement eux comme générateur).
- Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique fini pour tout n. Il admet comme générateur tout $\overline{i}$ tel que $i \wedge n = 1$; par exemple $\overline{1}$.

- Le sous-ensemble $\mu_n := \{z \in \mathbb{C},\ z^n = 1\}$ des racines $n$ièmes de l'unité est un sous-groupe cyclique de $\mathbb{C}^*$, de cardinal n (engendré par $\exp(2i\frac{\pi}{n})$ par exemple). Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ comme groupe.
- Trivialemennt, dans tout groupe $G \neq \{e\}$, la famille $G \setminus \{e\}$ est une famille de générateurs de G (mais pas forcément une très intéressante). On verra des familles plus intéressantes dans ce cours. Par exemple les transpositions engendrent le groupe symétrique S_n.

L'intérêt d'avoir une famille génératrice est qu'on peut écrire tous les éléments de G comme des mots de longeur finie en les éléments générateurs. Ce qui permet parfois de mieux comprendre le groupe et ses propriétés. Ceci conduit à la notion de groupes définis par générateurs et relations (que nous n'étudierons pas dans ce cours faute de temps !)

Remarque 3.63. Le Théorème de Lagrange et ses corollaires sont très utiles pour comprendre un groupe. On a déjà vu des exemples pour caractériser les sous-groupes et propriétés des éléments. Notons que vous pouvez appeler ces propositions et corollaires "Lagrange" aussi ; on vous comprendra. Voyons d'autres exemples.

Exemple 3.64. Si G est un groupe de cardinal 65379 alors aucun élément g de G ne vérifie $g^2 = e$. En effet, un tel élément serait d'ordre 2. Mais 2 ne divise pas 65379, donc un tel élément n'existe pas dans G (par le corollaire 3.51).

Exemple 3.65 (A quoi ressemble un groupe de cardinal 17 ?). Soit G un groupe de cardinal 17. Alors tout élément est d'ordre un diviseur de 17 par le corollaire du théorème de Lagrange. Comme 17 est premier, les seuls diviseurs sont 1 et 17. Le cas 1 correspond à l'élément neutre (par le corollaire 3.51). Donc tout les éléments (sauf e) sont d'ordre 17.

En particulier pour tout élément $g \neq e$, on a que $\langle g \rangle$ est de cardinal 17 ; et comme c'est un sous-groupe de G, alors $\langle g \rangle = G$.

Ainsi on vient de montrer que tout groupe de cardinal 17 est forcément cyclique (c'est la définition), en particulier abélien, et isomorphe à $\mathbb{Z}/17\mathbb{Z}$ (par le corollaire 3.55). Ainsi, à isomorphisme près, il y a un unique groupe de cardinal 17. Cette étude marche pour tout groupe de cardinal un nombre premier.

Exemple 3.66 (A quoi ressemble un groupe *abélien* de cardinal 9 ?). Par le corollaire du théorème de Lagrange, nous savons que tout élément d'un groupe G de cardinal 9 est d'ordre 1, 3 ou 9. Évidemment le seul élément d'ordre 1 est e (toujours par le corollaire 3.51).

Si maintenant il existe un élément g d'ordre 9, alors par le raisonnement de l'exercice précédent, $\langle g \rangle = G$ et donc G est cyclique isomorphe à $\mathbb{Z}/9\mathbb{Z}$ (par le corollaire 3.55).

Sinon, tous les éléments $\neq e$ sont d'ordre 3. Soit $a \neq e$. On a $\langle a \rangle = \{e, a, a^2\}$. Soit $b \neq e, a, a^2$ qui existe vu qu'il y a 9 éléments dans G. Comme b est d'ordre 3, $b^2 = b^{-1}$ (puisque $b^3 = e$). Il suit que $b^2 = b^{-1} \notin \langle a \rangle$ sinon b serait dans ce sous-goupe aussi. En particulier $\langle a \rangle \cap \langle b \rangle = \{e\}$

Regardons maintenant l'application $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to G$ donnée par $(\bar{i}, \bar{j}) \mapsto a^i b^j$. On peut vérifier que c'est bien un morphisme de groupes (attention : on utilise que G est abélien là). Il est par ailleurs injectif car si $a^i b^j = e$, alors $a^i = b^{-j}$ par simplification ce qui implique que a^i et b^{-j} sont dans $\langle a \rangle \cap \langle b \rangle = \{e\}$. Ainsi i et j sont des multiples de 3 par le (1) du corollaire 3.55. Ainsi $\bar{i} = \bar{j} = \bar{0}$ dans $\mathbb{Z}/3\mathbb{Z}$. Ce qui prouve l'injectivité. Comme ces deux groupes sont de même cardinaux, cette application est donc un isomorphisme de groupes.

On a donc montré qu'un groupe abélien d'ordre 9 *est isomorphe soit à* $\mathbb{Z}/9\mathbb{Z}$ *soit à* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Par ailleurs, ces deux derniers groupes ne sont pas isomorphes. En effet dans $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, tout élément est d'ordre plus petit que 3, donc pour tout x, $x^3 = 1$. Mais ce n'est pas

le cas dans $\mathbb{Z}/9\mathbb{Z}$ (par exemple $\overline{1}$ est d'ordre 9). Si on a un morphisme $f : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ alors $f(x)^3 = f(x^3)$ serait tout le temps égal à e. Donc $\overline{1}$ n'est pas dans l'image de f. Ainsi aucun tel morphisme de groupes ne peut être surjectif et donc il n'y a pas d'isomorphismes entre eux.

On peut démontrer, qu'en fait, tout groupe de cardinal 9 (ou plus généralement de cardinal p^2, p premier) est abélien.

Remarque 3.67. Si $f : G \to H$ est un isomorphisme de groupes, alors pour tout $g \in G$, on a $\mathrm{ord}(f(g)) = \mathrm{ord}(g)$. Cette affirmation a été vue dans le DM1.

De manière générale,un isomorphime de groupes transfère et préserve toutes les propriétés qui s'expriment en termes des axiomes de groupes (produit, inverse, élément neutre, et quantificateurs $\exists$, $\forall$) et de cardinaux. Ainsi un groupe isomorphe à un groupe abélien est abélien, un groupe isomorphe à un groupe cyclique est cyclique etc...

3.5. **Quelques constructions.** On rappelle ici quelques constructions utilisées pendant le cours et le TD. Tout d'abord le produit de groupes.

Lemme 3.68. *Soit $(G, *_G)$ et $(H, *_H)$ deux groupes. L'ensemble $G \times H$ muni de la multiplication*

$$\begin{array}{rcl} (G \times H) \times (G \times H) & \longrightarrow & G \times H \\ \big(g_1, h_1, g_2, h_2\big) & \longmapsto & (g_1 *_G g_2, h_1 *_H h_2) \end{array}$$

est un groupe, appelé ***produit direct*** *de G et H.*

Le produit direct de deux groupes revient donc juste à faire les opérations coordonnées par coordonnées sans aucun interaction entre elles.

Démonstration. Comme $g_1 *_G g_2$ et $h_1 *_H h_2$ sont respectivement dans G et H, $(g_1 *_G g_2, h_1 *_H h_2)$ est bien dans $G \times H$ et la loi est donc bien une loi de composition interne. On a que (e_G, e_H) est l'élément neutre. En effet, pour tous $g_1 \in G$, $h_1 \in H$, on a

$$(g_1 *_G e_G, h_1 *_H e_H) = (g_1, g_2) = (e *_G g_1, e *_H h_1).$$

On laisse en exercice de vérifier l'associativité et l'inversibilité (qui proviennent de celles de G et H respectivement) qui se font de manière similaire. □

Exemple 3.69.

- On peut noter que $(\mathbb{R}^2, +)$ est le groupe produit direct $(\mathbb{R}, +) \times (\mathbb{R}, +)$ puisque $(x_1, y_1 + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$.
- On a croisé le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. À isomorphisme près, c'est l'un des deux seuls groupes de cardinal 4 ; l'autre étant $\mathbb{Z}/4\mathbb{Z}$ comme nous le verrons. Ils sont non-isomorphes (voir le TD).
- Le lemme chinois dit que le *groupe produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ si $n \wedge m = 1$.*

  Preuve : on a un morphisme de groupes $p : \begin{array}{rcl} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \overline{k}^{nm} & \longmapsto & (\overline{k}^n, \overline{k}^m) \end{array}$: c'est une conséquence de la compatibilité de l'addition avec les congruences et du fait que $\overline{k}^{nm} = \overline{k'}^{nm}$ signifie que $k - k'$ est divisible par nm donc par n et par m et il suit que $\overline{k}^n = \overline{k'}^n$ et $\overline{k}^m = \overline{k'}^m$. Ainsi l'application est bien définie et par ailleurs les lois d'addition étant simplement données en prenant l'addition usuelle modulo les congruences, c'est facile de vérifier que c'est un morphisme de groupes.

  Les deux groupes sont de même cardinal, à savoir nm. Il suffit donc de vérifier que le morphisme est injectif pour avoir qu'il est bijectif. Calculons son noyau : il s'agit des classes $\overline{k}^{nm}$ telles que

$$\left\{ \begin{array}{lll} \overline{k}^n & = 0 & \in \mathbb{Z}/n\mathbb{Z} \\ \overline{k}^m & = 0 & \in \mathbb{Z}/m\mathbb{Z}. \end{array} \right. \iff \left\{ \begin{array}{lll} k & \equiv 0 & [n] \\ k & \equiv 0 & [m] \end{array} \right.$$

Or le dernier système est équivalent, par le lemme chinois puisque n et m sont premiers entre eux, à $k \equiv 0[nm]$ et donc $\overline{k}^{nm} = \overline{0}^{nm}$. L'injectivité est montrée, et donc on a le résultat.

Remarque 3.70 (Il y a des produits *PAS* direct)*.* Le produit direct de deux groupes est une construction simple et universelle (au sens où c'est défini tout le temps par une même formule) d'un nouveau groupe à partir de G et H. Mais, attention il peut exister d'autre structures de groupes (même compatibles avec celles de G et H) sur le produit $G \times H$. On verra notamment des exemples de produit semi-direct [14]dans les notes de cours sur la géométrie affine ou le groupe diédral.

Rajoutons une dernière notion utile pour les groupes non-abéliens.

Définition 3.71 (Centre d'un groupe)**.** Soit G un groupe. Le centre de G est le sous-ensemble $Z(G) = \{h \in G, \forall g \in G, gh = hg\}$ des éléments de G qui commutent avec tout le monde.

Lemme 3.72. *Le centre d'un groupe G est un sous-groupe abélien de G.*

Démonstration. On a déjà que $e \in Z(G)$ puisque $eg = ge(= g)$. Si $x, y \in Z(G)$, alors pour tout $g \in G$, on a $(xy)g = x(yg) = x(gy) = (xg)y = gxy$ en utilisant l'associativité de la loi de groupe et le fait que x, y soient dans le centre pour les égalités au milieu. On montre de même que si g est dans le centre g^{-1} aussi. En effet

$$gx = xg \iff x = g^{-1}xg \iff xg^{-1} = g^{-1}x$$

par simplification successives. □

Exemple 3.73.
- Évidement, $Z(G) = G$ si et seulement si G est abélien.
- Soit E un $\mathbb{F}$ espace vectoriel. Le centre $Z(GL(E))$ est égal à $\mathbb{F}\,\mathrm{id}$, c'est à dire les matrices d'homothéties.

4. Groupes symétriques/des permutations

Nous allons dans cette section étudier en détail un exemple fondamental de groupes, celui des bijections d'un ensemble *fini*. Rappelons que pour tout ensemble X, $(\mathrm{Bij}(X), \circ)$ est un groupe (proposition 2.11).

4.1. Généralités sur les groupes de bijections.

Ces groupes de bijections dans le cas fini interviennent dans de nombreux autres domaines des mathématiques et de manière générale les groupes de bijection d'un ensemble sont universels vis à vis de l'action d'un groupe, voir remarque 3.8. En particulier, ils agissent de manière naturel sur l'ensemble X :

Lemme 4.1. *L'application* $\begin{array}{ccc} \mathrm{Bij}(X) \times X & \longrightarrow & X \\ (f, x) & \longmapsto & f(x) \end{array}$ *est une action à gauche de* $(\mathrm{Bij}(X), \circ)$*, appelée* action canonique*.*

Cet exemple et très important ; vérifier que vous comprenez et savez refaire la preuve ci-dessous.

Démonstration. Notons, pour $f \in \mathrm{Bij}(E)$, $x \in X$, $f * x = f(x)$ l'action. On doit montrer que pour tout $f, g \in \mathrm{Bij}(X)$ et $x \in X$, on a $f * (g * x) = (f \circ g) * x$. Or

$$f * (g * x) = f * (g(x)) = f\big(g(x)\big) = (f \circ g(x)) = (f \circ g) * x$$

par définition de la composition. □

Remarque 4.2. La remarque 3.8 montre qu'en fait l'action de tout groupe G sur un ensemble X se factorise au travers de l'action canonique de $\mathrm{Bij}(X)$.

14. qui tient son nom du fait qu'une seule des composantes a une multiplication donnée comme pour le produit direct

Exemple 4.3. On considère l'action canonique de $\mathrm{Bij}(X)$ sur X. Alors

- pour tout $x \in X$, on a $\mathrm{stab}_x = \{f \in \mathrm{Bij}(X),\ f(x) = x\}$ c'est à dire l'ensemble des bijections pour lesquelles x est un point fixe.
- pour tout $g \in \mathrm{Bij}(X)$, on a $\mathrm{Fix}(g) = \{x \in X, g(x) = x\}$ est l'ensemble des points fixes de g.

Exercice 4.4. Démontrer les résultats énoncés dans l'exemple.

Ces groupes de bijection d'un ensemble fini ne dépendent (à isomorphismes près) que du cardinal de l'ensemble. Plus précisément, si X et Y sont en bijection (en particulier si ils ont même cardinal), ils ont des groupes de bijection isomorphes.

Proposition 4.5. *Soit $f : X \to Y$ une bijection entre deux ensembles. Alors l'application* $\begin{array}{ccc} \mathrm{Bij}(X) & \longrightarrow & \mathrm{Bij}(Y) \\ \varphi & \longmapsto & f \circ \varphi \circ f^{-1} \end{array}$ *est un isomorphisme de groupes.*

Démonstration. Il faut vérifier que $Ad_f : \begin{array}{ccc} \mathrm{Bij}(X) & \longrightarrow & \mathrm{Bij}(Y) \\ \varphi & \longmapsto & f \circ \varphi \circ f^{-1} \end{array}$ est bien définie. En effet les composées $f \circ \varphi \circ f^{-1}$ sont bien définies, mais il faut vérifier qu'elles donnent bien une bijection. C'est en fait immédiat car la composée de bijections (et l'inverse d'une bijection) est une bijection.

Montrons que c'est un morphisme de groupes : On a, pour tout $\varphi, \psi \in \mathrm{Bij}(X)$, que

$$Ad_f(\varphi \circ \psi) = f \circ (\varphi \circ \psi) \circ f^{-1} = f \circ \varphi \circ f^{-1} \circ f \circ \psi \circ f^{-1} = Ad_f(\varphi) \circ Ad_f(\psi)$$

en utiisant au milieu que $\mathrm{id}_Y = f \circ f^{-1}$. Cette égalité montre que Ad_f est un morphisme de groupes. Il ne reste plus qu'à voir qu'il est bijectif. On réutilise une idée que l'on a déjà vu (Proposition 3.7) : f^{-1} est aussi une bijection de Y sur X. On peut alors considérer $Ad_{f^{-1}} : \begin{array}{ccc} \mathrm{Bij}(Y) & \longrightarrow & \mathrm{Bij}(X) \\ \alpha & \longmapsto & f^{-1} \circ \alpha \circ f \end{array}$ qui est bien définie comme ci-dessus.

Comme $f \circ f^{-1} = \mathrm{id}_Y$ et $f^{-1} \circ f = \mathrm{id}_X$, on a que pour tout $\varphi \in \mathrm{Bij}(X)$ et $\alpha \in \mathrm{Bij}(Y)$,

$$Ad_f \circ Ad_{f^{-1}}(\alpha) = Ad_f(f^{-1} \circ \alpha \circ f) = f \circ f^{-1} \circ \alpha \circ f \circ f^{-1} = \mathrm{id}_Y \circ \alpha \circ \mathrm{id}_Y = \alpha$$

et de même

$$Ad_{f^{-1}} \circ Ad_f(\varphi) = Ad_{f^{-1}}(f \circ \varphi \circ f) = f^{-1} \circ f \circ \varphi \circ f^{-1} \circ = \mathrm{id}_X \circ \varphi \circ \mathrm{id}_X = \varphi.$$

Il suit que $Ad_{f^{-1}}$ est l'inverse de Ad_f et donc que Ad_f est bijective. □

4.2. **Groupe symétrique : définition, support, exemples.** Spécifions maintenant une famille de groupes de bijections importante.

Définition 4.6 (**Groupe des permutations/symétrique**)**.** On notera $S_n = \mathrm{Bij}(\{1, \ldots, n\})$ et on l'appellera groupe des permutations d'un ensemble à n-éléments ou parfois groupe symétrique sur n-éléments. Il est évidemment muni de la composition comme loi de groupe. On notera souvent $\sigma \cdot \tau = \sigma \circ \tau$ le produit.

On notera $S_0 = \mathrm{Bij}(\emptyset)$ également.

On trouvera parfois la terminologie de groupe symétrique d'ordre n, terminologie dangereuse car n n'est pas l'ordre de S_n (au sens du cardinal) ! Nous essaierons de l'éviter. On utilisera les deux autres de manière interchangeable.

Tout d'abord ce groupe est le [15] groupe des bijections de tout ensemble à n-éléments.

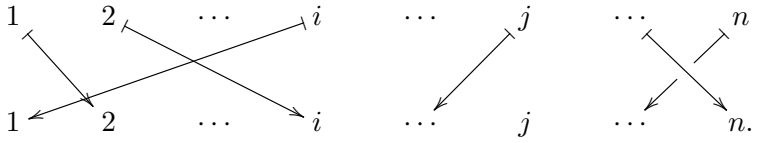
Corollaire 4.7. *Si X est un ensemble de cardinal n, alors $(\mathrm{Bij}(X), \circ)$ est un groupe isomorphe au groupe symétrique S_n.*

15. à isomorphisme de groupes près bien sûr

Démonstration. Par définition du cardinal (voir le cours de L1 d'algèbre et structures), on a qu'il existe une bijection $f : X \to \{1, , \dots, n\}$. La proposition 4.5 nous fournit un isomorphisme de groupes explicite entre $\mathrm{Bij}(X)$ et $S_n = \mathrm{Bij}(\{1, \dots, n\}$. □

Terminologie 4.8. On appelle un élément de S_n une *permutation.*

Pourquoi cette terminologie ? Tout simplement parce qu'une bijection de $\{1, \dots, n\}$ est une façon de réordonner [16] les chiffres $1...n$, autrement dit de les changer de place, autrement dit de les permuter. Autrement dit, un élément $\sigma \in S_n$ ressemble à cela :



Ceci suggère la notation standard ci-dessous.

Notation 4.9. On notera une permutation, c'est à dire un élément $\sigma \in S_n$, sous la forme

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Cette écriture se lit de haut en bas. Sur la ligne du dessus, on met les éléments aux départs, les antécédents, et sur la ligne du dessous on met les images de σ. En dessous de i, on met $\sigma(i)$.

Lemme 4.10. *On a* $\mathrm{card}(S_n) = n! = \prod_{i=1}^{n} i = n \cdot (n-1) \cdots 2 \cdot 1$.

Démonstration. Voir le L1. Il faut savoir faire cette preuve. Il s'agit de savoir compter le nombre de bijections entre deux ensembles de même cardinaux (ce qui est la même chose que le nombre d'injections). □

Remarque 4.11. Puisque S_n est fini, par le Théorème de Lagrange, tout élémént de S_n est d'ordre fini.

Exemple 4.12 (Exemples triviaux). On a que $S_0 = \{\mathrm{id}_\emptyset\}$ est le groupe trivial à un élément. En effet il existe une unique application $\emptyset \to \emptyset$ qui est l'identité.

De même, $S_1 = \{\mathrm{id}_{\{1\}}\}$ est le groupe trivial à un élément car il n'y a qu'une application de $\{1\}$ vers lui-même.

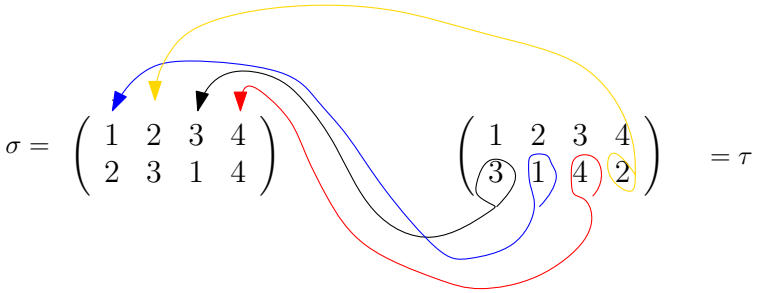
Les groupes S_n sont évidemment plus intéressant pour $n \geq 2$.

Exemple 4.13 (Le groupe S_2). En utilisant la notation 4.9, on a que $S_2 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{\mathrm{id}}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$

Exemple 4.14 (Le groupe S_3). Pour trouver tous les éléments de S_3, il suffit de procéder *algorithmiquement* comme suit : 1 peut avoir 3 images possibles 1, 2 ou 3. On commence alors à écrire tous les cas où 1 s'envoie sur 1 ; puis toutes celles où 1 s'envoie sur 2 et enfin toutes celles où 1 s'envoie sur 3.

Une fois qu'on a fixé l'image de 1, il reste deux choix possibles pour 2 : les deux valeurs différentes de 1. On écrit donc les 2 cas possibles pour chacun des choix de 1-ci dessus.

16. Rappelons qu'une bijection de $\{1, \dots, n\}$ sur un ensemble E est simplement une façon de numéroter de 1 à n les éléments de E, ou dit autrement, de positionner un élément en première position, un autre en deuxième, etc...



$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

FIGURE 1. Composition de deux permutations

Enfin il n'y a plus rien à choisir pour 3 puisqu'il reste qu'un seul élément non utilisé à l'arrivée. Cela donne :

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \right\}$$

Cet algorithme marche évidemment pour tout entier n !

Remarque 4.15 (**Inverse**). Avec l'écriture de la notation 4.9, il est facile de calculer l'inverse ou la composition.

En effet, ***il suffit de lire la permutation à l'envers, c'est à dire de bas en haut***, et de la réécrire dans le sens normal. En effet on a l'équivalence

$$\sigma(i) = j \iff i = \sigma^{-1}(j).$$

Donc $\sigma^{-1}(j)$ est l'élément au dessus de j dans l'écriture 4.9 ce qui justifie l'algorithme ci-dessus.

Exemple 4.16. Regardons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. Alors pour calculer σ^{-1} on regarde la préimage de 1, c'est à dire le nombre au dessus de 1 qui est 3, puis le nombre au dessus de 2 qui est 1 etc... Cela nous donne :

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \text{et} \qquad \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Remarque 4.17 (**Composition**). Comment calcule-t-on la structure de groupe de S_n. La structure de groupe est donnée par la composition (puisque c'est un groupe de bijection) : $\sigma * \tau = \sigma \circ \tau$. Donc $\sigma * \tau(i) = \sigma\big(\tau(i)\big)$. *Pour calculer la composition de σ et τ et l'écrire sous la forme de la notation 4.9, on part donc de i sur la première ligne, on regarde son image par τ, c'est à dire le nombre juste en dessous dans la deuxième ligne, on le reporte sur la première ligne de σ et on regarde le nombre juste en dessous et c'est le nombre qu'on veut !*. Voir la figure (1).

Exemple 4.18. Par exemple regardons le produit $\sigma \cdot \tau$ avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. En appliquant l'algorithme ci-dessus, on obtient que 1 s'envoie par τ sur 3 qui s'envoie par σ sur 1 :

$$1 \overset{\tau}{\mapsto} 3 \overset{\sigma}{\mapsto} 1.$$

De même, on a

$$2 \overset{\tau}{\mapsto} 1 \overset{\sigma}{\mapsto} 2, \qquad 3 \overset{\tau}{\mapsto} 4 \overset{\sigma}{\mapsto} 4, \qquad 4 \overset{\tau}{\mapsto} 2 \overset{\sigma}{\mapsto} 3.$$

On obtient donc

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

Remarque 4.19 (S_n est un sous-groupe de S_{n+1} canoniquement). Il est souvent pratique d'identifier a S_n comme un sous-groupe de S_m pour $m > n$. Il y a une façon canonique de le faire. En effet, l'application $\iota : S_n \mapsto S_m$ qui envoie σ sur la permutation $\iota(\sigma)$ définie, pour tout $i \in \{1, \dots, m\}$, par $\sigma(i) = \begin{cases} \sigma(i) & \text{si } i \leq n \\ i & \text{si } i > n \end{cases}$ est un morphisme de groupes injectif.

Il identifie S_n au sous-groupe de S_m des permutations qui laissent fixe tous les points plus grand strictement que n.

On identifiera souvent S_n avec ce sous-groupe sans en faire nécessairement la remarque !

On a vu que les groupes de bijections d'un ensemble X agissent canoniquement sur X. Ainsi S_n agit canoniquement sur $\{1, \dots, n\}$ par la formule, pour tout $\sigma \in S_n$, $i \in \{1, \dots, n\}$ (cf lemme 4.1) :

$$\sigma * i = \sigma(i). \tag{5}$$

En particulier, si $\sigma \in S_n$, on a que $\mathrm{Fix}(\sigma) = \{i \in \{1, \dots, n\}, \sigma(i) = i\}$ est l'ensemble des points fixe de σ. C'est à dire les points sur lesquels agit trivialement.

À l'opposé, on va s'intéresser aux points qui sont transformés par σ.

Définition 4.20 (Support d'une permutation). On appelle *support* d'une permutation σ le sous-ensemble

$$\mathrm{Supp}(\sigma) = \{1, \dots, n\} \setminus \mathrm{Fix}(\sigma) = \{i \in \{1, \dots, n\}, \sigma(i) \neq i\}.$$

Le support de σ est donc précisément le sous-ensemble des points qui sont envoyés sur des points *différents* par σ. Autrement dit, c'est l'endroit où il se passe des choses intéressantes/non-triviales pour σ. En particulier,

on doit retenir que : ***si*** $i \notin \mathrm{Supp}(\sigma)$***, alors*** $\sigma(i) = i$***.***

Exemple 4.21. On a $\mathrm{Supp}(\sigma) = \emptyset \iff \sigma = \mathrm{id}$.

Exemple 4.22. On a $\mathrm{Supp}\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}\right) = \{1, 2, 3\}$, $\mathrm{Supp}\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}\right) = \{2, 3\}$, $\mathrm{Supp}\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}\right) = \{1, 3, 4\}$.

Remarque 4.23. Quel que soit σ, $\mathrm{Supp}(\sigma)$ n'est jamais un singleton. En effet si $i \in \mathrm{Supp}(\Sigma)$, on a que $\sigma(i) = j \neq i$. Mais alors, par injectivité de σ, $\sigma(j) \neq j$ et donc $j \neq i$ est aussi dans le support de σ.

Les permutations dont le support est constitué d'exactement deux éléments s'appellent des *transpositions*. Nous les reverrons ci-dessous : ce sont aussi exactement les 2-cycles.

La notion de support est notamment intéressante car elle permet de véritablement partitionner σ en deux parties, l'une où elle est triviale (=égale à l'identité) et l'autre où c'est une bijection sans aucun points fixes. Précisément, on a l'*important lemme suivant.*

Lemme 4.24. *Soit $\sigma \in S_n$ une permutation.*

- *Alors la restriction de σ à son support est une bijection $\sigma_{|\mathrm{Supp}(\sigma)} : \mathrm{Supp}(\sigma) \xrightarrow{\simeq} \mathrm{Supp}(\sigma)$.*
- *On a $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$.*
- *On a $\mathrm{Supp}(\sigma \circ \tau) \subset \mathrm{Supp}(\sigma) \bigcup \sigma_{|\mathrm{Supp}(\tau)}$.*

Démonstration. Démontrons le premier point. Si $i \in \mathrm{Supp}(\sigma)$, alors $\sigma(i) \neq i$. Comme σ est injective, il suit que $\sigma(\sigma(i)) \neq \sigma(i)$. Donc $\sigma(i) \in \mathrm{Supp}(\sigma)$. Ainsi, la restriction $\sigma_{|\mathrm{Supp}(\sigma)}$ de σ à $\mathrm{Supp}(\sigma)$ est une application dont l'image est incluse dans $\mathrm{Supp}(\sigma)$, elle donne donc bien une application $\sigma_{|\mathrm{Supp}(\sigma)} \to \sigma_{|\mathrm{Supp}(\sigma)}$. Elle est de plus injective car restriction d'une application injective. Comme les ensembles de départs et d'arrivée sont les mêmes, de cardinal fini, cette application injective est donc en fait même bijective.

Pour le second point, ona que $i \neq \sigma(i) \iff \sigma^{-1}(i) \neq i$ en composant par σ^{-1} et en utilisant son injectivité. Ceci donne l'égalité des supports.

Pour le dernier point, il a été vu en TD. On rappelle qu'il suffit de montrer la contraposée : Si $x \notin (\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau)$, alors $x \notin \sigma \circ \tau$ ce qui par définition du support est équivalent à montrer que $\sigma \circ \tau(x) = x$ Or comme $x \notin \mathrm{Supp}(\tau)$, $\sigma \circ \tau(x) = \sigma(\tau(x)) = \sigma(x) = x$ car $x \notin \mathrm{Supp}(\sigma)$. □

Remarque 4.25. Dans le troisième point l'inclusion peut être stricte. Par exemple si $\tau = \sigma^{-1}$, alors $\sigma \circ \tau = \mathrm{id}$ est de support vide !

Mais il peut aussi bien sûr aussi y avoir égalité selon σ et τ. Un cas important est lorsque les supports sont disjoints. En effet, on a le lemme suivant.

Lemme 4.26. *Si σ et τ sont à support* disjoints [17]*, alors* $\mathrm{Supp}(\sigma \circ \tau) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$.

La preuve est une idée qui revient souvent avec les permutations.

Démonstration. On a déjà l'inclusion donnée par le lemme 4.24. On veut montrer l'inclusion inverse. Soit $i \in \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$. On doit voir que $\sigma \circ \tau(i) \neq i$. On a deux cas de figure, puisque $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$:

(1) soit $i \in \mathrm{Supp}(\sigma)$ mais $i \notin \mathrm{Supp}(\tau)$;
(2) soit $i \notin \mathrm{Supp}(\sigma)$ mais $i \in \mathrm{Supp}(\tau)$.

Considérons le premier cas : alors on a $\sigma(i) \neq i$ et $\tau(i) = i$. Donc

$$\sigma \circ \tau(i) = \sigma(\tau(i)) = \sigma(i) \neq i$$

comme voulu. Regardons le deuxième cas : on a $\tau(i) \neq i$. Par la première partie du lemme 4.24, on a que $\tau(i) \in \mathrm{Supp}(\tau)$. Donc il n'est pas dans le support de σ puisque ces ensembles sont disjoints. Il suit que $\sigma(\tau(i)) = \tau(i)$ qui est différent de i par ci-dessus. Donc

$$\sigma \circ \tau(i) = \sigma(\tau(i)) = \tau(i) \neq i$$

ce qui conclut. □

Les permutations à supports disjoints commutent entre elles, ce qui est une propriété *très importante.*

Proposition 4.27. *Soit σ et τ deux permutations à supports disjoints. Alors on a $\sigma \circ \tau = \tau \circ \sigma$. En particulier, pour tout $n \in \mathbb{N}$, on a*

$$(\sigma\tau)^n = \sigma^n \tau^n. \tag{6}$$

Démonstration. On calcule $\sigma \circ \tau(i)$ et $\tau \circ \sigma(i)$ pour tout $i \in \{1, \ldots, n\}$. La preuve est similaire à celle du lemme 4.26. On a 3 cas de figure :

(1) i n'est ni dans le support de σ, ni dans celui de τ ;
(2) $i \in \mathrm{Supp}(\sigma)$ mais $i \notin \mathrm{Supp}(\tau)$;

17. c'est à dire $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$

(3) $i \notin \mathrm{Supp}(\sigma)$ mais $i \in \mathrm{Supp}(\tau)$.

Dans le premier cas, on a $\sigma(i) = i = \tau(i)$ Et il suit que $\sigma(\tau(i)) = i = \tau(\sigma(i))$.

Dans le deuxième cas, on a $\tau(i) = i$. Alors $\sigma(\circ\tau(i)) = \sigma(i)$. Calculons $\tau \circ \sigma(i) = \tau(\sigma(i))$. Comme $i \in \mathrm{Supp}(\sigma)$, $\sigma(i)$ aussi par le lemme 4.24.(1). Donc $\sigma(i) \notin \mathrm{Supp}(\tau)$ et il suit que $\tau(\sigma(i)) = \sigma(i)$ ce qui conclut dans ce second cas.

Le troisième cas est similaire.

Le dernier point est un corollaire immédiat de la commutativité :

$$(\sigma\tau)^n = \sigma\tau\sigma\tau\sigma\tau\cdots\sigma\tau = \sigma\sigma\tau\tau\sigma\tau\cdots\sigma\tau = \cdots = \sigma^n\tau^n$$

en permutant tous les σ et tous les τ. □

Remarque 4.28. La propriété 3 du lemme 4.1 implique en particulier que $\mathrm{Supp}(\sigma^2) \subset \mathrm{Supp}(\sigma)$ Cela peut êter une égalité ou pas selon les valeurs de σ (par exemple si σ est un 3-cycle (voir ci-dessous) ce sera une égalité, mais ça n'est pas le cas pour une transposition.

De manière générale, $\mathrm{Supp}(\sigma^n) \subset \mathrm{Supp}(\sigma)$.

Remarque 4.29. Il suffit de connaître σ sur son support pour connaître tout σ puisque $\sigma(i) = i$ en dehors du support.

4.3. **Cycles et décompositions en cycles à support disjoints.** Nous allons étudier une classe simple de permutations, les cycles, généralisant les transpositions. On verra qu'elles permettent de décomposer en produits de permutations qui commutent ce qui simplifie grandement leur étude.

Définition 4.30. Soit $k \geq 2$ un entier. Un ***k*-cycle** de S_n est une permutation σ telle qu'il existe $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ des éléments distincts 2 à 2 et qu'on ait

- $\sigma(i) = i$ si $i \notin \{a_1, \ldots, a_k\}$;
- $\sigma(a_j) = a_{j+1}$ si $1 \leq j \leq k-1$;
- $\sigma(a_k) = a_1$.

On notera ce k-cycle $(a_1\, a_2\, \ldots\, a_k)$.

Il existe une unique permutation vérifiant les propriétés de la définition 4.30 car sa valeur est définie sur tous les entiers $i \in \{1, \ldots, n\}$.

Quelques propriétés 4.31. Les propriétés suivantes découlent directement de la définition.

- Par définition, $\mathrm{Supp}(a_1\, a_2\, \ldots\, a_k) = \{a_1, \ldots, a_k\}$.
- L'écriture $(a_1\, a_2\, \ldots\, a_k)$ n'est pas unique. En effet $(a_1\, a_2\, \ldots\, a_k) = (a_2\, a_3\, \ldots\, a_k\, a_1) = (a_3\, a_4\, \ldots\, a_k\, a_1\, a_2)$ ... Par exemple $(1\,3) = (3,1)$, $(7\,2\,4\,1) = (4\,1\,7\,2)$.
- En revanche $(a_1\, a_2\, \ldots\, a_k) \neq (a_2\, a_1\, a_3\, \ldots\, a_k)$ (si $k > 2$).

Exercice 4.32. Démontrer ces propriétés.

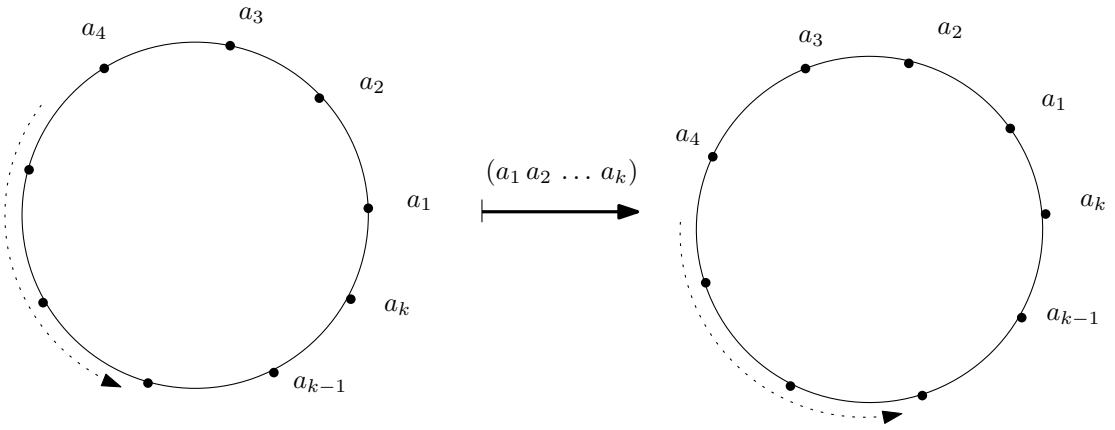
Terminologie 4.33. Un k-cycle s'appelle aussi un cycle de longueur k.

Un 2-cycle s'appelle une **transposition**.

On dira simplement σ est un cycle pour dire qu'il existe $k \geq 2$ tel que σ soit un k-cycle.

Notation 4.34. On notera $(a_1\, \ldots\, a_k) \cdot (i)$ l'image d'un élément $i \in \{1, \ldots, n\}$ par la permutation $(a_1\, \ldots\, a_k)$. Cette notation peut être un peu confusante, mais on doit se rappeler qu'il n'y a pas de 1-cycle et que donc la notation (i) signifiera toujours qu'on évalue une permutation sur l'élément i.

Remarque 4.35 (**Regardons les indices modulo k !**). Lorsque l'on définit un k-cycle, il est plus simple de considérer l'indice k dans a_k comme étant dans $\mathbb{Z}/k\mathbb{Z}$, cela permet de définir $(a_1\, a_2\, \ldots\, a_k) \cdot (a_i) = a_{i+1}$ (où on comprend les indices dans $\mathbb{Z}/k\mathbb{Z}$). Voir figure (2). On utilisera le plus souvent cette convention dans la suite.



Il est pratique de représenter un k-cycle sur un cercle pour comprendre la terminologie de *cycle* et la définition de $(a_1 \ldots a_k)$. Si on représente les a_i sur un cercle de 1 à k, alors l'action du k-cycle $(a_1 \ldots a_k)$ sur les a_i revient à tourner d'un cran le cercle sur la gauche.

FIGURE 2. Représentation graphique d'un k-cycle

Remarque 4.36. L'entier n n'apparaît pas dans la notation d'un k-cycle. C'est parce qu'il est en général sous-entendu. Et que par ailleurs on peut voir un k-cycle comme étant une permutation de tout S_n pour $n \geq \max(a_i,\, i = 1 \ldots k)$ puisque en dehors des a_i, le cycle agit trivialement et que l'on peut donc le plonger dans de tels S_m, voir la remarque 4.19.

Étudions maintenant les propriétés des cycles.

Il est très facile de lire l'inverse ou même les puissances d'un k-cycle.

Lemme 4.37. *Soit $k \geq 2$ et $\{a_1, \ldots, a_k\}$ deux à deux disjoints.*

- *On a $(a_1 \ldots a_k)^{-1} = (a_k\, a_{k-1} \ldots a_2\, a_1)$.*
- *Pour tout $i \in \mathbb{Z}$ et tout $j \in \{1, \ldots, n\}$, on a*

$$(a_1 \ldots a_k)^i \cdot (j) = \begin{cases} j & \text{si } j \notin \{a_1, \ldots, a_k\} \\ = a_{\ell+i} & \text{si } j = a_\ell \end{cases}$$

Dans cette deuxième écriture, on regarde bien sûr les indices s de a_s modulo k.

Démonstration. Par définition le k-cycle $(a_k\, a_{k-1} \ldots a_2\, a_1)$ agit trivialement sur tout élément $i \notin \{a_1, \ldots, a_k\}$ tout comme $(a_1 \ldots a_k)$. De plus il envoie a_j sur a_{j-1}. Or $(a_1 \ldots a_k)$ est définit par le fait que

$$(a_1 \ldots a_k) \cdot (a_i) = a_{i+1} \iff a_i = (a_1 \ldots a_k)^{-1} \cdot (a_{i+1}$$

par simplification. Il suit que $(a_k\, a_{k-1} \ldots a_2\, a_1)$ est bien l'inverse de $(a_1 \ldots a_k)$.

Passons à la deuxième affirmation. Tout d'abord par la remarque 4.28, on a que si $j \notin \{a_1, \ldots, a_k\}$, alors j n'est pas dans le support de $(a_1 \ldots a_k)^i$ et donc est laissé fixe par cette permutation. Il reste à voir le cas où $j = a_\ell$. Alors, par définition du k-cycle $(a_1 \ldots a_k)$, on a que $(a_1 \ldots a_k) \cdot (a_\ell) = a_{\ell+1}$. D'où en itérant i fois ce calcul,

$$\begin{aligned}(a_1 \ldots a_k)^i \cdot (a_\ell) &= (a_1 \ldots a_k)^{i-1}\big((a_1 \ldots a_k) \cdot (a_\ell)\big) \\ &= (a_1 \ldots a_k)^{i-1} \cdot (a_{\ell+1}) = (a_1 \ldots a_k)^{i-2} \cdot (a_{\ell+2}) = \cdots = a_{\ell+i}\end{aligned}$$

ce qui conclut. □

Notons qu'une preuve "graphique"découle facilement de l'étude de la figure (2) où l'inverse signifie tourner dans l'autre sens.

Remarque 4.38. En particulier, l'inverse d'un k-cycle est un k-cycle. Attention, une puissance d'un k-cycle n'est pas forcément un k-cycle. Par exemple $(1\,2\,3\,4)^2 = (1\,3) \circ (2\,4)$ est un produit de deux transpositions mais n'est pas un 4-cycle.

On en déduit facilement l'ordre d'un k-cycle.

Lemme 4.39. *Si σ est un k-cycle, alors* $\mathrm{ord}(\sigma) = k$.

Démonstration. Tout d'abord par le deuxième point du lemme 4.37, on a que

$$(a_1 \ \dots \ a_k)^k \cdot (a_\ell) = a_{\ell+k} = a_\ell$$

puisque les indices ℓ des a_ℓ sont regardés modulo k. Comme cette permutation envoie aussi $j \notin \{a_1, \dots, a_k\}$ sur j, on en déduit que $(a_1 \ \dots \ a_k)^k = \mathrm{id}$. Il reste à vérifier que pour $0 < i < k$, $(a_1 \ \dots \ a_k)^i \neq \mathrm{id}$. Mais là encore le lemme 4.37 permet de conclure puisque $(a_1 \ \dots \ a_k)^i \cdot (a_1) = a_{i+1} \neq a_1$ (car $1 < i+1 < k+1$). Donc k est bien le plus petit entier m strictement positif tel que $(a_1 \ \dots \ a_k)^m = \mathrm{id}$ et la proposition 3.53 permet de conclure. □

Remarque 4.40. Les deux lemmes précédents nous disent que si σ est un k-cycle, alors on peut réécrire *tous* les a_i et σ à partir de n'importe quel élément a_j par itération. Plus précisément, on a la formule suivante.

Proposition 4.41. *Si σ est un k-cycle, alors, pour tout $x \in \mathrm{Supp}(\sigma)$, on a*

$$\sigma = \big(x \, \sigma(x) \, \sigma^2(x) \ \dots \ \sigma^{k-1}(x)\big).$$

La formule permet de voir un cycle comme une succession de puissance d'un élément non-fixe quelconque.

Démonstration. Soit $\sigma = (a_1 \ \dots \ a_k)$. On a $\mathrm{Supp}(\sigma) = \{a_1, \dots, a_k\}$ (voir les propriétés 4.31). Or pour tout a_i et j, on a $\sigma^j(a_i) = a_{i+j}$ par le lemme 4.37. Il suit que

$$\big(a_i \, \sigma(a_i) \, \sigma^2(a_i) \ \dots \ \sigma^{k-1}(a_i)\big) = \big(a_i \, a_{i+1} \ \dots \ a_{i-1}\big) = (a_1 \ \dots \ a_k) = \sigma.$$

□

Nous allons maintenant voir que nous pouvons décomposer de manière (essentiellement) unique une permutation en *cycles* à support *disjoints*.

Remarque 4.42. Si $\sigma = \tau_1 \dots \tau_k$ avec les τ_i des cycles à supports disjoints, alors la proposition 4.27 nous donne immédiatement que pour tout $n \in \mathbb{Z}$,

$$\sigma^n = \tau_1^n \cdots \tau_k^n. \tag{7}$$

Et par ailleurs, on a que $\mathrm{Supp}(\sigma) = \bigcup_{i=1}^{k} \mathrm{Supp}(\tau_i)$ (par le lemme 4.26).

Le théorème suivant est le résultat le plus important de cette partie.

Théorème 4.43 (Théorème de décomposition des permutations)**.** *Soit $\sigma \in S_n$ une permutation différente de l'identité.*

- *Il existe une famille $\sigma_1, \dots, \sigma_k$ de* cycles *à supports* 2 à 2 disjoints *telle que*

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_k. \tag{8}$$

- *De plus la famille est* unique *à permutation des σ_j dans l'écriture* (8) *près. Plus précisément, si $\sigma = \tau_1 \circ \cdots \circ \tau_\ell$ est une autre décomposition en produit de cycles à supports disjoints alors $k = \ell$ et pour tout $i \in \{1, \dots, k\}$ il existe un* unique *$j \in \{1, \dots, \ell\}$ tel que $\sigma_i = \tau_j$.*

L'unicité se retraduit simplement par le fait que la famille $\{\sigma_1, \dots, \sigma_k\}$ dans l'écriture (8) *est unique mais que l'on peut bien sûr écrire le produit de ces éléments dans l'ordre que l'on veut*, puisqu'ils commutent tous (ce qui découle du fait que leurs supports sont disjoints). Notons aussi que les σ_j sont 2 à 2 distincts puisque leurs supports le sont.

Remarque 4.44. On peut réécrire simplement la propriété "$k = \ell$ et pour tout $i \in \{1, \dots, k\}$ il existe un *unique* $j \in \{1, \dots, \ell\}$ tel que $\sigma_i = \tau_j$" par il existe une bijection $\alpha : \{1, \dots, k\} \to \{1, \dots, \ell\}$ telle que, pour tout i, on a $\sigma_i = \tau_{\alpha(i)}$.

Remarque 4.45 (Calcul en utilisant la décomposition). Par le lemme 4.24, on a que, pour toute décomposition $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$ en cycles à support disjoints, on a $\mathrm{Supp}(\sigma)$ est la réunion (disjointe) des $\mathrm{Supp}(\sigma_i)$.

Par ailleurs, si $x \in \mathrm{Supp}(\sigma_i)$, alors $\sigma_i(x)$ est aussi dans le support de σ_i (par le lemme 4.24). Par conséquent, ni x ni $\sigma_i(x)$ ne sont dans le support des autres σ_j ($j \neq k$). Il suit que $\sigma_j(x) = x$ et $\sigma_j(\sigma_i(x)) = \sigma_i(x)$ pour $j \neq i$. Ainsi en appliquant l'identité (8), on obtient

$$\forall x \in \mathrm{Supp}(\sigma_i), \qquad \sigma(x) = \sigma_i(x). \tag{9}$$

Remarque 4.46. L'unicité est complétement fausse si on ne suppose pas à supports disjoints. par exemple $(1\,2) = (1\,2)(1\,2)(1\,2)$ et $(1\,2\,3) = (1\,2)(2,3)$.

Démonstration du théorème 4.43. La preuve ci-dessous est technique. Ce qu'il convient de faire est de comprendre le principe. Nous verrons qu'en pratique cette décomposition est facile à trouver et c'est ça qui sera important. L'idée est de construire les cycles σ_i un par un. Ils ne font évidemment intervenir que le support de σ par la remarque précédente.
Idée clé : on part d'un point $x \in \mathrm{Supp}(\sigma)$ et on suit les itérés de x par σ, c'est à dire $\sigma(x)$,...$\sigma^k(x)$.. jusqu'à ce que l'on retombe sur x. Cela va nous donner un cycle $(x\,\sigma(x) \cdots \sigma^{d-1}(x))$ qui sera un des cycles σ_i. L'idée est directement tirée de la proposition 4.41. On passe ensuite à un élément du support pas atteint par ce cycle et on continue.

Vérifions que cela marche en détail (ça va donc être un peu technique, mais c'est vraiment l'idée précédente que l'on va réaliser).
Étape 1. Prenons $x_1 \in \mathrm{Supp}(\sigma)$ (par exemple le plus petit élément du support, mais ce n'est pas nécessaire ; n'importe lequel marche ; un tel x_1 existe car $\sigma \neq \mathrm{id}$). Montrons qu'il existe un entier $m > 0$ tel que $\sigma^m(x_1) = x_1$. On utilise le lemme des tiroirs : la famille $\{\sigma^i(x_1), i \in \mathbb{N}\}$ est finie puisque incluse dans $\{1, \dots, n\}$. Or il y a une infinité d'indices, il y a donc deux valeurs $i < j$ telles que $\sigma^i(x_1) = \sigma^j(x_1)$. On en déduit par simplification (lemme 3.11) que $\sigma^{j-i}(x_1) = x_1$ avec $j - i > 0$. On peut donc trouver d_1 le plus petit entier $m > 0$ satisfaisant $\sigma^m(x_1) = x_1$.
Étape 1bis. On regarde la famille $\{x_1, \sigma(x_1), \dots \sigma^{d_1-1}(x_1)\}$. Tous ces éléments sont 2 à 2 disjoints. En effet, si il existait $0 \leq p < q \leq d_1 - 1$ tels que $\sigma^p(x_1 = \sigma^q(x_1)$ alors on aurait par simplification $\sigma^{q-p}(x_1) = x_1$ ce qui contredirait la minimalité de d_1 car $0 < q - p < d_1$. On peut donc poser $\sigma_1 = \big(x_1\,\sigma(x_1)\,\dots\,\sigma^{d_1-1}(x_1)\big)$ qui est un d_1-cycle. (*Aparté :* si le lecteur voit une ressemblance entre ce début de preuve et celle de la proposition 3.53, ce n'est pas un hasard du tout. On a construit une sous-famille d'ordre d_1 à partir de σ et d'un élément du support en regardant les puissance comme quand on prend un élément d'ordre d_1 dans un groupe.).

Par construction de ce d_1-cycle, $\mathrm{Supp}(\sigma_1) = \{x_1, \dots, \sigma^{d_1-1}(x_1)\}$. On a de plus la formule

$$\forall y \in \mathrm{Supp}(\sigma_1), \qquad \sigma(y) = \sigma_1(y). \tag{10}$$

Cette formule est immédiate puisque un tel y s'écrit $\sigma^i(x_1)$ et donc $\sigma(y) = \sigma^{i+1}(y) = \sigma_1(y)$ puisque $\sigma_1 = \big(x_1\,\sigma(x_1)\,\dots\,\sigma^{d_1-1}(x_1)\big)$.
Notons deux choses :

- $\mathrm{Supp}(\sigma_1) \subset \mathrm{Supp}(\sigma)$puisque par construction $\sigma(y) \neq y$ si $y \in \mathrm{Supp}(\sigma_1)$ (c'est précisément le résultat du début de l'étape 1bis).
- $\mathrm{Supp}(\sigma) \backslash \mathrm{Supp}(\sigma_1)$ est de cardinal *strictement* plus petit que $\mathrm{Supp}(\sigma)$ car $\mathrm{Supp}(\sigma_1) \neq \emptyset$.

On va maintenant itérer cette procédure.
Étape 2. On prend $x_2 \in \mathrm{Supp}(\sigma) \setminus \mathrm{Supp}(\sigma_1)$. Et on réitère la construction de l'étape 1. On obtient $d_2 > 0$ minimal tel que $\sigma^{d_2}(x_2) = x_2$.
Étape 2bis. La famille $\{x_2, \sigma(x_2), \dots \sigma^{d_2-1}(x_2)\}$ est constituée d'éléments sont 2 à 2 disjoints par le même argument que l'étape 1bis. Ils ne sont pas non-plus dans $\mathrm{Supp}(x_1)$. Démontrons ce point : si il existait $\sigma^j(x_2) = \sigma^i(x_1)$, alors, en composant par σ^{d_2-j}, on obtiendrait $x_2 = \sigma^{d_2}(x_2) = \sigma^{d_2-j+i}(x_1) \in \mathrm{Supp}(\sigma_1)$.

On peut donc poser $\sigma_2 = \big(x_2\, \sigma(x_2) \dots \sigma^{d_2-1}(x_2)\big)$ qui est un d_2-cycle à support disjoint de σ_1. On a de plus (comme dans le cas 1bis) la formule

$$\forall y \in \mathrm{Supp}(\sigma_2), \qquad \sigma(y) = \sigma_2(y). \tag{11}$$

Notons deux choses :

- $\mathrm{Supp}(\sigma_2) \subset \mathrm{Supp}(\sigma)$puisque par construction $\sigma(y) \neq y$ si $y \in \mathrm{Supp}(\sigma_1)$ (c'est précisément le résultat du début de l'étape 1bis.
- $\mathrm{Supp}(\sigma) \setminus (\mathrm{Supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2)$ est de cardinal *strictement* plus petit que $\mathrm{Supp}(\sigma) \setminus \mathrm{Supp}(\sigma_1)$ car $\mathrm{Supp}(\sigma_2) \neq \emptyset$.

On peut continuer cette opération en faisant une étape 3 et 3bis et ainsi de suite tant qu'il reste des éléments dans $\mathrm{Supp}(\sigma) \setminus \big(\mathrm{Supp}(\sigma_1) \cup \dots \cup \mathrm{Supp}(\sigma_i)\big)$ (après i étapes). Comme on réduit strictement la taille du cardinal de $\mathrm{Supp}(\sigma) \setminus \big(\mathrm{Supp}(\sigma_1) \cup \dots \cup \mathrm{Supp}(\sigma_i)\big)$ à chaque étape, au bout d'un moment il n'y a plus d'éléments disponibles et les étapes s'arrêtent. Et à chaque étape j, on a

$$\forall y \in \mathrm{Supp}(\sigma_j), \qquad \sigma(y) = \sigma_j(y). \tag{12}$$

Fin de la preuve de l'existence : Soit k la dernière étape dans le procédé précédent. On a que les σ_i sont à supports deux à deux disjoints et que la réunion de leur support est égal au support de σ. Démontrons que

$$\sigma = \sigma_1 \circ \dots \circ \sigma_k$$

. Il suffit de vérifier qu'ils prennent les mêmes valeurs pour tout $i \in \{1, \dots, n\}$.

- Si $i \notin \mathrm{Supp}(\sigma)$, alors il n'est dans le support d'aucun σ_j et donc pour tout j, $\sigma_j(i) = i$ d'où $\sigma_1 \circ \dots \circ \sigma_k(i) = i = \sigma(i)$.
- Si $i \in_{\mathrm{Supp}} (\sigma)$, il existe un unique j tel que $i \in \mathrm{Supp}(\sigma_j)$. On a de plus par l'équation (12) que $\sigma(i) = \sigma_j(i)$. Comme i et donc $\sigma_j(i) = \sigma(i)$ (lemme 4.24) sont dans le support de σ_j, on obtient que pour tout $p \neq j$, $\sigma_p(i) = i$ et $\sigma_p(\sigma(i)) = \sigma(i)$. Il suit encore que

$$\sigma_1 \circ \dots \circ \sigma_k(i) = \sigma_1 \circ \dots \sigma_j(i) = \sigma_j(i) = \sigma(i).$$

Finalement on a bien montré que pour tout $i \in \{1, \dots, n\}$, on a $\sigma(i) = \sigma_1 \circ \dots \circ \sigma_k(i)$ et donc $\sigma = \sigma_1 \circ \dots \circ \sigma_k$. Ouf !

Preuve de l'unicité de la décomposition. La preuve de l'unicité va être plus facile car on a déjà essentiellement fait le travail. En effet, par l'équation (9) (dans la remarque 4.45), nous avons que pour tout $x \in \mathrm{Supp}(\sigma_i)$, on a $\sigma_i(x) = \sigma(x)$. Or le cycle σ_i s'écrit juste $(x\, \sigma_i(x) \cdots \sigma_i^{d_x-1}(x))$ par la proposition 4.41, avec d_x est l'ordre de σ_i. Comme nous l'avons vu, cet ordre est par définition le plus petit entier $d > 0$ tel que $\sigma^d(x) = x$. Enfin le support de σ_i est donc $\{x, \sigma(x), \cdots, \sigma^{d_x-1}(x)\}$ d'après l'écriture du cycle. Finalement, en se rappelant que $\sigma_i^k(x) = \sigma^k(x)$, on vient donc de montrer que $\sigma_i = (x\, \sigma(x) \cdots \sigma^{d_x-1}(x))$.

La même chose est vraie pour la décomposition $\sigma = \tau_1 \circ \dots \circ \tau_\ell$: le cycle $\tau_j = (y\, \sigma(y) \dots \sigma^{d_y-1}(y))$ pour tout $y \in \mathrm{Supp}(\tau_j)$, où d_y est l'ordre de τ_j, et c'est par définition le plus petit entier $d > 0$ tel que $\sigma^d(y) = y$. Enfin le support de τ_j est donc $\{y, \sigma(y), \cdots, \sigma^{d_y-1}(y)\}$ d'après l'écriture du cycle.

En d'autres termes, les cycles σ_i, τ_j sont *complètement* déterminés par σ. En effet, soit maintenant $x \in \mathrm{Supp}(\sigma)$, alors il est dans le support d'un **unique** σ_i et d'un **unique** τ_j. On obtient de l'analyse que l'on vient de faire, en notant $d_x > 0$ le plus petit entier $d > 0$ tel que $\sigma^d(x) = x$ que

$$\sigma_i = (x\, \sigma(x) \cdots \sigma^{d_x-1}(x)) = \tau_j$$

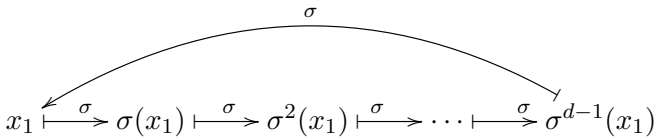
Par conséquent pour chaque élément du support on détermine exactement un des cycles de la famille des σ_i et un de la famille des τ_j qui sont égaux (et donc ont le même support et la même contribution au support de σ). En faisant ça pour tous les éléments du support de σ on établit exactement l'unicité demandée ! □

Remarque 4.47. On peut voir l'identité comme une permutation dont la décomposition en cycles est vide.

Si σ est un cycle, alors sa décomposition est elle même bien sûr. Et c'est la seule possible par unicité.

Algorithme pour décomposer en cycles à supports disjoints : l'algorithme reprend l'idée de la preuve. Il est facile à faire (la difficulté dans la preuve consiste à vérifier et expliquer pourquoi il marche à tous les coups et qu'il y a unicité).

- On regarde les $\sigma(x)$ et on prend le premier élément x_1 que l'on trouve tel que $\sigma(x_1) \neq x_1$ (c'est à dire qui soit dans le support de σ). On écrit alors le cycle $\sigma_1 = (x_1\, \sigma(x_1) \cdots \sigma^{d-1}(x_1))$ obtenu en suivant les images successives des éléments par x jusqu'à ce que l'on retombe sur x_1 :



  On peut "barrer" les éléments utilisés dans σ pour éviter de les réutiliser.
- S'il n'y a plus d'éléments dans le support de σ qui ne soit pas dans celui de σ_1, on s'arrête là. Sinon, on prend un x_2 dans le support de σ qui n'est pas dans celui de x_1 et on refait l'opération ci-dessus pur avoir $\sigma_2 = (x_2\, \sigma(x_2) \cdots \sigma^{d_2-1}(x_2))$. Si tous les éléments du support de σ sont dans ceux de σ_1 et σ_2, on s'arrête là et $\sigma = \sigma_1 \circ \sigma_2$. Sinon on continue en prenant $x_3 \in \mathrm{Supp}(\sigma) \setminus \big(\mathrm{Supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2)\big)$ et on réitère l'opération jusqu'à ce qu'on ne puisse plus.

En pratique cet algorithme est efficace. On verra des exemples en TDs, CCs et DMs.

Exemple 4.48. On va appliquer l'algorithme de décomposition en cycles à supports disjoints à la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 3 & 5 & 7 & 10 & 11 & 8 & 1 & 6 & 4 & 16 & 13 & 12 & 17 & 2 & 15 & 9 & 14 \end{pmatrix}.$$

On l'a représenté également dans la figure (3). On a que $\sigma(1) \neq 1$ donc on construit le premier cycle σ_1 en regardant les images successives de 1 :

$$1 \longmapsto 3 \longmapsto 7\,, \qquad \text{cela nous donne } \sigma_1 = (1\,3\,7).$$

Le prochain élément est 2 et $\sigma(2) \neq 2$, donc on construit un cycle partant de 2 en regardant ses images successives :

$$2 \longmapsto 5 \longmapsto 11 \longmapsto 13 \longmapsto 17 \longmapsto 14\,, \quad \text{cela donne } \sigma_2 = (2\ 5\ 11\ 13\ 17\ 14).$$

L'élément 3 est déjà apparu dans un cycle, donc on ne le regarde pas. Et on passe donc à 4 qui n'a pas encore été utilise et s'envoie sur $10 \neq 4$. On trouve

$$4 \longmapsto 10 \longmapsto 16 \longmapsto 9\,, \quad \text{cela donne } \sigma_3 = (4\ 10\ 16\ 9).$$

Description graphique de l'algorithme de décomposition en cycles à supports disjoints pour

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 3 & 5 & 7 & 10 & 11 & 8 & 1 & 6 & 4 & 16 & 13 & 12 & 17 & 2 & 15 & 9 & 14 \end{pmatrix}.$$

On a que $\sigma(1) \neq 1$ donc on construit le premier cycle σ_1 en regardant les images successives de 1:

$$1 \longmapsto 3 \longmapsto 7\,, \qquad \text{cela nous donne } \sigma_1 = (1\,3\,7).$$

Dans le dessin ci-dessous on a barré en rouge tous les éléments de ce cycle. On fait de même en partant de 2 pour trouver le cycle (dont les éléments sont rayés en jaune).

$$2 \longmapsto 5 \longmapsto 11 \longmapsto 13 \longmapsto 17 \longmapsto 14\,, \quad \text{cela donne } \sigma_2 = (2\,5\,11\,13\,17\,14).$$

On fait de même pour trouver les cycles bleus et vert:

$$4 \longmapsto 10 \longmapsto 16 \longmapsto 9 \qquad 6 \longmapsto 8$$

.

$$\begin{pmatrix} \cancel{1} & \cancel{2} & \cancel{3} & \cancel{4} & \cancel{5} & \cancel{6} & \cancel{7} & \cancel{8} & \cancel{9} & \cancel{10} & \cancel{11} & 12 & \cancel{13} & \cancel{14} & 15 & \cancel{16} & \cancel{17} \\ \cancel{3} & \cancel{5} & \cancel{7} & \cancel{10} & \cancel{11} & \cancel{8} & \cancel{1} & \cancel{6} & \cancel{4} & \cancel{16} & \cancel{13} & 12 & \cancel{17} & \cancel{2} & 15 & \cancel{9} & \cancel{14} \end{pmatrix}.$$

FIGURE 3. Un exemple de décomposition en cycles

L'élément 5 est déjà apparu avant donc on ne le regarde pas. On passe à $6 \longmapsto 8$ qui nous donne la transposition $\sigma_4 = (6\,8)$.

Les éléments suivants sont déjà tous apparus jusqu'à 12. Mais 12 s'envoie sur lui même donc ne donne pas de cycle (il n'est pas dans le support). On voit que tous les autres éléments ont déjà été utilisés, à l'exception de 15 qui n'est pas non plus dans le support. On conclut :

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 = (1\,3\,7)\,(2\,5\,11\,13\,17\,14)\,(4\,10\,16\,9)\,(6\,8)$$

La décomposition en éléments simples est utile pour comprendre les différents types de permutation possibles dans S_n et comment elles interagissent.

Par exemple

- Une permutation $\sigma \in S_n$ ne peut contenir qu'au plus un cycle de longueur n. Auquel cas elle est égale à ce cycle de longueur n. Il existe $(n-1)!$ tels cycles.
- Une permutation $\sigma \in S_n$ ne peut contenir qu'au plus un cycle de longueur $n-1$. Auquel cas elle est égale à ce cycle de longueur $n-1$. En effet le théorème de décomposition ne laisse pas la place pour avoir un autre élément dans la décomposition.
- Une permutation $\sigma \in S_n$ est un produit d'au plus $\lfloor n/2 \rfloor$ transpositions à supports disjoints.

Exercice 4.49. Démontrer ces propriétés.

Exemple 4.50 (Étude de S_4 via les décompositions possibles). On va lister les éléments de S_4 en fonction de leur décompositions possibles. Notons que, pour une permutation de S_4, les décompositions en cycles à supports *disjoints* possibles sont

- σ *est un* 4*-cycle :* il y a 6 possibilités (on les obtient en commençant par 1, puis en regardant les 3! autres possibilités pour choisir les éléments restants. Voir le TD pour les détails) : $(1\,2\,3\,4)$, $(1\,2\,4\,3)$, $(1\,3\,2\,4)$, $(1\,3\,4\,2)$, $(1\,4\,2\,3)$, $(1\,4\,3\,2)$.
- σ *est un 3 cycle :* il y a $4 \times 2 = 8$ possibilités : 4 choix pour l'élément qui n'est pas dans le support puis une fois cet élément choisi 2 choix possibles de 3-cycle correspondant aux 3 éléments restants. Précisément on obtient $(1\,2\,3)$, $(1\,3\,2)$, $(1\,2\,4)$, $(1\,4\,2)$, $(1\,3\,4)$, $(1\,4\,3)$, $(2\,3\,4)$, $(2\,4\,3)$.
- σ *est un produit de deux transpositions à supports disjoints :* On a 3 choix possible : 1 doit être dans une transposition associée à 2, 3, ou 4 et dans ce cas l'autre transposition du produit est imposée. On a donc $(1\,2)(3\,4)$,$(1\,3)(2\,4)$ et $(1\,4)(2\,3)$.
- σ *peut être une transposition :* on a $\binom{4}{2} = 6$ choix possibles. $(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$.
- σ *peut être l'identité.*

Au total on retrouve bien les $4! = 24$ permutations possibles. L'unicité dans le théorème de décomposition assure que toutes ces décompositions donnent des permutations différentes.

Une propriété intéressante de la décomposition en cycles à supports disjoints et que sa nature (le nombre et la longueur des cycles intervenant) est stable par conjugaison.

Lemme 4.51. *Soit $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$ une décomposition en cycles à supports disjoints. Alors pour tout $\tau \in S_n$, la décomposition en cycles à supports disjoints de $\tau \circ \sigma\tau^{-1} = \circ \cdots \circ \left(\tau \circ \sigma_k \circ \tau^{-1}\right)$ où les $\left(\tau \circ \sigma_1 \circ \tau^{-1}\right)$ sont des cycles à supports disjoints de même ordre que σ_k.*

Démonstration. Sera vue en TD. □

Remarque 4.52 (Calcul de l'ordre via la décomposition en cycles à supports disjoints). La commutativité des cycles à supports disjoints rend facile le calcule de l'ordre d'une permutation. En effet, on a par la formule que (7)

$$(\sigma_1 \cdots \sigma_k)^n = \sigma_1^n \circ \cdots \circ \sigma_k^n$$

Par exemple si on cherche l'ordre de $\sigma = (1\,3\,5)\,(2\,4)$, on a

$$\big((1\,3\,5)\,(2\,4)\big)^n = (1\,3\,5)^n\,(2\,4)^n = (1\,3\,5)^{r_3(n)}\,(2\,4)^{r_2(n)}$$

où $r_i(n)$ est le reste de n dans la division euclidienne par i (car le premier cycle est d'ordre 3 et le second d'ordre 2). Les $(1\,3\,5)^{r_3(n)}$ et $(2\,4)^{r_2(n)}$ sont à supports distincts (puisque les permutations de départ l'étaient). Donc cette permutation est triviale si $(1\,3\,5)^{r_3(n)} = \mathrm{id}$ et $(2\,4)^{r_2(n)} = \mathrm{id}$ (par unicité dans le théorème de décomposition 4.43). Ainsi pour que $\sigma^n = \mathrm{id}$, il faut que $r_2(n) = 0$, c'est à dire n pair et $r_3(n) = 0$, c'est à dire n divisible par 3. Par conséquent, l'ordre de σ est le ppcm de 3 et 2, c'est donc 6. Nous verrons de nombreux exemples de ce genre en TD et DM.

Remarque 4.53 (**Familles génératrices de S_n**). Le théorème de décomposition 4.43 implique que toute permutation est un produit de cycles. Donc les cycles sont une famille de générateurs de S_n. On peut trouver des familles plus petites. Par exemple, les transpositions suffisent en raison du lemme suivant.

Proposition 4.54. *Soit $(a_1 \ldots a_k)$ un k-cycle de S_n. Alors on a l'égalité :*

$$(a_1 \ldots a_k) = (a_1\,a_2)(a_2\,a_3)\cdots(a_{k-1}\,a_k).$$

En particulier, les transpositions engendrent S_n : $S_n := \langle (i\,j),\, i \neq j \rangle$.

Attention le terme de droite n'est pas une décomposition en cycles à support disjoints (ce ne serait pas possible par unicité de toutes façons). Les transpositions en question ont des supports en commun.

Démonstration. Il faut vérifier que, pour tout $x \in \{1, \dots, n\}$, on a $(a_1 \dots a_k) \cdot x$ et $(a_1\, a_2)(a_2\, a_3) \cdots (a_{k-1}\, a_k) \cdot x$ (où on note $\sigma \cdot x = \sigma(x)$ l'évaluation de la permutation en x qui n'est rien d'autres que l'action canonique. On choisit cette notation pour éviter de confondre (x) avec un cycle). Si $x \notin \{a_1, \dots, a_k\}$ alors x n'est dans le support d'aucune des permutations en jeu et on a donc

$$(a_1 \dots a_k) \cdot x = x = (a_1\, a_2)(a_2\, a_3) \cdots (a_{k-1}\, a_k) \cdot x.$$

Si $x = a_i$, alors, d'une part $(a_1 \dots a_k) \cdot a_i = a_{i+1}$. D'autre part, pour $j > i$, on a que $(a_j\, a_{j+1}) \cdot a_i = a_i$. Il suit que

$$\begin{aligned}(a_1\, a_2)(a_2\, a_3) \cdots (a_{k-1}\, a_k) \cdot a_i & \\ &= (a_1\, a_2)(a_2\, a_3) \cdots (a_{k-2}\, a_{k-1}) \cdot a_i \\ &= (a_1\, a_2)(a_2\, a_3) \cdots (a_i\, a_{i+1}) \cdot a_i \\ &= (a_1\, a_2)(a_2\, a_3) \cdots (a_{i-1}\, a_i) \cdot a_{i+1} \text{ (car } (a_i\, a_{i+1}) \cdot a_i = a_{i+1}) \\ &= a_{i+1}.\end{aligned}$$

Ceci marche pour tous les a_j sauf a_k (car il n'y a pas de tels j). Pour a_k, on calcule

$$\begin{aligned}(a_1\, a_2)(a_2\, a_3) \cdots (a_{k-1}\, a_k) \cdot a_k & \\ &= (a_1\, a_2)(a_2\, a_3) \cdots (a_{k-2}\, a_{k-1}) \cdot a_k \\ &= \cdots = (a_1\, a_2) \cdot a_2 = a_1.\end{aligned}$$

Par suite, ces deux permutations prennent bien les mêmes valeurs et sont donc égales.

Le théorème de décomposition implique que toute permutation est un produit de cycles. Or ce que nous venons de démontrer est que tout cycle est un produit de transpositions. Par suite, toute permutation est un produit de transposition. Ce qui montre que $G \subset \langle (i\, j),\, i \neq j \rangle$ et donc (l'autre inclusion étant par définition) que $G = \langle (i\, j),\, i \neq j \rangle$. □

Exemple 4.55. On verra en TD que S_n peut aussi être engendré par une transposition et un n-cycle : $S_n = \langle (1\, 2), (1\, 2 \cdots n) \rangle$.

4.4. **Signature d'une permutation.** La signature est un invariant important des permutations, qui intervient notamment dans la définition du déterminant en algèbre linéaire.

Rappelons que la proposition 4.54 implique que ***toute permutation est un produit de transpositions*** (mais pas forcément à supports disjoints).

Proposition et Définition 4.56. *Soit $\sigma = s_1 \cdots s_k$ une décomposition de σ en produits de* transpositions*. Alors, le nombre $(-1)^k$ est* indépendant *de la décomposition et est appelé* **la signature de** *σ. Il sera noté* $\operatorname{sgn}(\sigma)$ *ou* $(-1)^\sigma$*.*

Autrement dit $\operatorname{sgn}(\sigma) = (-1)^k$ pour *toute* écriture de σ comme un produit de transpositions avec k-transpositions.

Avant de démontrer la proposition, nous allons nous intéresser à des conséquences.

Corollaire 4.57. *La signature vérifie les propriétés suivantes :*

- $\operatorname{sgn}(id) = 1$
- *Pour toute transposition τ, on a* $\operatorname{sgn}(\tau) = -1$.
- *Pour tout k-cycle $(a_1 \cdots a_k)$, on a* $\operatorname{sgn}\big((a_1 \cdots a_k)\big) = (-1)^{k-1}$
- *pour tout σ, $\tau \in S_n$, on a* $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau)$*. Autrement dit :*

  La signature est un morphisme de groupes $(S_n, \circ) \longrightarrow (\{1, -1\}, \times)$

Démonstration. Tout d'abord, une permutation est le produit d'une permutation (c'est à dire elle même) ce qui donne le deuxième point. Pour l'identité, on remarque que $\mathrm{id} = \tau \circ \tau$ pour toute transposition τ (car $\tau^{-1} = \tau$), ce qui donne $\operatorname{sgn}(\mathrm{id}) = (-1)^2 = 1$ (on peut aussi appliquer le résultat au produit vide).

Pour le troisième point, on applique la proposition 4.54 qui nous dit qu'un k-cycle est un produit de $(k-1)$-transpositions.

Enfin, si $\sigma = s_1 \cdots s_k$ et $\tau = r_1 \cdots r_\ell$ avec s_i, r_j des transpositions, alors

$$\sigma \circ \tau = s_1 \cdots s_k \, r_1 \cdots r_\ell$$

est une écriture du produit en $k+\ell$ transpositions. D'où

$$\operatorname{sgn}(\sigma \circ \tau) = (-1)^{k+\ell} = (-1)^k \, (-1)^\ell = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau).$$

Cette dernière propriété traduit exactement que sgn est un morphisme de groupes. □

Pour démontrer la proposition (et définition) 4.56, on va introduire une autre façon de compter ce nombre (qui sera indépendante de la décomposition).

Définition 4.58. Une **inversion d'une permutation** $\sigma \in S_n$ est une paire $\{i, j\}$ avec $i \neq j \in \{1, \dots n\}$ telle que $(i-j)(\sigma(i) - \sigma(j)) < 0$.

On notera $I(\sigma)$ le nombre d'inversions d'une permutation σ. Autrement dit le nombre de paires $\{i, j\}$ qui sont des inversions.

Autrement dit, une inversion de σ est une paire telle que σ inverse l'ordre de i et j (pour la relation d'ordre $\leq$ standard sur les entiers).

Remarque 4.59. De manière équivalente, une inversion de σ est une paire (k, ℓ) avec $1 \leq k < \ell \leq n$ telle que $\sigma(k) > \sigma(\ell)$. Pour voir l'équivalence entre les deux notions, il suffit d'associer à toute paire $\{i, j\}$ le couple $\big(\min(i, j), \max(i, j)\big)$.

Terminologie 4.60. On dira souvent que σ *inverse l'ordre* de $\{i, j\}$ si $\{i, j\}$ est une inversion et *préserve l'ordre* de $\{i, j\}$ sinon.

Exemple 4.61. Regardons la transposition $(1\,2)$ dans S_n avec $n \geq 2$. Alors $(1\,2)$ inverse la paire $\{1, 2\}$ et aucune autre paire (car $(1\,2)$ envoie tout $i \geq 3$ sur lui même). Donc $I\big((1\,2)\big) = 1$.

De manière générale pour chercher les inversions de σ on regarde toutes les paires $\{1, i\}$ et on a une inversion pour chaque i tel que $\sigma(i) < \sigma(1)$ (il y en a donc $\sigma(1) - 1$) ; cela règle elc as de toutes les paries contenant 1. Puis on regarde toutes les paires $\{2, j\}$ avec $j > 2$; et cette paire est un inversion si et seulement si $\sigma(j) < \sigma(2)$. Et ainsi de suite !

Exemple 4.62. Pour le cycle $(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, nous avons une inversion contenant 1 (la paire $\{1, 3\}$, et une autre inversion contenant 2 ($\{2, 3\}$). Donc $I\big((1\,2\,3)\big) = 2$.

Exemple 4.63. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Comme $\sigma(1) = 4$, toutes les paires contenant 1 sont des inversions. On en a donc 3 contenant 1. Une paire $\{2, j\}$ avec $j > 2$ est une inversion si et seulement si $\sigma(j) < \sigma(2) = 3$. On voit que les deux paires $\{2, 3\}$ et $\{2, 4\}$ en sont. On a donc 2 telles inversions. Il reste à regarder la paire $\{3, 4\}$. C'est aussi une inversion car $\sigma(3) = 2 > \sigma(4) = 1$. Au total on a donc $I(\sigma) = 3 + 2 + 1 = 6$. On remarque que dans cet exemple, toutes les paires sont des inversions.

Le lemme clé pour démontrer 4.56 est le suivant

Lemme 4.64. *Soient σ, τ deux permutations de S_n. Alors on a que*

$$I(\sigma \circ \tau) - I(\sigma) - I(\tau) \text{ est pair.}$$

En particulier

$$(-1)^{I(\sigma\circ\tau)} = (-1)^{I(\sigma)}(-1)^{I(\tau)}. \tag{13}$$

Démonstration. Soit (i,j) avec $i<j$ un couple. Alors, par définition, $\{i,j\}$ est une inversion pour $\sigma\circ\tau$ si $\sigma(\tau(i))>\sigma(\tau(j))$ ce qui est équivalent à l'une des deux conditions suivantes :

- τ préserve l'ordre de $\{i,j\}$ **et** σ inverse l'ordre de $\{\tau(i),\tau(j)\}$ (cf terminologie 4.60) ;
- τ inverse l'ordre de $\{i,j\}$ et σ préserve l'ordre de $\{\tau(i),\tau(j)\}$.

Notons que ces deux conditions sont disjointes (et que par injectivité de τ, on a bien que $\tau(i)\neq\tau(j)$ ce qui justifie que l'on peut parler d'inversions de la paire $\{\tau(i),\tau(j)\}$).

Notons $P_2=\big\{\{i,j\},i\neq j\in\{1,\dots,n\}\big\}$ l'ensemble des paires dans $\{1,\dots,n\}$. Par injectivité de σ, on a que $\sigma(P_2)=P_2$.

Notons maintenant, pour tout $\alpha\in S_n$,

$$P_2^{\alpha,-}:=\{\{i,j\}\in P_2,\ \{i,j\}\text{ est une inversion de }\alpha\},$$

$$P_2^{\alpha,+}:=\{\{i,j\}\in P_2,\ \{i,j\}\text{ n'est pas une inversion de }\alpha\}$$

et soit $B_\sigma^\tau=\big\{\{i,j\}\in P_2,\{\tau(i),\tau(j)\}\in P_2^{\sigma,-}\big\}$. Notons que $I(\alpha)=\mathrm{card}(P_2^{\alpha,-})$ par définition. Et de plus $\mathrm{card}(B_\sigma^\tau))=I(\sigma)$. En effet $\{i,j\}\mapsto\{\tau(i),\tau(j)\}$ est une bijection de P_2 sur lui-même puisque τ est bijectif. Par conséquent les paires dans B_σ^τ sont en bijection avec celles de $P_2^{\sigma,-}$.

Avec toutes ces notations et les deux conditions précédentes (dont on a vu qu'elles étaient disjointes), on obtient que

$$\begin{aligned}I(\sigma\circ\tau)&=\mathrm{card}\Big(P_2^{\tau,-}\setminus B_\sigma^\tau\Big)+\mathrm{card}\big(B_\sigma^\tau\setminus\big(P_2^{\tau,-}\cap B_\sigma^\tau\big)\big)\\&=\mathrm{card}(P_2^{\tau,-})-\mathrm{card}\big(P_2^{\tau,-}\cap B_\sigma^\tau\big)+\mathrm{card}(B_\sigma^\tau)-\mathrm{card}\big(P_2^{\tau,-}\cap B_\sigma^\tau\big)\big)\\&=I(\sigma)+I(\tau)-2\mathrm{card}\big(P_2^{\tau,-}\cap B_\sigma^\tau\big).\end{aligned}$$

Il suit que $I(\sigma\circ\tau)-I(\sigma)-I(\tau)$ est un nombre pair.

Et de plus

$$(-1)^{I(\sigma\circ\tau)}=(-1)^{I(\sigma)+I(\tau)-2\mathrm{card}\left(P_2^{\tau,-}\cap B_\sigma^\tau\right)}=(-1)^{I(\sigma)}\,(-1)^{I(\tau)}.$$

□

Lemme 4.65. *Si σ est une* transposition*, alors $I(\sigma)$ est impair.*

Démonstration. Par hypothèse on a $\sigma=(a\,b)$ avec $a<b$. Déjà toute paire $\{i,j\}$ qui ne contient pas a et b n'est pas une inversion car σ préserve i et j dans ce cas.

Considérons les paires $\{a,i\}$ avec $i\neq a,b$. Alors, si $i<a$, $\sigma(a)=b>a>i=\sigma(i)$ et donc cette paire n'est pas une inversion. de même si $i>b$, cette paire n'est pas une inversion. En revanche si $a<i<b$, alors $\sigma(a)-\sigma(i)=b-i>0$ est de signe opposé à $a-i<0$, donc c'est une inversion. Il y en a $b-a-1$ de cette forme. Si la paire est de la forme $\{j,b\}$ avec $j\neq a,b$, alors la même analyse montre que c'est une inversion de σ si et seulement si $a<j<b$. Il y en a donc aussi $b-a-1$. Enfin la paire $\{a,b\}$ est une inversion. Au total on a trouvé

$$I\big((a\,b)\big)=1+2(b-a-1)$$

qui est bien un nombre impair. □

Armé de ces deux lemmes, la démonstration de 4.56 devient facile. En effet on va pouvoir interpréter la signature comme $(-1)^{I(\sigma)}$ qui ne dépend que de σ et pas d'une décomposition.

Démonstration de la proposition et définition 4.56. Soit $\sigma=s_1\cdots s_k$ une décomposition en produit de transpositions. On a alors d'après le deuxième point du lemme 4.64 que

$$(-1)^{I(\sigma)}=(-1)^{I(s_1\cdots S_k)}=(-1)^{I(s_1)}\cdots(-1)^{I(s_k)}=(-1)^k$$

où la dernière égalité suit du lemme 4.65 qui donne que pour chaque transposition s on a $(-1)^{I(s)} = -1$.

Ainsi on a montré que la quantité $(-1)^k$ est égale à la quantité $(-1)^{I(\sigma)}$ qui ne dépend pas d'une quelconque écriture de σ en transpositions. Elle est donc indépendante d'une telle écriture. □

Remarque 4.66. On a en particulier démontré dans la preuve de 4.56 que

$$\operatorname{sgn}(\sigma) = (-1)^{I(\sigma)}. \tag{14}$$

On utilise souvent $(-1)^{I(\sigma)}$ comme définition de la signature car elle est indépendante de l'écriture (et on montre alors cette formule). Bien sûr, c'est équivalent et nous avons préféré insister sur la formule la plus pratique pour faire des calculs.

Remarque 4.67 (**La signature est multiplicative. Servez vous en !**). On a vu dans le corollaire 4.57 que *la signature est un morphisme de groupes* ; autrement dit elle est multiplicative. En particulier

$$\forall \sigma = \sigma_1 \cdots \sigma_k, \quad \operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma_1) \cdots \operatorname{sgn}(\sigma_k). \tag{15}$$

En particulier, cela s'applique si les σ_i sont des cycles (que les supports soient disjoints ou pas) et en plus dans ce cas là on peut utiliser le corollaire 4.57 pour faire le calcul.

Exemple 4.68. On a $\operatorname{sgn}\big((1\,3\,7\,9)\,(2\,4)\,(6\,5\,8)\big) = (-1)^3(-1)^1(-1)^2 = 1$.

Il faut connaître par cœur le corollaire 4.57 car il est très pratique pour faire des calculs.

5. Zoologie des groupes et leur classification

Nous avons étudié les définitions générales des groupes et quelques groupes particuliers en détail. Faisons un petit bilan de ce que l'on a vu. Tout d'abord il existe des groupes très différents : par exemple il existe des groupes de cardinal infini et même non-dénombrable, des groupes finis, des groupes commutatifs, des groupes non-commutatifs. Voici une liste d'exemples de groupes importants à garder en tête et de leurs propriétés à connaître :

- Les *groupes additifs* des espaces vectoriels, par exemple $(\mathbb{K}^n, +)$ où $\mathbb{K}$ est un corps. On a en particulier $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ munis de l'addition. Dans la même nature, on a aussi $(\mathbb{Z}, +)$.
- Les éléments inversibles d'un anneau unitaire et leur sous-groupes, par exemple $(\mathbb{R}^*, *)$, $(\mathbb{R}_*^+, *)$, $\mathbb{C}^*$, $\{z \in \mathbb{C},\ |z| = 1\}$ le cercle unité de $\mathbb{C}$. Cela n'ont pas été vraiment ce que l'on a étudié à fond.
- Les groupes cycliques finis C, qui sont tous isomorphes à un $\mathbb{Z}/n\mathbb{Z}$ où $n = \operatorname{Card}(C)$ est le cardinal du groupe C. Ceux là sont évidemment très importants et en arithmétique et en théorie des groupes, notamment car le groupe engendré par tout élément d'un groupe est cyclique (possiblement $\mathbb{Z}$ si d'ordre infini). C'est à dire, comme on l'a vu, que si g est d'ordre fini n dans un groupe G, alors $\langle g \rangle = \{e, g, g^2, \cdots, g^{d-1}\}$ où d est d'ordre g et on a pour tout entier $i \in \mathbb{Z}$, $g^i \cdot g^j = g^{i+j} = g^{r_{i+j}}$ où r_{i+j} est le reste de $i + j$ dans la division euclidienne de $i + j$ par d.
- Les groupes de bijections, où leur sous-groupes de bijections vérifiant certaines propriétés. En particulier, pour tout ensemble X, on a $(\operatorname{Bij}(X), \circ)$ les bijections de X vers lui-même muni de la composition des applications.

  On a croisé le sous-groupe des bijections du plan qui préserve un carré, mais aussi $GL(E)$ le groupe des isomorphismes linéaires d'un espace vectoriel E (qui est le sous-groupe des bijections de E formées des bijections qui sont en plus des applications linéaires) et son sous-groupe $SL(E)$. On va revenir sur certains de ces sous-groupes dans la suite du cours.

Si I est un intervalle, en analyse on peut aussi considérer le sous-groupe de $\mathrm{Bij}(I)$ formé par les bijections continues de I dans I.

Notons que le choix d'une base permet d'identifier, c'est à dire de donner un isomorphisme de groupes, $GL(E)$ avec $GL_n(\mathbb{K})$ les matrices inversibles.

Par ailleurs, on a vu que le groupe $\mathrm{Bij}(X)$ est fondamental au sens où il encode les actions de tout groupe sur X (revoir la définition de cela).

- Un cas particulier des bijections est le cas fini : $S_n = \mathrm{Bij}(\{1, \dots, n\})$, les groupes symétriques. C'est un groupe très très important que nous avons étudié en détail ; il est important notamment lorsque on étudie des actions sur des ensembles finis et des symétries. On verra en exercice que tout groupe fini est (isomorphe à) un sous-groupe d'un groupe symétrique. Il convient de comprendre la notion de cycles, de décomposition en cycles à supports disjoints et la signature. C'est un bon exercice de chercher des sous-groupes de S_n, en particulier pour $n = 3, 4$. Un sous-groupe important général de S_n est le groupe alterné A_n qui est le noyau de la signature.

Classifier tous les groupes (c'est à dire en avoir une compréhension exhaustive) est un problème excessivement ardu malgré l'omniprésence des groupes en mathématiques. Rappelons que lorsque l'on regarde des Évidemment, pour les groupes de petit cardinal, on peut comprendre de manière exhaustive la situation. Par exhaustive, on veut dire à *isomorphisme près*. Voilà quelques exemples :

- Les groupes de cardinaux 1 ne sont pas très intéressant. Ils contiennent seulement un élément neutre, donc de la forme $\{e\}$ avec $e * e = e$.
- Il n'y a, à isomorphisme près, qu'un seul groupe de cardinal p, pour p un nombre premier (si on ne se rappelle plus de la preuve, voir le corrigé du contrôle continu 1). C'est à dire qu'un groupe de cardinal p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. En particulier il est commutatif. C'est en particulier le cas pour $n = 2, 3$
- Il existe, à isomorphisme près, deux groupes de cardinaux 4 ; tous les deux commutatifs : il s'agit de $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- Il existe un seul groupe commutatif de cardinal 6 : il s'agit de $\mathbb{Z}/6\mathbb{Z}$. En revanche, il existe aussi un groupe de cardinal 6 non-commutatif : S_3.
- Il existe à isomorphismes près deux groupes non commutatifs d'ordre 8 : il s'agit de Q_8 (voire TD) et du groupe diédral de cardinal 8 que nous verrons plus tard. Et il y en a 3 de commutatifs (à isomorphisme près) : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$.

Terminons cette partie avec un théorème utile pour les groupes finis qui montre qu'un groupe contient des éléments d'ordre tout diviseur premier :

Théorème 5.1 (de Cauchy)**.** *Soit G un groupe fini. Si p est un nombre premier divisant* $\mathrm{card}(G)$*, alors il existe (au moins) un élément d'ordre p dans G*

Remarque 5.2. Attention le résultat n'est pas vrai si p n'est pas premier. Par exemple, il n'y a pas d'éléments dordre $8 = 2^3$ dans $(\mathbb{Z}/2\mathbb{Z})^3$.

Ce résultat permet d'aider à classifier les différents types de groupes. Il admet des généralisations puissantes appelés théorème de Sylow, que nous ne verrons cependant pas en cours. Il dit par exemple que, dans un groupe d'ordre 6, il existe forcément un élément d'ordre 2 et un élément d'ordre 3 (qui sont forcément distincts puisqu'ils n'ont pas le même ordre).

Remarque 5.3. (culturel) Le Théorème de Cauchy a des généralisations très fortes appelées Théorème de Sylow. Ils établissent entre autre que pour un groupe fini G dont le cardinal est $\mathrm{card}(G) = p_1^{i_1} \cdots p_r^{i_r}$ (où les p_i sont premiers), alors, il existe des sous-groupes de cardinaux $p_j^{i_j}$ pour tout j.

6. Sous-groupes normaux, groupes quotients

On va ici expliquer une généralisation dans le cas non-commutatif de la construction que l'on a vu de $\mathbb{Z}/n\mathbb{Z}$. Cette généralisation est plus subtile mais fondamentale en théorie des groupes. De nombreux exemples de groupes sont définis ainsi.

Pour cela rappelons que l'on a une action à droite canonique d'un sous-groupe H d'un groupe G sur G (Définition 3.17) : pour tout $g, \in G$, $h \in H$, $g^h = g * h$. À cette action est associée la relation d'équivalence $\mathscr{R}_H$: $g\mathscr{R}_H y \Leftrightarrow y^{-1}x \in H$. On a oté G/H l'ensemble quotient de G par la relation $\mathscr{R}_H$. Notons $\pi : G \to G/H$ la projection canonique.

La question que l'on va se poser, c'est si G/H a une structure de groupe canonique, au sens qu'elle est compatible [18] avec celle de G, ce que l'on exprimera par le fait que l'application quotient est un morphisme de groupes.

On a vu que c'était le cas pour $\mathbb{Z}/n\mathbb{Z}$, mais ce n'est pas le cas en général. Cette existence sera lié au fait que le sous-groupe est normal au sens ci-dessous.

6.1. Sous-groupes normaux/distingués.

Définition 6.1. Un sous-groupe H d'un groupe G est dit normal (ou distingué) si, pour tout $g \in G$, et tout $h \in H$, on a $ghg^{-1} \in H$. Autrement dit, H est stable par conjugaison par des éléments de g.

Notons, pour tout sous-ensemble $A \subset G$ et tout élément $g, h \in G$, $gA := \{g * a,\ a \in A\}$ et de même $Ah = \{a * g,\ a \in A\}$.

Le lemme suivant précise en termes ensemblistes ce que veut dire être normal.

Lemme 6.2. *Les propriétés suivantes sont équivalentes :*

(1) H est distingué,
(2) pour tout $g \in G$, on a $gHg^{-1} \subset H$,
(3) pour tout $g \in G$, on a $gHg^{-1} = H$.

Exercice 6.3. Démontrer le lemme

Remarque 6.4. Les deux terminologies : normal et distingué se trouve dans la littérature. La première étant nettement plus répandue à l'international que la seconde.

Introduisons une terminologie standard adaptée à la situation :

Définition 6.5. Deux parties H_1, H_2 d'un groupe G sont dites conjuguées si il existe un élément $g \in G$ telles que $g * H_1 * g^{-1} = H_2$.

On appelle conjugaison par g l'application [19] $G \to G$ donnée par $h \mapsto g * h * g^{-1}$.

La terminologie s'applique à des sous-parties quelconques, en particulier à des singletons et on peut donc parler d'éléments conjugués.

Le lemme nous dit qu'un sous-groupe H est normal si et seulement si il est égal à tous ses conjugués.

Voilà quelques exemples importants :

Exemple 6.6.
- Le groupe G est évidemment distingué dans lui même. De même, le sous-groupe trivial $\{e\}$ est normal dans G. En effet $\forall g \in G$, $g*e*g^{-1} = g*g^{-1} = e$.
- **Si G est un groupe abélien, alors tout sous-groupe est normal**. En effet, on a alors , pour tout $g \in G$, et tout $h \in H$, on a, par commutativité, que $ghg^{-1} = gg^{-1}h = eh = h \in H$.

18. sans exiger une telle comaptibilité, la question n'a pas de sens : on a vu que, par exemple, tout ensemble fini peut être muni d'une structure de groupes. Mais cette structure n'a en général aucun rapport avec celle de G

19. que nous avons déjà croisé

- Soit $f : G \to K$ un **morphisme de groupes**. Alors son **noyau** $\mathrm{Ker}(f)$ **est un sous-groupe normal** de G. En effet $\forall g \in G$ et pour tout $x \in \mathrm{Ker}(f)$, on doit montrer que gxg^{-1} est dans $\mathrm{Ker}(f)$. C'est à dire que $f(gx^{-1}) = e_K$ (le neutre de K). Hors

$$\begin{aligned} f(gxg^{-1}) &= f(g)f(x)f(g)^{-1} \text{ car } f \text{ est un morphisme de groupes} \\ &= f(g)e_K f(g)^{-1} \text{ car } x \in \mathrm{Ker}(f) \\ &= f(g)f(g)^{-1} = e_K. \end{aligned}$$

- L'exemple précédent nous dit en particulier que le sous-groupe $SL_n(\mathbb{K})$ est distingué dans $GL_n(\mathbb{K})$ puisque c'est le noyau du morphisme de groupes déterminant.

Il y a aussi des contre-exemples bien sûr. En voilà deux importants :

Exemple 6.7.
- Considérons la transposition (12) dans S_n (avec $n \geq 3$). Alors le sous-groupe engendré par (12), qui est juste $\{\mathrm{id}, (12)\}$ (puisque (12) est d'ordre 2) n'est *pas* normal. En effet on a que

$$(13)(12)(13)^{-1} = (13)(12)(13) = (13)(132) = (32) \notin \{id, (12)\}.$$

- Le sous-groupe orthogonal $O_n(\mathbb{R})$ (voir le cours d'algèbre 4 ou la suite de celui-ci) n'est pas normal dans $GL_n(\mathbb{R})$ dés que $n \geq 2$. En effet, une matrice orthogonale O est la donnée d'une base orthonormée $\mathscr{B}$. Si $\mathscr{B}'$ est une base non-orthonormée et P la matrice de passage, alors POP^{-1} est la matrice de $\mathscr{B}'$ dans la base canonique. Elle n'est pas orthogonale puisque $\mathscr{B}'$ ne l'est pas.

La conjugaison préserve les structures du groupe au sens suivant

Lemme 6.8. *Soit G un groupe et $g \in G$.*

- *La conjugaison par G est un isomorphisme de groupes de G sur lui même.*
- *Pour tout sous-ensemble H de G, on a que H est un sous-groupe si et seulement si ses conjugués $g * H * g^{-1}$ sont aussi des sous-groupes.*

En particulier, si H_1 et H_2 sont conjugués, alors ils ont même cardinaux (car la conjugaison est une bijection).

Exercice 6.9. Démontrer le lemme.

Remarque 6.10 (Conjugaison et commutativité). La conjugaison mesure précisément à quel point deux éléments x, y d'un groupe G ne commutent pas. En effet on a la relation souvent pratique

$$x * y = (x * y * x^{-1}) * x$$

qui provient du fait que $x * y = x * y * e = x * y * (x^{-1} * x)$. Cette relation dit donc que *quand on fait passer x à droite de y, alors y est transformé en son conjugué par x*. On a évidement une relation analogue si on fait passer y à gauche de x :

$$x * y = y * (y^{-1} * x * y).$$

6.2. **Groupes quotients.** On en arrive au théorème généralisant la construction des $\mathbb{Z}/n\mathbb{Z}$.

Théorème 6.11. *Soit H un sous-groupe d'un groupe $(G, *)$.*

- *Il existe sur l'ensemble quotient G/H une structure de groupe telle que la projection canonique $\pi : G \to G/H$ soit un morphisme de groupes* si et seulement si *H est un sous-groupe normal.*
- *Si H est normal, cette structure de groupe est unique et donnée par $\overline{x} \cdot \overline{y} = \overline{x * y}$.*

Lorsque H est normal, le groupe G/H donné par le théorème s'appelle le **groupe quotient de G par H**.

Démonstration. La première chose à remarquer est qu'en fait, il n'y a qu'une seule structure de groupes répondant à la question. Cela provient du fait que la projection canonique $G \to G/H$ est surjective. En particulier, pour toute $a, b \in G/H$, il existe x, y dans G tels que $a = \overline{x}$, $b = \overline{y}$.

Si π est un morphisme de groupes, alors on doit avoir que

$$ab = (\overline{x})\pi(\overline{y}) = \pi(x)\pi(y) = \pi(x * y) = \overline{x * y}.$$

Ceci montre donc que la seule multiplication possible est donnée par la formule annoncée.

Il reste à montrer que cette formule *est bien définie* et fait bien de G/H un groupe. En effet il y a une ambiguité dans cette définition : on a choisi des représentants x et y dans G des classes a et b de G/H.

Pour voir que la formule a du sens, il faut voir que cela ne dépend pas de ce choix.

C'est à dire que si on avait choisi d'autres représentants x', y' dans G tels que $a = \overline{x'}$, $b = \overline{y'}$, alors $\overline{x * y} = \overline{x' * y'}$. En effet dans ce cas là, la façon de choisir les représentants, ne change pas la valeur de la classe dans G/H qu'on obtient à la fin. Elle ne dépend donc que des classes a et b et est donc bien définie sur G/H.

On a la propriété :

> H est un sous-groupe normal si et seulement si quelques soient $x, x' \in G$ tels que $\overline{x} = \overline{x'}$ et $y, y' \in G$ tels que $\overline{y} = \overline{y'}$, on a $\overline{x * y} = \overline{x' * y'}$.

Démontrons cette propriété : l'hypothèse $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ signifie qu'il existe $h, k \in H$ tels que $x' = x * h$ et $y' = y * h$. On veut montrer que

$$x' * y' \in x * y * H \quad \Longleftrightarrow \quad x * h * y * k \in x * y * H.$$

En multipliant par x^{-1} puis y^{-1} à gauche (c'est à dire en simplifiant), on obtient qu'il suffit (et même qu'il est équivalent) que

$$y^{-1} * h * y * k \in H.$$

Or comme H est un groupe qui contient k (donc $H * k^{-1} = H$), en multipliant à droite par k^{-1} on obtient $y^{-1} * h * y \in H$ ce qui est vrai justement car H est normal.

Si on a pas remarqué qu'on a en fait raisonné par équivalence, on montre l'implication dans l'autre sens par contraposée : si H n'est pas normal, il existe $x \in G$, $h \in H$, tel que $x * h * x^{-1} \notin H$.

Alors $\overline{h} = \overline{e}$, mais $\overline{h * x^{-1}} \neq \overline{x^{-1}}$ car justement $(x^{-1})^{-1} * h * x^{-1} = x * h * x^{-1} \notin H$. Ceci conclut la preuve de la propriété.

Maintenant qu'on sait que la multiplication est bien définie, vérifier que c'est bien une structure de groupes est facile. L'associativité, l'inverse et le neutre provienent de celle de la multiplication de G. Par exemple $\overline{e_G}$ est le neutre pour G/H car

$$\overline{x} * \overline{e_G} = \overline{x * e_G} = \overline{x} = \overline{e_G * x} = \overline{e_G} * \overline{x}.$$

□

Exemple 6.12. Le sous-groupe $n\mathbb{Z}$ de $(\mathbb{Z}, +)$ est normal (puisque $\mathbb{Z}$ est abélien). On a alors que $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ est bien le groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$.

Remarque 6.13. Il faut bien faire attention que dans le théorème on demande que la projection canonique soit un morphisme de groupes. Autrement dit que la structure de groupe de G/H soit induite par celle de G. Sans cette propriété, G/H est un simple ensemble et on peut le munir de structures de groupes évidemment, mais qui n'ont plus de rapport avec celle de G.

Rappelons que $\text{card}(G/H) = \dfrac{\text{card}(G)}{\text{card}(H)}$. On en déduit que lorsque H est normal, tout élément du groupe quotient G/H est d'ordre divisant $\dfrac{\text{card}(G)}{\text{card}(H)}$.

Énonçons maintenant le théorème fondamental sur les morphismes associés à un groupe quotient. On rappelle le résultat vu en TD :

Proposition 6.14. *Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble X et $\pi : X \to X_{/\mathscr{R}}$ l'application quotient. Soit Y un ensemble. Alors on a une bijection naturelle entre les applications de $X_{/\mathscr{R}}$ vers Y et l'ensemble des applications de X vers Y qui sont constantes sur les classes d'équivalence.*

Cette bijection est donnée par $(X_{/\mathscr{R}} \xrightarrow{\overline{f}} Y) \mapsto X \xrightarrow{\overline{f}\circ\pi} Y$.

Dire qu'une application $f : X \to Y$ est constante sur les classes veut dire que si $x\mathscr{R}x'$, alors $f(x) = f(x')$.

La proposition dit alors essentiellement que si on a une telle application, il existe une unique application $\overline{f} : X_{/\mathscr{R}} \to Y$ telle que pour tout $x \in X$, on a $f(x) = \overline{f}(\overline{x})$

(on dit que f se factorise de manière unique au travers de $X_{/\mathscr{R}}$).

Si on rajoute les structures de groupe on aboutit au résultat suivant :

Théorème 6.15. *Soit H un sous-groupe normal d'un groupe G et K un groupe. Il existe une bijection canonique entre les morphismes de groupes $G/H \to K$ et les morphismes de groupes $G \to K$ tels que $H \subset \text{Ker}(f)$.*

Autrement dit, *un morphisme de groupes de G/H vers K est simplement la donnée d'un morphisme de groupes de G vers K tel que $f(H) = \{e_K\}$*, c'est à dire qui "s'annule sur H". Le lien entre les deux est que pour un tel morphisme il existe une unique application $\overline{f} : G/H \to K$ telle que pour tout $g \in G$, on a $f(g) = \overline{f}(\overline{g})$.

Comme la surjection canonique est...une surjection, on a que

$\overline{f}$ est une surjection si et seulement si f est une surjection.

Démonstration. En vertu de la proposition 6.14, pour montrer qu'une application $f : G \to K$ passe au quotient, il suffit de vérifier que si $x\mathscr{R}_H y$, alors $f(x) = f(y)$. Or $x\mathscr{R}_H y$ signifie précisément qu'il existe $h \in H$ tel que $y = x * h$. On a alors, que

$$\begin{aligned} f(y) &= f(x*h) = f(x) * f(h) \text{ car } f \text{ est un morphisme de groupes} \\ &= f(x) * e_K = f(x) \text{ car } h \in H \text{ et donc } f(h) = e_K. \end{aligned}$$

Cela donne l'existence de $\overline{f}$ comme application. Il reste à vérifier que c'est un morphisme de groupes. Or, pour toute classe $c, d \in G/H$ on peut trouver $x, y \in G$ tels que $c = \overline{x}$, $d = \overline{y}$ et on a

$$\begin{aligned} \overline{f}(c*d) = \overline{f}(\overline{x}*\overline{y}) = \overline{f}(\overline{x*y}) = f(x*y) \text{ (par définition de } \overline{f}) \\ = f(x) * f(y) = \overline{f}(\overline{x} * \overline{f}(\overline{y}) = \overline{f}(c) * \overline{f}(d). \end{aligned}$$

□

Exemple 6.16. Considérons deux groupes $(G, *_G)$ et $(H, *_H)$. On peut former le groupe produit $G \times H$ (3.68). Alors le sous-ensemble $\{e\} \times H \subset G \times H$ est un sous-groupe. On peut vérifier que c'est un sous-groupe normal et que le groupe quotient $G \times H/\{e\} \times H$ est isomorphe à $(G, *_G)$.

Exercice 6.17. Démontrer ces affirmations.

On retrouve comme corollaire une propriété que l'on a déjà vu "à la main".

Corollaire 6.18. *Soit $(G, *)$ un groupe.*

- *Un morphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $(G,*)$ est uniquement déterminé par un élément $g \in G$ tel que $g^{*n} = e$.*
- *La bjiection entre morphismes et $\{g, \in G,\ g^{*n} = e\}$ est donnée comme suit. À un morphisme de groupes $\mathbb{Z}/n\mathbb{Z} \xrightarrow{f} G$ on associe l'élément $f(1)$ et réciproquement à un tel g, on associe le morphisme donné par $f(\overline{n}) = g^{*n}$.*

Démonstration. On a vu en cours qu'un morphisme $f : (\mathbb{Z}, +) \to (G, *)$ est équivalent à la donnée de $f(1) \in G$ via la formule $f(n) = (f(1))^{*n}$.

En vertu du théorème 6.15, il suffit donc de voir quand $n\mathbb{Z} \subset \ker(f)$. Or ceci veut dire que $f(n) = e_G$ c'est à dire $f(1)^{*n} = e$ puisque n est générateur de $n\mathbb{Z}$. □

Exemple 6.19. L'application $\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ donnée par $n \mapsto \overline{3n}^{12}$ est un morphisme de groupes. Son noyau est $\{n \in \mathbb{Z}, 3n \equiv_{12} 0\} = 4\mathbb{Z}$. Il suit du théorème que l'on a un morphisme de groupes $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dont la formule est $\overline{x}^4 \mapsto \overline{3x}^1 2$. Cet exemple se généralise facilement à d'autres $\mathbb{Z}/n\mathbb{Z}$.

Exemple 6.20. Considérons le sous-groupe $3\mathbb{Z}/6\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ (c'est à dire $\{\overline{0}^6, \overline{3}^6\}$). C'est forcément un sous-groupe normal puisque $\mathbb{Z}/6\mathbb{Z}$ est abélien.

Considérons, l'application $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $\overline{x}^6 \mapsto \overline{x}^3$ (c'est à dire qui prend un nombre modulo 6 et le regarde modulo 3.) et c'est un morphisme de groupes surjectifs (laissé en exercice ; cela découle directement des définitions).

Comme $f(3\overline{x}^6) = \overline{3x}^3 = 0$, on obtient que f induit un morphisme de groupes surjectifs $\overline{f} : \mathbb{Z}/6\mathbb{Z}/(3\mathbb{Z}/6\mathbb{Z}) \to \mathbb{Z}/3Z$.

Démontrons qu'il est en plus injectif. On a que $\overline{x}^3 = \overline{0}^3$ si et seulement si $x \equiv_3 0$, c'est à dire que $x \in 3\mathbb{Z}$. Il suit que $\overline{x}^6 \in 3\mathbb{Z}/6$ et donc $\ker(\overline{f}) = [\overline{0}] \in \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$.

Par conséquent $\overline{f}$ est un isomorphisme : $\mathbb{Z}/6\mathbb{Z}/(3\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$.

Exemple 6.21. Il est facile de vérifier que $\{-1, 1\}$ est un sous-groupe de $(\mathbb{R}^*, \times)$, qui par commutativité est normal. On a donc un groupe quotient $\mathbb{R}^*/\{\pm 1\}$. Par ailleurs, l'application valeur absolue $\mathbb{R}^* \to \mathbb{R}^*_+$, $x \mapsto |x|$ est un morphisme de groupes surjectif. Son noyau est précisément $\{\pm 1\}$ si bien qu'on obtient un isomorphisme de groupes $\mathbb{R}^*/\{\pm 1\}$ avec $(\mathbb{R}^*_+, \times)$.

Exemple 6.22. On peut montrer d'une manière similaire aux exemples précédents que le cercle vu comme le sous-groupe des nombres complexes de modules 1 est isomorphe au groupe quotient $\mathbb{R}/\mathbb{Z}$ (via l'application $t \mapsto \exp(2i\pi t)$.)

Les exemples précédents identifient tous les quotients construits avec des groupes classiques vu autrement. Ce n'est pas toujours le cas (par exemple $\mathbb{Z}/n\mathbb{Z}$), nous verrons d'autres exemples plus tard. La plupart des exemples précédents sont des exemples de la proposition suivante :

Théorème 6.23 (Premier théorème d'isomorphisme)**.** *Soit $f : G \to K$ un morphisme de groupes. Alors l'application $[x] \mapsto f(x)$ est bien définie et un isomrphisme de groupes de $G/\ker(f)$ sur (le sous-groupe) $\mathrm{Im}(f)$.*

Démonstration. Par le théorème 6.15, on a immédiatement que l'application $f : x \mapsto f(x)$ passe au quotient par le sous-groupe $\ker(f) \subset G$ pour donner un morphisme de groupes. Par définition l'application induite $\overline{f} : G/\ker(f) \to H$ est donnée par $[x] \mapsto f(x)$, cets à dire celle donnée par l'énoncé. Ce qui prouve que cette application est un morphisme de groupe bien défini. On a que $\overline{f}$ est surjective puisque pour tout $y \in \mathrm{Im}(f)$, il existe x tel que $y = f(x)$ et donc $y = \overline{f}([x])$. Il reste à voir l'injectivité. Mais

$$\overline{f}([x]) = e_k \ \Leftrightarrow\ f(x) = e_K \ \Leftrightarrow\ x \in \ker(f) \ \Leftrightarrow\ [x] = [e] \in G/\ker(f)$$

ce qui donne l'injectivité de $\overline{f}$ et donc finalement que $\overline{f}$ est un isomorphisme. □

Proposition 6.24 (Théorème d'isomorphisme des groupes quotients)**.** *Soit $K \subset H$ deux sous-groupes normaux d'un groupe G. Alors H/K est un sous-groupe normal de G/K et on a un isomorphisme naturel de groupes $(G/K)/(H/K) \cong (G/H)$. Cet isomorphisme est donné par $\overline{\overline{g}^K}^{H/K} \mapsto \overline{g}^H$ (qui est bien définie).*

L'énoncé se retient facilement car il se comporte exactement comme la simplification des fractions !

Exercice 6.25. Démontrer cette proposition.

6.3. **Actions de groupes et quotients.** Soit $(G, *)$ un groupe agissant (disons à gauche, mais on peut tout faire à droite aussi bien-sûr) sur un ensemble X ; on note ${}^g x$ le résultat de l'action d'un $g \in G$ sur un élément $x \in X$.

On a la relation d'équivalence (3.20) associée à cette action et rappelons que, par définition, on a que la classe $C_x = \{{}^g x, g \in G\}$. Attention, en général, l'écriture ${}^g x$ n'est pas unique pour un élément de C_x : il existe plusieurs $g \in G$ pour lesquels l'élément ${}^g x$ est le même. En fait il y en a précisément autant que d'éléments de stab_x :

Proposition 6.26. *Quel que soit $x \in X$, stab_x est un sous-groupe de G et on a une bijection naturelle $G/\mathrm{stab}_x \cong C_x$ donnée par $\overline{g} \mapsto {}^g x$.*

Démonstration. On a déjà vu que c'était un sous-groupe (lemme 3.14). L'action de G sur X nous donne en particulier l'application $\phi_x : G \to C_x$ définie par $g \mapsto {}^g x$ qui est *surjective* (par définition les éléments s'écrivant sous la forme ${}^g x$ sont bien ceux de l'orbite de x). Par ailleurs, cette application est constante sur les classes de stab_x. En effet, si $x \mathscr{R}_{\mathrm{stab}_x} y$, alors on a $y = x * h$ avec h un élément de stab_x. Et alors

$$ {}^{g*h}x = {}^g({}^h x) = {}^g x $$

par définition du stabilisateur.

En vertu de la proposition 6.14, l'application $\phi_x : g \mapsto {}^g x$ passe donc au quotient et on a donc une application (encore *surjective*) $\overline{\phi_x} : G/\mathrm{stab}_x \to X$ donnée précisément par la formule du lemme : $\overline{\phi_x}(\overline{g}) = {}^g x$. Il reste à voir qu'elle est injective. Autrement dit que $\overline{\phi_x}(\overline{g}) = \overline{\phi_y}(\overline{g'})$ implique $\overline{g} = \overline{g'}$. Or $\overline{\phi_x}(\overline{g}) = \overline{\phi_y}(\overline{g'})$ signifie que ${}^g x = {}^{g'} x$. En faisant agir ${g'}^{-1}$ sur cette égalité, on obtient

$$\begin{aligned} {}^{(g')^{-1}}({}^g x) &= {}^{(g')^{-1}}({}^{g'} x) \\ {}^{(g')^{-1}*g} x &= {}^{(g')^{-1}*g'} x \\ {}^{(g')^{-1}*g} x &= {}^e x = x \end{aligned}$$

ce qui montre que $(g')^{-1} * g \in \mathrm{stab}_x$ et donc $g \mathscr{R}_{\mathrm{stab}_x} g'$ et donc $\overline{g} = \overline{g'}$. □

On peut (en tout cas on devrait) se demander comment se comporte le stabilisateur d'un élément y par rapport à celui d'un élément qui est dans sa même classe de conjugaison. La réponse (importante !) est qu'ils sont conjugués.

Proposition 6.27. *Soit $(G, *)$ un groupe agissant sur un ensemble X et $x \in X$. Alors, pour tout $y \in C_x$, on a que stab_y est* conjugué [20] *à stab_x : $\exists g \in G$ tel que $\mathrm{stab}_y = g * \mathrm{stab}_x * g^{-1}$.*

Démonstration. Tout d'abord, il existe $g \in G$ tel que $y = {}^g x$ par hypothèse.

Soit $h \in G$. Alors $h \in \mathrm{stab}_y$ si et seulement si

$$ {}^h y = y \Leftrightarrow {}^h({}^g x) = {}^g x \tag{16} $$

Or pour tout $s \in G$, $a, b \in X$, on a que

$$ a = b \iff {}^s a = {}^s b $$

20. Définition 6.5

En effet $a = b$ implique ${}^s a = {}^s b$ en faisant agir s sur les deux membres. Réciproquement, en faisant agir s^{-1} (par la magie de l'existence d'inverse dans un groupe) sur l'égalité ${}^s a = {}^s b$ on obtient

$$ {}^{s^1}({}^s a) = {}^{s^{-1}}({}^s b) \Leftrightarrow {}^{s^{-1}s}a = {}^{s^{-1}s}b \Leftrightarrow {}^e a = {}^e b \Leftrightarrow a = b. $$

On applique cela au membre de droite de (16) en agissant par g^{-1} et on obtient

$$ {}^h y = y \Leftrightarrow {}^{hg}x = {}^g x \Leftrightarrow {}^{g^{-1}}({}^{hg}x) = {}^{g^{-1}}({}^g x) \Leftrightarrow {}^{g^{-1}hg}x = {}^e h \Leftrightarrow {}^{g^{-1}hg}x = x $$

Par conséquent $h \in \mathrm{stab}_y$ si et seulement si $g^{-1}hg \in \mathrm{stab}_x$. On en conclut que $\mathrm{stab}_x = g^{-1}\mathrm{stab}_y g$ ou de manière équivalente $\mathrm{stab}_y = g\mathrm{stab}_x g^{-1}$. On a bien obtenu que les stabilisateurs sont conjugués. □

La proposition 6.26 donne des formules très utiles pour compter des symétries ou en mathématiques discrètes et informatique dans des problèmes de dénombrement :

Corollaire 6.28. *Soit G un groupe agissant sur un ensemble X.*

- *Pour tout $x \in X$, on a*
$$ \mathrm{card}(C_x) = \frac{\mathrm{card}(G)}{\mathrm{card}(\mathrm{stab}_x)}, $$
- *et* $\mathrm{card}(X) = \mathrm{card}(G) \left(\sum_{C_x \in X_G} \frac{1}{\mathrm{card}(\mathrm{stab}_x)} \right)$.

Ce corollaire exprime notamment le cardinal des orbites en fonction du cardinal des stabilisateurs et vice-versa.

Démonstration. La proposition 6.26 nous donne une bijection entre C_x et le cardinal du quotient G/stab_x. Ils ont donc les mêmes cardinaux et on a vu (c'est le théorème de Lagrange) que $\mathrm{card}(G/\mathrm{stab}_x) = \dfrac{\mathrm{card}(G)}{\mathrm{card}(\mathrm{stab}_x)}$. La première formule est donc démontrée.

Puisque les classes d'équivalence forment une partition de X, alors, $\mathrm{card}(X) = \sum_{\alpha \in X_G} \mathrm{card}(\alpha)$ et de la première formule découle la seconde. □

Enfin on a le théorème important suivant (compagnon du précédent) très utile dans les problèmes de comptage, qui relie les points fixes et le nombre d'orbites distinctes.

Rappelons que X_G **est le quotient de X par l'action de G**, cf 3.21 (autrement dit l'ensemble obtenu en identifiant entre eux tous les points de X qui sont dans une même orbite).

Théorème 6.29 (dit de Burnside)**.** *Soit G un groupe fini agissant*[21] *sur un ensemble fini X. On a*

$$ \mathrm{card}(X_G) = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \mathrm{card}(\mathrm{Fix}(g)) $$

Ce théorème est souvent utile pour calculer le cardinal de l'ensemble quotient X_G.

Démonstration. La preuve[22] consiste à regarder comment l'action globale de G se distribue sur les différentes orbites en remarquant que si x est un point fixe de g, alors g est dans le stabilisateur de x ; ce qui va permettre de comparer orbites, stabilisateurs et fixateurs.

Précisément l'idée est de considérer

$$ S := \{(y, g) \in X \times G,\ {}^g y = y\} $$

21. le résultat est vrai que l'action soit à droite ou à gauche
22. faite dans le cas d'une action à gauche. Le cas à droite se fait de même.

autrement dit l'ensemble des paires constituées d'un élément de X et d'un élément du groupe pour lequel il est fixe. D'un autre côté dire que y est fixé par g revient à dire que $g \in \mathrm{stab}_y$. Autrement dit, on va pouvoir compter les éléments dans cet ensemble de deux manières différentes : en faisant la somme, sur chaque y, des éléments dans stab_y et aussi en faisant la somme sur chaque g des éléments de $\mathrm{Fix}(g)$. Cela nous donnera (à division par $\mathrm{card}(G)$ près) les deux membres de l'équation que l'on doit démontrer !

En particulier, la deuxième décomposition nous dit que S est la réunion disjointe (sur $g \in G$) des $\mathrm{Fix}(g)$ et donc :

$$\mathrm{card}(S) \;=\; \sum_{g\in G} \mathrm{card}(\mathrm{Fix}(g)). \tag{17}$$

D'un autre côté nous avons aussi que S est la réunion *disjointe* $\bigcup_{x\in X} \mathrm{stab}_x$. Il suit que

$$\mathrm{card}(S) \;=\; \sum_{x\in X} \mathrm{card}(\mathrm{stab}_x) = \sum_{x\in X} \frac{\mathrm{card}(G)}{\mathrm{card}(C_x)} \tag{18}$$

par le corollaire 6.28. Par ailleurs on sait que les classes d'équivalence forment une partition de X : $X = \bigcup_{C_x\in X_G} C_x$. Ainsi on peut réécrire le membre de droite sous la forme

$$\begin{aligned} \sum_{x\in X} \frac{\mathrm{card}(G)}{\mathrm{card}(C_x)} &= \mathrm{card}(G) \sum_{C_x\in X_G} \sum_{y\in C_x} \frac{1}{\mathrm{card}(C_y)} \\ &= \mathrm{card}(G) \sum_{C_x\in X_G} \sum_{y\in C_x} \frac{1}{\mathrm{card}(C_x)} \;(\text{car } C_y = C_x \text{ si } y \in C_x) \\ &= \mathrm{card}(G) \sum_{C_x\in X_G} 1 = \mathrm{card}(G)\,\mathrm{card}(X_G). \end{aligned} \tag{19}$$

On déduit des égalités (19), (18) et (17) que

$$\mathrm{card}(G)\,\mathrm{card}(X_G) \;=\; \mathrm{card}(S) \;=\; \sum_{g\in G} \mathrm{card}(\mathrm{Fix}(g))$$

ce qui nous donne l'égalité voulue.

□

II. Symétries et Groupes en Géométrie

1. Un peu de philosophie et d'histoire

1.1. **Groupes associés à une situation géométrique.** La notion de groupes et d'actions de groupe est étroitement reliée à la géométrie et la notion de "symétrie". Avec ce point de vue, on voit un groupe comme le groupe des transformations d'un espace conservant des propriétés géométriques.

Nous allons plus précisément étudier la géométrie en dimension 2 et 3 à la fin du cours. En attendant, donnons des exemples de cette philosophie.

- La *géométrie affine ou vectorielle* : c'est à dire celle du plan, de l'espace de dimension 3 ou de plus grande dimension où on considère la notion de droite, droite parallèles, triangles etc... La notion importante est celle d'être colinéaire, c'est à dire sur la même droite, d'être sécants (c'est à dire de se couper). La différence entre la géométrie affine et la géométrie vectorielle tient en ce qu'on ne fixe pas d'origine (le 0) dans la première.
- La *géométrie eucldienne* (affine ou vectorielle) où l'on ajoute en plus à la géométrie affine la notion de distance, et donc de carrés, angles, triangles isocèles, etc... C'est en général celle à laquelle vous pensez intuitivement. Nous la définirons précisément plus loin (et vous le voyez en algèbre 4 également).
- On peut s'intéresser à une géométrie intermédiaire : on peut ajouter non pas la notion de distance, mais seulement de volume [23], c'est à dire l'aire en dimension 2, dans un espace affine et s'intéresser donc aux transformations qui préserve ce volume.
- Plus spécifiquement, parmi des exemples vu en TDs, on peut s'intéresser aux symétries d'un carré, cube ou autre objet géométrique et à ses spécificités.
- Il existe des géométries *non-euclidiennes* où on a des notions de distance différente et donc des figures géométriques différentes à préserver. Ces objets ne sont pas si ésotériques : par exemple nous vivons sur une sphère soumis à une géométrie sphérique, et la géométrie hyperbolique est importante dans la notion d'espace-temps de la physique.

Quel est le rapport avec les groupes ? Et bien le groupe en question dans ces contextes géométriques va être le sous-groupe des bijections de l'ensemble sous-jacent qui préserve les propriétés géométriques qui nous intéressent. En général, ce groupe *caractérise* cette structure, si bien qu'on peut (et cela arrive en pratique) définir la géométrie par le groupe.

Remarque 1.1 (Un peu d'histoire). À la fin du XIXème siècle, le programme d'Erlangen promu par Felix Klein, a été un programe de recherche très influent (jusqu'à nos jours) en mathématiques qui a justement pris pour point de vue de comparer (et construire) les différents types de géométrie en se basant sur les actions de leurs groupes de symétrie. Il a notamment permis de mieux comprendre des géométries non-euclidiennes et d'en construire des exemples. L'existence de géométrie non-euclidienne a été longtemps un sujet de recherche ne mathématiques. Voir la partie 1.2 sur les axiomes d'Euclide pour en voir les enjeux.

Voyons quelques exemples : dans le cas de la géométrie affine ou vectorielle, c'est le contenu du théorème suivant (qui est culturel et pas à connaître).

23. ce qui n'est pas aussi simple que cela à définir

Théorème 1.2 (Théorème fondamental de la géométrie affine)**.** *Soit E un espace affine*[24] *ou vectoriel (de dimension au moins 2). Soit f une bijection de E dans E. Alors on a :*

Cas Vectoriel: *f est linéaire, si et seulement si, f envoie trois points alignés sur trois points alignés (autrement dit préserve les droites) et vérifie $f(0) = 0$.*

Cas Affine: *f est affine si et seulement f envoie trois points alignés sur trois points alignés (autrement dit préserve les droites).*

Autrement dit, le théorème dit que $GL_n(\mathbb{R})$ est *exactement* le groupe des transformations bijectives de $\mathbb{R}^n$ qui envoie des droites sur des droites (et donc en particulier de telles applications sont donc nécessairement linéaires). Le mot affine dans le théorème précédent veut essentiellement dire que c'est la composée d'une translation et d'un élément de $GL_n(\mathbb{R})$ (si E de dimension n).

Dans le même ordre d'idée, on a le résultat suivant dans le cas où on rajoute la notion de distance/longueurs (ou angles...).

Théorème 1.3. *Soit $\mathbb{R}^n$ muni de sa structure euclidienne*[25]*. Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une bijection.*

Cas Vectoriel: *(f préserve les distances et $f(0) = 0$) si et seulement si f est une isométrie linéaire (c'est à dire un élément de $O_n(\mathbb{R})$).*

Cas Affine: *f préserve les distances si et seulement f est une isométrie affine.*

On pourrait multiplier les exemples. Notamment le groupe intéressant en ce qui concerne la préservation des volumes (orientés) est $SL_n(\mathbb{R})$ (que nous avons déjà croisé en exemples et exercices).

Si on s'intérèsse à un cube dans $\mathbb{R}^3$, alors on peut regarder le groupe de toutes les isométries de l'espace qui le préservent par exemple. C'est à dire le groupe qui encode les propriétés géométriques d'un cube etc...

Pour résumer, on peut penser une situation géométrique, ou des symétries[26] comme la donnée d'un groupe agissant sur un ensemble (par exemple le plan, ou le cube etc...), le groupe étant vu comme les symétries de l'ensemble ou les transformations de l'ensemble préservant une certaine structure (qu'on appelera géométrique).

Terminologie : dans ce contexte, l'ensemble sera souvent appelé espace (suivi d'un adjectif décrivant le type de géométrie) et le groupe les symétries de l'espace ou simplement le groupe (suivi du même adjectif décrivant le type de géométrie).

Nous allons dans les parties suivantes voir des exemples de géométrie et symétrie et en étudier certains-importants et universels-plus à fond. Ces exemples ne s(er)ont pas déconnectés de ceux des autres cours de mathématiques, bien-sûrs, et en particulier de celui d'algèbre 4.

1.2. **Intermède culturel : les 5 axiomes d'Euclide.** Cette petite partie est purement *culturelle* et vaguement historique. Nous ne définirons rien précisément, mais nous la citons pour l'élève curieux et parce que ces axiomes, en particulier le cinquième a été la source de beaucoup de développements en géométrie, et notamment l'interprétation via des actions de groupes.

Dans son traité phare, les *Éléments*, Euclide pose 5 axiomes pour fonder les bases de la géométrie (de l'espace), qu'on appelerait aujourd'hui euclidienne. Plutôt que de parler de longueur, il parle d'angles, et en particulier d'angles droit. Et plus précisément, il s'agit de géométrie des figures que l'on peut étudier à la règle et au compas. Autrement dit les objets de base sont des points, droites, demi-droites, segments, cercles.

24. Pour l'instant il n'est pas nécessaire d'être plus précis qu'avant sur la définition

25. c'est à dire le produit scalaire usuel, autrement dit la notion de distance usuelle dont le plus court chemin entre 2 points est une droite

26. y compris en dehors des mathématiques : que ce soit la physique, mécanique, chimie

Par axiome, il entend essentiellement des principes évidents et acceptés de tous avec lesquels on va baser toutes les constructions et démonstrations mathématiques en suivant les règles de logique.

Voici la liste des 5 axiomes :

(1) Par deux points distincts quelconques passe un segment de droite ;
(2) Un segment de droite peut être prolongé indéfiniment en une ligne droite ;
(3) Étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre ;
(4) Tous les angles droits sont égaux ;
(5) étant donné un point et une droite ne contenant pas le point, il passe toujours une unique parallèle à cette droite passant par ce point.

Remarque 1.4 (Axiome 4). Le quatrième axiome doit sembler bizarre. Mais il provient du fait qu'Euclide n'a pas dans son traité la notion de mesure d'un angle (il est en train de construire les bases de la géométrie). Du coup qu'appelle-t-il angle droit ? Et bien lorsque deux droites se coupent (sont sécantes en termes plus pompeux), elles forment ce qui est appelé (par définition) deux angles : l'un obtu, l'autre inclus. Si ces deux anles sont égaux, alors on appelle cet angle un angle droit. Je vous laisse dessiner une figure pour vous convaincre que c'est une bonne définition.

Ce quatrième axiome d'Euclide signifie que cette situation où les angles obtus et inclus sont égaux n'arrive que si les angles sont "égaux". Par égal, on doit comprendre ce qu'on nomme maintenant congruent de nos jours, ce qui signifie qu'on peut superposer, exactement l'une sur sur l'autre, deux configurations de droites vérifiant la condition dangle droit en utilisant une translation et une rotation. Notions que l'on peut définir en terme de règle et compas. Évidemment, en terme modernes, on utilisera plutôt le fait que ces deux configuratiosn peuvent être placées l'une sur l'autre en utilisant une isométrie *positive*[27].

Autrement dit, ces deux configurations sont égales dans cet axiome, si elles sont dans la même orbite pour l'action du groupe des isométries positives (qui on le verra, en dimension 2 n'est rien d'autre que celui engendré par les translations et rotations).

Remarque 1.5. Le *cinquième axiome* que nous donnons n'est en fait *PAS* celui donné originellement par Euclide (qui est plus pénible à énoncer). Mais un axiome équivalent (du à Playfair). Notons qu'il suffirait de l'énoncer sous la forme *étant donné un point et une droite ne contenant pas le point, il passe au plus une parallèle à cette droite passant par ce point* car les autres axiomes permettent de montrer qu'il existe toujours au moins une telle droite.

Pendant longtemps des mathématiciens ont cherché à montrer que ce cinquième axiome est en fait inutile. C'est à dire qu'on pouvait le démontrer à partir des autres. La construction de géométrie non-euclidienne au début du XIXème siècle a montré que non. En effet, des géométries vérifiant les autres axiomes mais pas celui là ont été découvertes. Géométries devenues par la suite importante dans de nombreux domaines.

Notons que de nombreux mathématiciens ont tenté de résoudre ce problème en donnant d'autres formulations de cet axiome, mais souvent lorsqu'ils arrivaient à une preuve, c'est qu'à un moment ou autre ils utilisaient une des 4 façons usuelles de définir le mot parallèle à savoir :

(1) deux droites sont parallèles si elles ne se coupent pas.
(2) Deux droites sont parallèles si la distance entre un point d'une des droite et l'autre droite reste constante lorsque le point parcourt la droite
(3) Deux droites sont parallèles lorsque elles définissent les mêmes angles lorsqu'elles sont coupées par toute troisième droite.

27. nous n'avons pas encore défini ce dernier terme, voir la suite du cours

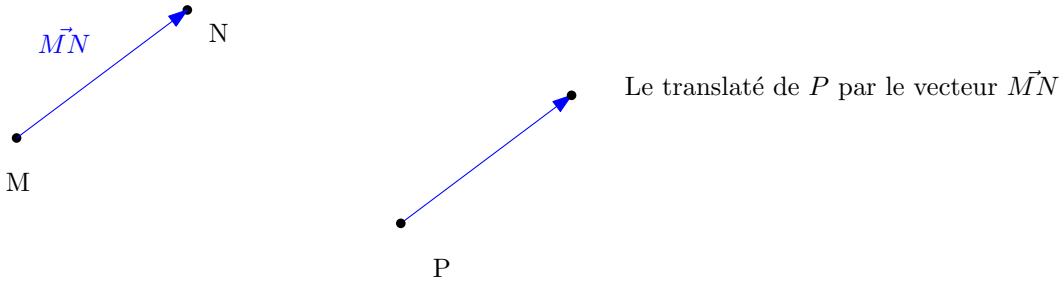


FIGURE 4. Vecteurs dans un espace affine

(4) Deux droites sont parallèles lorsque elles définissent les mêmes angles lorsque il existe une troisième droite qui les coupe en définissant les mêmes angles.

Or ces notions ne sont pas toutes équivalentes si on se limite seulement aux 4 premiers axiomes...

Nous allons donner un modèle de la géométrie affine en utilisant les notions d'espace vectoriels et action de groupes dans les parties suivantes. Voir définition 2.1.

2. Notions de géométrie affine et euclidiennes

Les espaces affines et les espaces vectoriels sont deux notions très proches, masi *différentes*. Il faut avoir en tête qu'un espace affine est comme un espace vectoriel où l'on a pas choisi d'origine, ou plus précisément un espace vectoriel est la donnée d'un espace affine où on a spécifié l'origine, le point 0 de l'espace. Cette dernière notion s'utilise souvent en physique où on change ou choisit un repère de coordonnées (ce qui revient à chosiir une origine puis une base de l'espace affine).

Un espace *affine de dimension 2 représente donc le plan traditionnel de la géométrie, et un espace affine de dimension 3 notre espace ambiant.*

Par espace ambiant on sous-entend "le monde" qui nous entoure (au sens du déplacement physique en trois directions) ; celui dans lequel vivent les droites, points, plans etc.... Donc l'intuition que vous en avez vous sera utile. Nous allons voir ci-dessous comment mathématiser cette construction. Mais il ne faudra pas que cela gâche votre intuition géométrique.

Pourquoi ne peut-on pas se contenter de la notion d'espace vectoriel (de dimension 3) pour cela ? Tout simplement parce que notre univers n'a ni direction, ni points privilègiés et encore moins de structure de groupe naturelle (contrairement aux espaces vectoriels). On peut précisément faire une identification de l'espace avec $\mathbb{R}^3$ (resp. avec sa structure euclidienne canonique) si on choisit exactement une origine et une base, à savoir 3 directions non-colinéaires (resp. 2 à 2 orthogonales) et on peut mesurer ds vecteurs entre deux points que l'on peut transporter partout. C'est cela que va encoder un espace affine.

En pratique on sait aussi mesurer une distance entre deux points et c'est ce que codera la géométrie affine euclidienne ci-dessous.

De manière générale, dans l'espace ou plan affine, à tout couple de point M, N on peut associer le vecteur $\vec{MN}$ et on peut additionner des vecteurs, ou les multiplier par un scalaire. On ne peut pas addiitoner des points en revanche. On peut par contre les translater en suivant un vecteur. Notons aussi qu'un vecteur peut être déterminé par différentes paires de points. Enfin, si on choisit une origine arbitraire (c'est à dire un point) O dans l'espace, alors on peut identifier tout point M avec le vecteur $\vec{OM}$ et ainsi identifier, via ce point l'espace affne avec un espace vectoriel ; dont le 0 est le point O (arbitrairement) choisi.

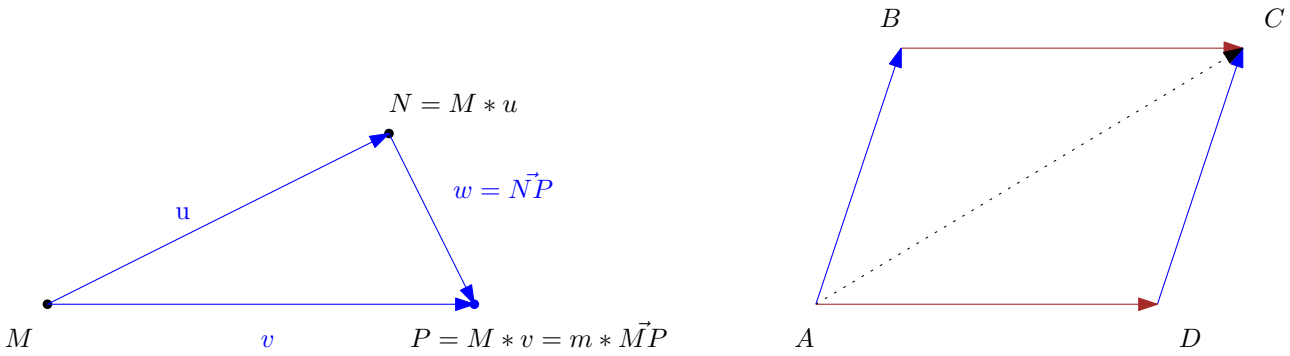


FIGURE 5. À gauche, trois points M, N, P et les vecteurs qui les relient illustrant Chasle. À droite, une repésentation graphique de l'identité du parallèlogramme

La structure des vecteurs ets précisément analogue de celle des éléments d'un espace... *vectoriel*. La notion de translation par un vecteur rappelle elle celle d'une action...

2.1. **Espaces affines.** On formalise l'idée donnée d'espace affine et de son lien avec la notion de vecteur via précisément une action de groupe.

Définition 2.1. Un espace affine est la donnée d'un ensemble non-vide $\mathscr{E}$, d'un espace vectoriel E et d'une action $*$ (à droite) de E sur $\mathscr{E}$ qui vérifie la condition suivante :

$$\forall M, N \in \mathscr{E} \quad \exists! u \in E \text{ tel que } N = M * u. \tag{20}$$

Terminologie :

- L'espace vectoriel E est appelé la direction de l'espace affine ou espace vectoriel sous-jacent.
- On notera aussi $\vec{MN}$ l'unique vecteur u tel que $N = M * u$.
- La **dimension d'un espace affine** $(E, \mathscr{E}, *)$ est la dimension de l'espace vectoriel E.

Notons que cette définition a du sens avec n'importe quel corps de base $\mathbb{K}$. Même si dans la suite nous allons nous concentrer sur le cas $\mathbb{K} = \mathbb{R}$.

On notera simplement souvent $\mathscr{E}$ un espace affine (en sous-entendant donc la donnée de E et $*$).

Il faut comprendre $u = \vec{MN}$ comme *le* vecteur entre les points M et N et la définition dit alors qu'entre deux points il existe un unique vecteur (au sens vu au collège/lycée) et que l'ensemble de tous ces vecteurs a naturellement la structure d'un espace vectoriel (addition et action du corps de base donc). Cf figure (5)

Il est important de comprendre pourquoi la définition ci-dessus encode bien l'idée que nous avons donné. D'une part, comme on vient de le dire, l'existence et l'unicité du u dans la condition (20), dit précisément que 2 points définissent bien un (et un seul) vecteur bien précis. D'autre part, le fait qu'on ait une action dit que tout vecteur donne un moyen de déplacer un point sur une autre. Précisément, l'action dit que le vecteur $\vec{MN}$ est précisément le vecteur qui fait passer du point M au point N.

L'exemple suivant est l'exemple fondamental (auquel tous les exemples peuvent se ramener par une bijection affine). C'est l'exemple sur lequel vous devez vous concentrer.

Exemple 2.2 (*Structure canonique d'espace affine sur un espace vectoriel).* Pour tout espace vectoriel E, on a un espace affine canonique $(E, E, +)$ où l'action est simplement l'addition

de E sur lui-même. Autrement dit, on définit pour $M \in E$, $u \in E$, l'action $E \times E \to E$ par

$$M * u := M + u \in E.$$

Exercice 2.3. Vérifier que $(E, E, +)$ est bien un espace affine.

En particulier en prenant $E = \mathbb{K}^n$, on a donc une structure canonique d'espace affine sur $\mathbb{K}^n$. Il faut prendre conscience que si on regarde $E = \mathbb{K}^n$ comme un espace affine, on oublie le rôle particulier du point 0 dans $\mathbb{K}^n$ (vu comme espace affine).

Décryptons la structure affine canonique de $(\mathbb{K}^n, \mathbb{K}^n, +)$. Soit $M = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $N = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ deux points de $\mathbb{K}^n$ (écrits comme des vecteurs colonnes).

Si $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ est un vecteur, on a par définition de l'action que

$$M * u = M + u = \begin{pmatrix} x_1 + u_1 \\ \vdots \\ x_n + u_n \end{pmatrix}$$

Le vecteur $\overrightarrow{MN}$ est donné par

$$\overrightarrow{MN} = N - M = \begin{pmatrix} y_1 - x_1 \\ \vdots \\ y_n - x_n \end{pmatrix}.$$

En effet, on a que ce vecteur est l'unique élément $\overrightarrow{MN}$ de $\mathbb{K}^n$ tel que $M * \overrightarrow{MN} = N$ ce qui veut dire que $M + \overrightarrow{MN} = N$ c'est à dire $\overrightarrow{MN} = N - M$.

Exemple 2.4. Le produit (cartésien) de 2 espaces affines $(\mathscr{E}, E, *_E)$, $(\mathscr{F}, F, *_F)$ est muni d'une structure d'espace affine de direction $E \times F$ et d'action $*_{E\times F} = *_E \times *_F$.

Remarque 2.5. Si on avait autorisé l'ensemble $\mathscr{E}$ à être vide dans la définition 2.1, l'ensemble vide $\emptyset$ pourrait être muni d'une structure d'espace affine de direction n'importe quel espace vectoriel et de dimension arbitraire. Ce qui est un peu contre-intuitif.

On a déj dit que l'action des vecteurs transporte les poitns en d'autres. En langage géométrique on dit "translate". Formalisons cela.

Définition 2.6. Soit $(\mathscr{E}, E, *)$ un espace affine. Soit $u \in E$, on appelle **translation de vecteur** u, l'application $t_u := \left\{ \begin{array}{ccc} \mathscr{E} & \to & \mathscr{E} \\ N & \mapsto & N * u \end{array} \right.$ donnée par l'action de u sur les éléments.

Exemple 2.7. En particulier, pour tout $M, N \in \mathscr{E}$ on a que $t_{\overrightarrow{MN}}(M) = M * \overrightarrow{MN} = N$.

Exemple 2.8. Prenons $\mathbb{K}^n$ muni de sa structure canonique d'espace affine. Et soit $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ un vecteur quelconque. Alors la translation t_u de vecteur u est l'application

$$M = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto M + u = \begin{pmatrix} x_1 + u_1 \\ \vdots \\ x_n + u_n \end{pmatrix}.$$

L'espace vectoriel E s'identifie en fait, y compris en tant que groupe, avec les translations. Précisément :

Lemme 2.9. *Soit $(\mathscr{E}, E, *)$ un espace affine. Le sous-ensemble* $\mathbf{Tran}(\mathscr{E})$ *des translations est un sous-groupe de* $\mathrm{Bij}(\mathscr{E})$. *L'application $u \mapsto t_u$ est un isomorphisme de groupes entre $(E, +)$ et $(\mathbf{Tran}(\mathscr{E}), \circ)$. En particulier,* $\mathbf{Tran}(\mathscr{E})$ *est abélien.*

Cet isomorphisme est appelé l'isomorphisme canonique entre translations et espace vectoriel sous-jacent de $\mathscr{E}$.

On en déduit (puisque t est un morphisme de groupes) que pour tout $M, N \in \mathscr{E}$,

$$(t_{\overrightarrow{MN}})^{-1} = t_{-\overrightarrow{MN}} = t_{\overrightarrow{NM}}. \tag{21}$$

Démonstration. Par définition $\mathbf{Tran}(\mathscr{E}) = \mathrm{Im}(t)$. Il reste à voir que les translations sont bien bijectives, qu'elles forment un sous-groupe et que t est un morphisme de groupes injectif.

Le point clé sera l'existence et l'unicité du vecteur $u = \overrightarrow{MN} \in E$ tel que $N = M * u$ pour deux points $M, N \in \mathscr{E}$. Par définition d'une action $t_0(M) = M * 0 = M$ car 0 est le neutre de E. Il suit que $t_0 = \mathrm{id}$ et donc $\mathrm{id} \in \mathbf{Tran}(\mathscr{E})$.

Pour montrer que t_u est une bijection, on va exhiber son inverse. En effet,

$$\begin{aligned} t_{-u}(t_u(M)) = (M * u) * (-u) &= M * (u - u) \text{ car } * \text{ est ue action} \\ &= M * 0 = M \text{ car 0 est neutre et } * \text{ une action} \\ &= = M * (-u + u) = t_u(t_{-u}(M)) \end{aligned}$$

par le même raisonement. Ceci montre que t_{-u} est l'inverse de t_u et que ce dernier est donc bijectif en particulier. Et que donc l'inverse de t_u est t_{-u} qui est bien dans $\mathbf{Tran}(\mathscr{E})$.

Montrons la stabilité par composition : on doit montrer que $t_u \circ t_v$ est une transposition. On va montrer que en fait $t_u \circ t_v = t_{u+v}$. Cela revient à montrer que pour tout $M \in \mathscr{E}$, on a $t_u \circ t_v(M) = t_{u+v}(M)$. Or

$$t_u \circ t_v(M) = t_u(M * v) = (M * v) * u = M * (v + u) \text{ (par propriété d'une action).}$$

Or $v + u = u + v$ par commutativité de l'addition dans un espace vectoriel. Et donc $M * (v + u) = M * (u + v) = t_{u+v}(M)$ ce qui conclut.

On a donc bien montré que $\mathbf{Tran}(\mathscr{E})$ est un sous-groupe.

On a par ailleurs vu que $u \mapsto t_u$ est un morphisme de groupes en montrant la stabilité par composition.

Montrons l'injectivité. On a que $\ker(u \mapsto t_u))\{v \in E,\, t_v = \mathrm{id}\}$. Mais si on a $t_v(M) = M$ alors $M * v = M = M * 0$ et par unicité du vecteur dans la définition d'un espace affine, $v = 0$. Ce qui conclut. □

Exemple 2.10. En particulier, pour tout $M, N \in \mathscr{E}$ on a que $t_{\overrightarrow{MN}}(M) = M * \overrightarrow{MN} = N$ et $t_{-\overrightarrow{MN}}(N) = t_{\overrightarrow{NM}}(N) = M$.

On a quelques propriété bien connues (et on peut vérifier que cette construction vérifie tous les axiomes de la géométrie au sens de Euclide et du collège/lycée) :

Proposition 2.11. *Soit $\mathscr{E}$ un espace affine.*

Relation de Chasles: *Soit M, N, P trois points d'un espace affine. Alors $\vec{MP} = \vec{MN} + \vec{NP}$*
Identité du parallélogramme: *Soient $A, B, C, D \in \mathscr{E}$. On a*

$$\vec{AB} = \vec{DC} \iff \vec{AD} = \vec{BC}.$$

Un quadrilatère vérifiant l'identité du parallèlogramme s'appelle évidemment un *parallélogramme*... On laisse en exercice de vérifier pourquoi et de faire des dessins.

Démonstration. On a par définition que $N = M * \vec{MN}$ et $P = N * \vec{NP}$. Par définition d'un action on obtient $P = N * \vec{NP} = (M * \vec{MN}) * \vec{NP} = M * (\vec{MN} + \vec{NP})$. Par unicité d'un vecteur envoyant un point sur un autre, on obtient que $\vec{MN} + \vec{NP} = \vec{MP}$.

La deuxième identité suit de la première et de la considération des égalités

$$\vec{AB} + \vec{BC} = \vec{AC} = \vec{AD} + \vec{DC}.$$

Si $\vec{AB} = \vec{DC}$, alors l'identité se simplifie en $\vec{AD} = \vec{BC}$ et réciproquement. Voir la figure (5) qui est plus parlante que cette preuve ! □

Remarque 2.12 (Terminologie générale). La propriété (20) que vérifie l'action de E sur $\mathscr{E}$ dit deux choses en même temps :

(1) Il y a une seule orbite (c'est à dire classe d'équivalence). En effet, deux points sont toujours reliés par l'action d'un élément de E.
(2) Le stabilisateur de tout $x \in \mathscr{E}$ est trivial $\text{stab}_x = \{0\}$. Cela découle de l'unicité. En effet si $x * u = x$, alors comme $x * 0 = x$ (par définition d'une action), par unicité $u = 0$.

Soit G un groupe agissant sur X. On dit que l'**action est transitive** si il vérifie la condition 1, à savoir qu'il n'y a qu'une seule orbite.

On dit que l'**action est libre** si il vérifie la deuxième, à savoir que les stabilisateurs sont tous triviaux.

Autrement dit l'action de E sur $\mathscr{E}$ est donc à la fois libre et transitive. Ce type de propriétés apparaît souvent lorsque l'on définit des géométries via des groupes.

Exemple 2.13. L'action de $GL_n(\mathbb{R})$ sur $\mathbb{R}^n \setminus \{0\}$ est évidemment transitive. Mais elle n'est pas libre.

En revanche l'action d'un sous-groupe H sur un groupe est libre mais pas transitive (sauf si le sous-groupe est le groupe tout entier).

2.2. **Sous-espaces affines.** Précisons maintenant les sous-espaces affines et donc les notions de droites, plans affines etc...

Définition 2.14. Soit $(\mathscr{E}, E, *)$ un espace vectoriel. Un sous-ensemble $\mathscr{F}$ de $\mathscr{E}$ est un sous-espace affine si il existe un point $x_0 \in \mathscr{E}$ et un sous-espace vectoriel F de E tels que

$$\mathscr{F} = \{x_O * u,\ u \in F\}.$$

On notera $x_0 * F := \{x_O * u,\ u \in F\}$. En particulier $x_0 = x_0 * 0 \in \mathscr{F}$.

C'est à dire qu'un sous-espace affine est la donnée d'un point particulier et de tous les points qu'on obtient à partir de lui en faisant agir les vecteurs d'un sous-espace vectoriel donné.

Autrement pour définir un sous-espace affine il suffit d'un point et d'un sous-espace vectoriel de E (mais plusieurs points distincts peuvent définir le même sous-espace).

La première remarque est

Lemme 2.15. *Soient F et F' deux sus-espaces vectoriels de E. Et x, x' deux points de $\mathscr{E}$. Si $x * F = x' * F'$ alors on a*

- $F = F'$
- $x' \in x * F$ *et* $x \in x' * F$.

Autrement dit, si on se donne un sous-espace affine $\mathscr{F}$, *le sous-espace vectoriel F dans la définition est* ***uniquement*** *défini* (il n'y en a pas 2 différents qui marchent). Et par ailleurs si $\mathscr{F} = x_0 * F$ est un sous-espace affine, alors on a qu'il est aussi égal à $x * F$ pour tout autre point x dans $\mathscr{F}$.

Si on résume un sous-espace affine est donc équivalent à la donnée de n'importe quel point du sous-espace et d'un sous-espace vectoriel F.

Terminologie *: on appelle dimension d'un sous-espace affine la dimension du sous-espace vectoriel F (qui est unique par le lemme). Un sous-espace affine de dimension 1 est appelé droite affine, un sous-espace affine de dimension 2 est appelé plan affine, un point est un sous-espace de dimension* 0*. Etc...*

Preuve du lemme 2.15. On a par hypothèse que $x' \in x' * F' = x * F$, donc il existe $u \in F$ tel que $x' = x * u$, ce qui veut dire que $\vec{xx'} \in F$. Notons que le deuxième point est donc éjà prouvé. On en déduit que $x * F = x' * F$ comme suit : si $y \in x' * F$, alors il existe $v \in F$ tel que $y = x' * v = (x * \vec{xx'}) * v = x * (\vec{xx'} + v) \in x * F$ car $\vec{xx'} + v \in F$ puisque F est un sous-groupe. Cela donne l'inclusion $x' * F \subset x * F$ et par un raisonnement symmétrique on a aussi $x * F \subset x' * F$. Ce qui donne a conclusion par double inclusion.

Il suffit maintenant pour finir de montrer que $x' * F = x' * F'$ implique $F = F'$.

Soit $u \in F$. On a $y = x' * u \in x' * F$. Mais comme $x' * Fx' * F'$, on a que $x' * u = x' * u'$ avec $u' \in F'$. Par unicité dans la condition (20), on ene dduit $u = u'$ et donc $u \in F'$. Conclusion $F \subset F'$. Par un raisonement similaire, on trouve $F' \subset F$ ce qui donne l'égalité voulue ! □

Le lemme suivant est rassurant et sans surprise.

Lemme 2.16. *Si $\mathscr{F}$ est un sous-espace affine, alors $(\mathscr{F}, F, *)$ est un espace affine.*

Démonstration. On va utiliser que l'action de $F \subset E$ sur $\mathscr{E}$ se restreint à $\mathscr{F}$. Soit $M, N \in \Gamma_{x_0}(F)$. Alors, il existe $u, v \in F$ uniques tels que $M = x_0 * u$ et $N = x_0 * v$. Il suit que

$$N = x_0 * (u + v - u) = (x_0 * u) * (v - u) = M * (v - u).$$

Or $v - u \in F$ (c'est un sous-espace vectoriel). Donc il existe un élément $f := v - u$ dans F tel que $N = M * f$. Par ailleurs, cet élément est unique puisque c'est déjà le cas dans E. Cela montre que l'action de E restreinte à F donne une structure d'espace affine à l'ensemble $\Gamma_{x_0}(F)$. □

Exercice 2.17. Démontrer le dernier point.

Exemple 2.18. Une droite affine de $\mathbb{R}^2$ (vu comme espace affine) est l'ensemble des points $\{(x, y) \in \mathbb{R}^2,\ ax + by = c\}$ où $a, b, c \in \mathbb{R}$ sont des paramètres quelconques si ce n'est que $(a, b) \neq (0, 0)$.

Exemple 2.19. Un sous-espace vectoriel de E est évidemment un sous-espace affine de $(E, E, +)$, mais comme l'exemple précédent le montre, il y en a bien d'autres.

De même, si $f : E \to F$ est une application linéaire, alors, pour tout $v \in \mathrm{im}(f)$, l'image réciproque $f^{-1}(v)$ est un sous-espace affine de E. Mais ce n'est pas un sous-espace vectoriel sauf si $v = 0$.

Définition 2.20. Deux sous-espaces affines $\mathscr{F}, \mathscr{G}$ sont parallèles si ils ont la même direction.

Notons que dans cette définition, pour être parallèle, il faut être de même dimension. Une droite n'est donc pas parallèle à un plan. On peut évidemment étendre cette définition à des sous-espaces de dimensions différente, en assertant que la directin de l'un est un sous-espace vectoriel de l'autre mais nous ne le ferons pas. Et préférerons dans ce cas expliciter cette dernière phrase.

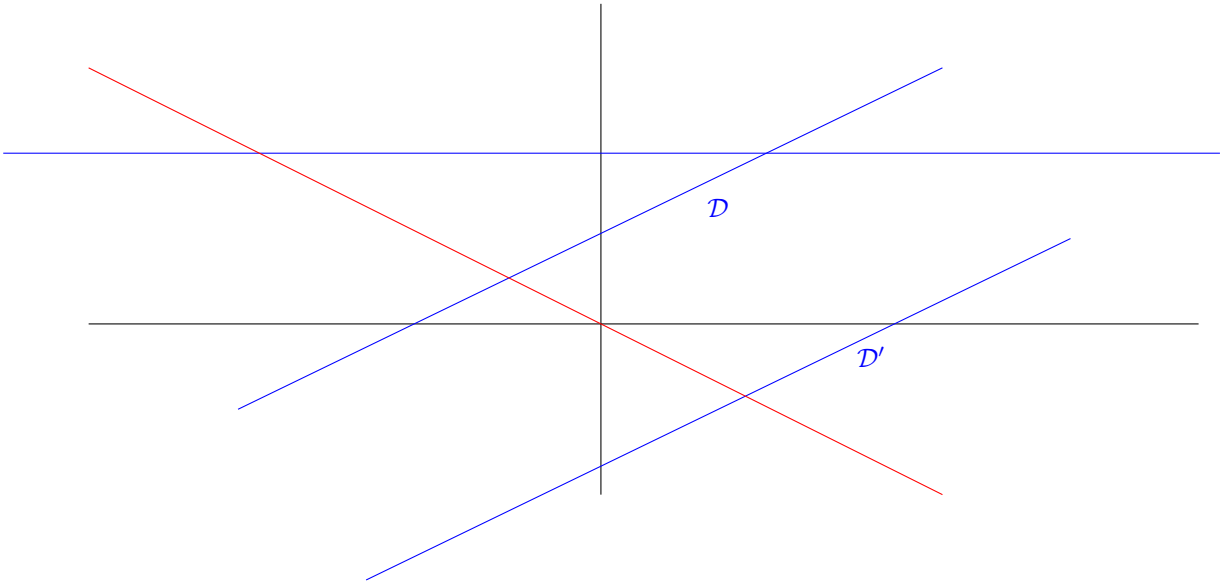


FIGURE 6. En bleu des droites affines non-vectorielles de $\mathbb{R}^2$. En rouge une droite vectorielle (en particulier affine). Les droites $\mathscr{D}$ et $\mathscr{D}'$ sont parallèles.

Lemme 2.21. *Le parallèlisme est une relation d'équivalence.*

Exercice 2.22. Démontrer le lemme.

Comme promis, précisons quelques propriétés géométriques qui sont effectivement vérifiées par les espaces affines (et qui montrent que ces derniers satisfont les axiomes d'Euclide).

Exemple 2.23.
- Pour tout point du plan affine et toute droite de ce plan il existe une unique paralèlle à la droite passant par le point.
- Si deux sous-espaces affines sont parallèles, alors ils sont soit confondus, soit leur intersection est vide (ils n'ont donc pas de points communs).

Nous laissons les démonstrations en exercice pour ceux qui veulent.

Exemple 2.24. Soit $f : E \to F$ une application linéaire. Alors $f^{-1}(u)//f^{-1}(v)$ quels que soient $u, v \in F$: leur direction est $\mathrm{Ker}(f)$.

2.3. **Choix d'une origine.** Comme annoncé, tout choix d'un point identifie (bijectivement) $\mathscr{E}$ avec son espace vectoriel sous-jacent E :

Lemme 2.25. *Pour tout point $x_0 \in \mathscr{E}$, l'application* $\Gamma_{x_0} : \left\{ \begin{array}{ccc} E & \to & \mathscr{E} \\ u & \mapsto & x_0 * u \end{array} \right.$ *est une bijection (qui envoie* 0 *sur x_0). Sa réciproque est l'application $x \mapsto \vec{x_0x}$.*

Il faut comprendre l'idée géométrique. Une fois fixé un point base x_0, pour tout point x, on a un le vecteur $\vec{x_0x}$, qui est l'unique vecteur qui fait passer de x_0 à x. On peut donc identifier x à ce vecteur et c'est exactement ce que fait la bijection donnée. Voir encore la figure (5). Voilà cette idée mise en preuve formelle.

Démonstration. Il suffit de vérifier que les applications sont bien réciproques l'une de l'autre. Notons pour cette preuve $\Phi_{x_0} : x \mapsto \vec{x_0x}$. Cette application est bien définie puisque ce vecteur $\vec{x_0x}$ est uniquement défini. On a alors que pour tout $u \in E$,

$$\Phi_{x_0} \circ \Gamma_{x_0}(u) = \Phi_{x_0}(x_0 * u) = u$$

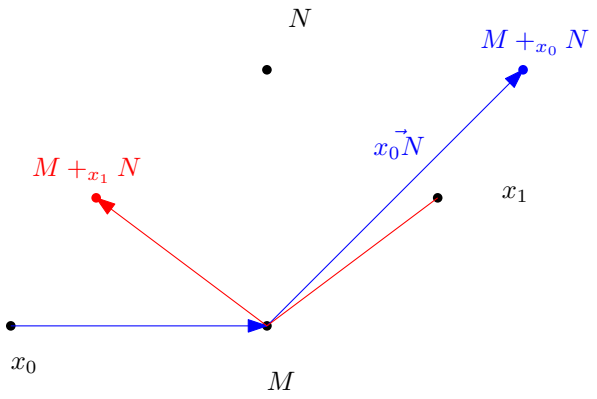


FIGURE 7. Deux choix d'origine différents x_0 et x_1 et deux exemples d'addition des points M et N via chacune de ces identifications. Qui sont à l'évidence très différentes.

car $u = x_0(\vec{x_0} * u)$ par la propriété d'unicité de l'action. De plus, pour tout $x \in \mathscr{E}$, on a

$$\Gamma_{x0} \circ \Phi(x) = \Gamma_{x_0}(\vec{x_0x}) = x$$

par définition. Ces applications sont bien inverses l'une de l'autre et donc bijectives. □

Une fois identifiés les points de $\mathscr{E}$ aux vecteurs de E par ce choix d'un point x_0, on peut maintenant les additioner comme dans E ou les multiplier par un scalaire. Cela s'appelle *transférer* la structure vectorielle de E via la bijection.

Définition 2.26. Soit $x_0 \in \mathscr{E}$. On munit $\mathscr{E}$ des opérations :

- pour tout $x, y \in \mathscr{E}$, $x +_{x_0} y = x_0 * \left(\vec{x_0x} + \vec{x_0y}\right)$;
- pour tout $\lambda \in \mathbb{K}$ et $x \in \mathscr{E}$, $\lambda *_{x_0} x = x_0 * \left(\lambda\vec{x_0x}\right)$.

Ici $\mathbb{K}$ est le corps au dessus duquel est défini la structure vectorielle de E. On conseille de faire des dessins ou regarder la figure (7).

Proposition 2.27. *Soit $(\mathscr{E}, E, *)$ un espace affine. Alors $(\mathscr{E}, +_{x_0}, *_{x_0})$ est un espace vectoriel de neutre x_0 et de plus Γ_{x_0} est un isomorphisme linéaire.*

Exercice 2.28. Démontrer cette proposition (indic : cela suit essentiellement du lemme précédent)

Remarque 2.29. Attention, cette structure d'espace vectoriel dépend du point x_0. Et il n'y en a pas si on ne fixe pas de point au préalable.

Lemme 2.30. *Pour tout $x \in \mathscr{E}$ et $F \subset E$, on a que*

$$\Gamma_x(F) = \{x * v,\ v \in F\}.$$

EN particulier, soit $\mathscr{F}$ un sous-ensemble d'un espace affine $(\mathscr{E}, E, *)$. Alors

(1) on a que $\mathscr{F}$ est un sous-espace affine si et seulement si il existe $x_0 \in \mathscr{F}$ et F un SEV de E tels que $\mathscr{F} = \Gamma_{x_0}(F)$.
(2) Si $\mathscr{F}$ est affine, alors le F du point précédent est exactement la direction de $\mathscr{F}$ et de plus pour tout $y \in \mathscr{F}$, on a que $\mathscr{F} = \Gamma_y(F)$.

Démonstration. Puisque un sous-espace affine $\mathscr{F}$ s'écrit sous la forme $\mathscr{F} = x * F$ où F est sa direction (unique) et x un poitn quelconque de $\mathscr{F}$, par le lemme 2.15 on a juste à montrer la première égalité : $\Gamma_x(F) = \{x * v,\ v \in F\} = x * F$. Ce qui est par définition car pour tout $v \in F$, $\Gamma_{x_0}(v) = x_0 * v$. □

2.4. **Applications affines et groupe affine.** Précisons maintenant les transformations entre espaces affines.

Essentiellement, il s'agit d'applications linéaires "à une translation de l'origine près". De manière générale, nous montrerons que les applications affines construites sont des généralisations de $x \mapsto ax + b$ (de $\mathbb{R}$ dans $\mathbb{R}$).

L'idée est qu'une application affine est une application qui va envoyer les vecteurs (entre deux points) sur des vecteurs de l'espace d'arrivé, linéairement.

Définition 2.31. Soit $(\mathscr{E}, E, *)$ et $(\mathscr{F}, F, *')$ deux espaces affines.

- Une application $f : \mathscr{E} \to \mathscr{F}$ est affine si il existe $x_0 \in \mathscr{E}$ et une application linéaire $\vec{f} : E \to F$ tels que, pour tout $x \in \mathscr{E}$, on ait

$$\vec{f}(\overrightarrow{x_0x}) = \overrightarrow{f(x_0)f(x)}. \tag{22}$$

- Un *isomorphisme affine* est une application affine qui est aussi une bijection.

En particulier une application affine est déterminée par l'image d'un point et une application linéaire par la formule, valable pour tout $x \in \mathscr{E}$,

$$f(x) = f(x_0) * \vec{f}(\overrightarrow{x_0x}). \tag{23}$$

En prenant $x = x_0 * \vec{u}$ on obtient que la formule (22) est équivalente [28] à

$$\vec{f}(\vec{u}) = \overrightarrow{f(x_0)f(x_0 * \vec{u})}. \tag{24}$$

Notons que cette formule définit la fonction $\vec{f}$ à partir de f.

On conseille de regarder les notes manuscrites du cours et/ou de faire des dessins pour comprendre cette formule finalement assez simple : une application affine s'obtient en prenant à parti d'un point x_0 et son image $f(x_0)$ l'application envoyant un point M sur le point obtenu à partir de $f(x_0)$ en appliquant l'image par $\vec{f}$ du vecteur $\vec{x_0M}$.

Lemme 2.32. *Soit $\vec{f}$ une application linéaire et $x_0 \in \mathscr{E}$ tels que pour tout $x \in \mathscr{E}$, on ait $\vec{f}(\overrightarrow{x_0x}) = \overrightarrow{f(x_0)f(x)}$.*

Alors pour tout point $x_0' \in \mathscr{E}$ et tout $x \in \mathscr{E}$, on a

$$\vec{f}(\overrightarrow{x_0'x}) = \overrightarrow{f(x_0')f(x)}.$$

Démonstration. On écrit simplement $x_0' = x_0 * \overrightarrow{x_0x_0'}$. Alors, pour tout $x \in \mathscr{E}$, on a $x_0' * \overrightarrow{x_0'x} = x = x_0 * \overrightarrow{x_0x}$.

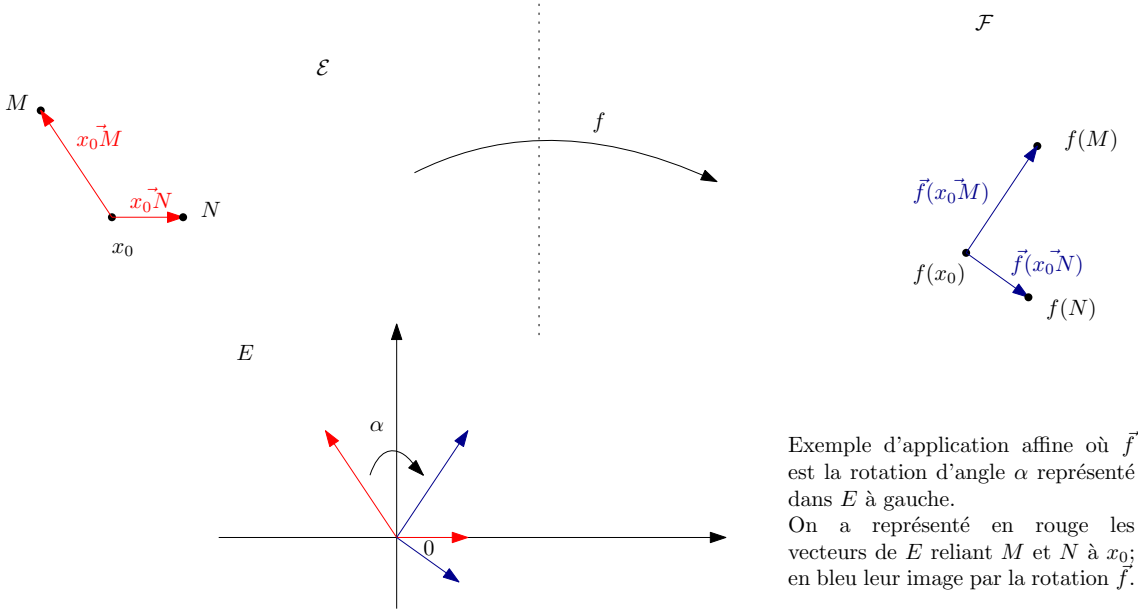
Nous devons montrer que $\vec{f}(\vec{x_0'x}) = \overrightarrow{f(x_0')f(x)}$, autrement dit (encore et toujours par unicité dans la condition sur l'action de E sur $\mathscr{E}$) que $f(x_0') * \vec{f}(\vec{x_0'x}) = f(x_0') * \overrightarrow{f(x_0')f(x)}$. Or $f(x_0') * \overrightarrow{f(x_0')f(x)} = f(x)$. Donc on doit montrer que $f(x_0') * \vec{f}(\vec{x_0'x}) = f(x)$. Par hypothèse sur x_0, on a

$$f(x_0') * \vec{f}(\vec{x_0'x}) = \big(f(x_0) * \vec{f}(\overrightarrow{x_0x_0'})\big) * \vec{f}(\overrightarrow{x_0'x}) = f(x_0) * \big(\vec{x_0x_0'} + \vec{f}(\vec{x_0'x}\big) = f(x_0) * \vec{f}(\vec{x_0x_0'} + \vec{x_0'x})$$

car $\vec{f}$ est linéaire. Comme $\overrightarrow{x_0x_0'} + \overrightarrow{x_0'x} = \overrightarrow{x_0x}$ par Chasle et que $f(x) = f(x_0) * \vec{f}(\vec{x_0x})$, on en déduit le résultat.

□

28. car par définition $\overrightarrow{x_0(x_0 * u)} = u$.



Exemple d'application affine où $\vec{f}$ est la rotation d'angle α représenté dans E à gauche.
On a représenté en rouge les vecteurs de E reliant M et N à x_0; en bleu leur image par la rotation $\vec{f}$.

FIGURE 8. Exemple d'application affine

Le lemme dit que être une application affine ne dépend *pas* du choix du point base que vous prenez (ce qui serait très étrange sinon).

En particulier, cela dit que l'application $\vec{f}$ définie par la formule (24) est indépendante du point x_0. On a donc bien une application $f \mapsto \vec{f}$ de l'ensemble des applications affines vers les applications linéaires.

Remarque 2.33 (**Comment vérifier qu'une application est affine ?**). D'après la formule donnée et le lemme 2.32, pour voir si une application est affine il suffit de prendre n'importe quel point x_0 et de vérifier si l'application

$$u \longmapsto \vec{f}(\vec{u}) := \overrightarrow{f(x_0)f(x_0 * \vec{u})}$$

est linéaire de E dans F.

Donc ***pour tester si une application $f : \mathscr{E} \to \mathscr{F}$ est affine, il suffit de voir si la formule $\vec{f}(u) = \overrightarrow{f(x_0)f(x_0 * u)}$ définit bien une application linéaire*** et ceci en prenant x_0 n'importe quel point..

À retenir : *une application affine est donc la donnée de l'image $f(x_0)$ d'un point x_0 et une application linéaire $\vec{f} : E \to E$ telle que $f(M) = f(x_0) * \vec{f}(\overrightarrow{x_0M})$. Autrement dit qu'on calcule l'image de M en appliquant le vecteur $\vec{f}(\overrightarrow{x_0M})$ à $f(x_0)$. Ce qui signifie concrètement : en translatant $f(x_0)$ par le vecteur (dépendant de $\vec{f}$) $\vec{f}(\overrightarrow{x_0M})$.* Voir la figure (8).

Exemple 2.34. Soit E un espace vectoriel vu comme espace affine. Une application linéaire $f : E \to E$ est affine et $\vec{f} = f$. En effet, l'action de E sur lui même étant par addition, on a que pour tout $x, y \in E$, que le vecteur

$$\vec{xy} = y - x$$

ce qui découle de la formule $y = x + (y - x)$. Il suit que, pour tout $u \in E$, on a

$$\overrightarrow{f(x_0)f(x_0 + u)} = (f(x_0) + f(u)) - f(x_0) = f(u).$$

De plus, une application affine $f : E \to E$ est une application linéaire si et seulement si $f(0) = 0$

Exercice 2.35. Démontrer la dernière affirmation.

Exemple 2.36 (**applications affines dans $\mathbb{K}^n$**). Voici l'exemple le plus important d'applications affines dans ce cours. Considérons les espaces $\mathbb{K}^\ell$ avec leurs structures canoniques d'espace affine ($\ell \geq 0$) . On identifie un point de $\mathbb{K}^\ell$ avec un vecteur colonnne $X = \begin{pmatrix} x_1 \\ \vdots \\ x_\ell \end{pmatrix}$.

Proposition 2.37. *Alors une application $\mathbb{K}^n$ dans $\mathbb{K}^m$ est affine si et seulement si elle s'écrit sous la forme*

$$X \longmapsto MX + B$$

où $M \in M_{m,n}(\mathbb{K})$ est une matrice et $B \in \mathbb{K}^m$ est un vecteur quelconque.

En particulier, une application affine s'écrit de manière unique comme la composée d'une application linéaire (ici $X \mapsto MX$) et d'une translation (de vecteur $B = f(0)$).

Démonstration. On part de la définition d'une application affine $f : \mathbb{K}^n \to \mathbb{K}^n$. On rappelle que le vecteur $\overrightarrow{XY}$ est égal à $Y - X$; en particulier $\overrightarrow{OX} = X$. En appliquant l'égalité (24) en $x_0 = 0$, on a pour tout $X \in \mathbb{K}^n$ que

$$f(X) = f(0) * \vec{f}(\overrightarrow{0X}) = f(0) + \vec{f}(X).$$

Comme $\vec{f}$ est linéaire, il existe une *unique* matrice M telle que $\vec{f}(X) = MX$. En notant $B = f(0)$ on obtient bien $f(X) = MX + B$. On peut noter que $B = f(0)$ est forcé par la définition. Cette écriture est donc unique.

Par ailleurs, l'application $f(X) = MX + B$ est la composée de la translation $t_B : X \mapsto X + B$ avec l'application linéaire $\vec{f} : X \mapsto MX$. L'écriutre est unique car M est donnée par $\vec{f}$ et $B = f(0)$ sont complétement déterminés par f. □

Remarque 2.38. Soit x_0 un point d'un espace affine (resp.euclidien) $\mathscr{E}$. Au vu de l'exemple 2.34 précédent, l'isomorphisme Γ_{x_0} (lemme 2.25) envoie une application linéaire $f : E \to E$, sur une application affine : précisément, l'application $\vec{f} \mapsto \left(x \mapsto x_0 * \left(\vec{f}(\overrightarrow{x_0 x})\right)\right)$ de $\mathscr{E}$ dans lui-même est affine. Son image est exactement l'ensemble des applications affines $f : \mathscr{E} \to \mathscr{E}$ telles que $f(x_0) = x_0$, c'est à dire qui laissent fixe x_0.

On prendra garde en revanche, que dans le cas d'un espace affine général, pour qu'une application linéaire définisse une application affine, il faut encore une fois choisir un point base. Dans l'exemple 2.34 on avait 0 comme point base canonique.

Exercice 2.39. Démontrer la remarque si le coeur et le temps vous en disent.

Définition 2.40. On note $\mathbf{Aff}(\mathscr{E})$ l'ensemble des applications affines bijectives de $\mathscr{E}$ dans lui même.

C'est l'analogue du groupe linéaire $GL(E)$ pour les espaces vectoriels. Cf la propriété 3 ci-dessous.

Proposition 2.41. *Soit $f : \mathscr{E} \to \mathscr{F}$ une application affine f.*

1. *On a que f est bijective si et seulement si l'application linéaire associée $\vec{f}$ l'est.*
2. *Si $g : \mathscr{F} \to \mathscr{G}$ est une autre application affine, alors $g \circ f$ est affine et $\overrightarrow{g \circ f} = \vec{g} \circ \vec{f}$.*
3. *L'inverse d'une application affine inversible f est affine et $\vec{f}^{-1} = \vec{f}^{-1}$. En particulier, $\mathbf{Aff}(\mathscr{E})$ est un sous-groupe de $(\mathrm{Bij}(\mathscr{E}), \circ)$.*

(4) *L'image d'un sous-espace affine par une application affine est un sous-espace affine. Ainsi une application affine envoie 3 points alignés en 3 points alignés*
(5) *L'image inverse d'une application affine est un sous-espace affine.*

Démonstration. Soit f affine et x_0, $\vec{f}$ comme dans la définition 2.1. On utilise l'égalité suivante, vraie pour tout $x \in \mathscr{E}$:

$$f(x) = f(x_0) * \vec{f}(\overrightarrow{x_0 x}).$$

Par ailleurs pour tout point $y \in \mathscr{F}$, il existe un unique $v \in F$ tel que $y = f(x_0) * v$ (par définition d'un espace affine).

(1) Montrons le point 1. En particulier, si f est surjective, alors pour tout $v \in F$, il existe x tel que $f(x_0) * v = f(x)$ et par unicité, $v = \vec{f}(\overrightarrow{x_0 x})$ ce qui montre que $\vec{f}$ est surjective. Réciproquement, si $\vec{f}$ est surjective, pour tout $y \in \mathscr{F}$, il existe $u \in E$ tel que $\vec{f}(u) = v$ et il suit que $f(x_0 * u) = f(x_0) * \vec{f}(u) = f(x_0) * v = y$; d'onc f est surjective.

On a montré que f est surjective si et seulement si $\vec{f}$ l'est.

Pour l'injectivité ; supposons que f est injective. Alors, pour tout $u, v \in E$, si $\vec{f}(u) = \vec{f}(v)$, on a que $f(x_0) * \vec{f}(u) = f(x_0) * \vec{f}(v)$ et donc $f(x_0 * u) = f(x_0 * v)$ (par définition d'une application affine) ce qui implique par injectivité de f que $x_0 * u = x_0 * v$ et donc $u = v$. On a bien que $\vec{f}$ est injective. La réciproque se démontre de la même manière : soit $M, N \in \mathscr{E}$. Si $f(M) = f(N)$, alors $f(x_0) * \vec{f}(\overrightarrow{x_0 M}) = f(x_0) * \vec{f}(\overrightarrow{x_0 N})$ et par unicité, on a $\vec{f}(\overrightarrow{x_0 M}) = \vec{f}(\overrightarrow{x_0 N})$. Par injectivité de $\vec{f}$, on obtient $\overrightarrow{x_0 M} = \overrightarrow{x_0 N}$ et donc $N = M$.

(2) Passons au deuxième point. Il suffit de prendre $x_0 \in \mathscr{E}$ quelconque. On a que pour tout $u \in E$,

$$\begin{aligned}
\overrightarrow{g \circ f(x_0) g \circ f(x_0 * u)} &= \overrightarrow{g(f(x_0)) g(f(x_0 * u))} \\
&= \overrightarrow{g(f(x_0)) g(f(x_0) * \vec{f}(u))} \text{ (car } f \text{ est affine)} \\
&= g(f(x_0) * \vec{g}(\vec{f}(u)) \text{ (car } g \text{ est affine)} \\
&= g(f(x_0) * \vec{g} \circ \vec{f}(u)
\end{aligned}$$

Comme $\vec{g} \circ \vec{f}$ est linéaire (composée d'applications linéaires) cela nous done immédiatement que $g \circ f$ est affine et que $\overrightarrow{g \circ f} = \vec{g} \circ \vec{f}$.

(3) On utilise que l'inverse d'une application linéaire est linéaire. Et de plus on a que $f^{-1}(y) = x \Leftrightarrow y = f(x)$ d'où, en notant $x_0 = f^{-1}(y_0)$, on a que

$$\overrightarrow{y_0 y} = \overrightarrow{f(x_0)\, f(x)} = \vec{f}(\overrightarrow{x_0 x}) \iff \vec{f}^{-1}(\overrightarrow{y_0 y}) = \overrightarrow{x_0 x} = \overrightarrow{f^{-1}(y_0)\, f^{-1}(y)}$$

en appliquant l'inverse de $\vec{f}$. Comme $\vec{f}^{-1}$ est bien linéaire, on en déduit que f^{-1} est bien affine et l'identité $\vec{f^{-1}} = \vec{f}^{-1}$. Cette propriété, al précédente et le fait que id est une bijection affine nous donne que $\mathbf{Aff}(\mathscr{E})$ est un sous-groupe.

(4) Soit $\mathscr{F} = x * F$ un sous-espace affine. Alors $f(\mathscr{F}) = f(x_0) * \vec{f}(F)$ d'après la formule (23). Comme l'image d'un sous-espace vectoriel par une application linéaire est un sous-espace vectoriel, on conclut.
(5) Se démontre de même.

□

2.5. **Structure des groupes affines.** Le groupe affine $\mathbf{Aff}(\mathscr{E})$ est plus gros que le groupe linéaire, mais la différence est facile à comprendre. Elle est précisément déterminée par les translations.

Proposition 2.42. *L'application*

$$\begin{array}{ccc} \mathbf{Aff}(\mathscr{E}) & \to & GL(E) \\ f & \mapsto & \vec{f} \end{array}$$

est un morphisme de groupes surjectif dont le noyau est le groupe $\mathbf{Tran}(\mathscr{E})$ *des translations de* $\mathscr{E}$.

Démonstration. On a déjà vu dans la remarque 2.33 que $f \mapsto \vec{f}$ est bien définie. Montrer que c'est un morphisme de groupes revient à montrer que $\overrightarrow{g \circ f} = \vec{g} \circ \vec{f}$ ce qui est contenu dans le proposition 2.41.

Calculons le noyau de ce morphisme de groupes. Soit $x_0 \in \mathscr{E}$. Si $\vec{f} = \mathrm{id}$, alors pour tout M dans $\mathscr{E}$, on a

$$f(M) = f(x_0) * \vec{f}(\overrightarrow{x_0M}) = f(x_0) * \overrightarrow{x_0M} = (x_0 * \overrightarrow{x_0f(x_0)}) * \overrightarrow{x_0M} = x_0 * (\overrightarrow{x_0M} + \overrightarrow{x_0f(x_0)}).$$

Ainsi $f(M) = M * \overrightarrow{x_0f(x_0)} = t_{\overrightarrow{x_0f(x_0)}}(M)$. Par suite, f est la translation de vecteur $\overrightarrow{x_0f(x_0)}$. Réciproquement, en remontant ce calcul on obtient bien qu'une translation est dans le noyau. Par double inclusion on a bien démontré que le noyau est égal à $\mathbf{Tran}(\mathscr{E})$.

Pour la surjectivité, considérons $\varphi \in GL(E)$. Soit $x_0 \in \mathscr{E}$. L'application

$$\gamma_{x_0}(\varphi) : \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E} \\ M & \mapsto & x_0 * \varphi(\overrightarrow{x_0M}) \end{array} \tag{25}$$

est affine car φ est linéaire. En effet

$$\overrightarrow{\gamma_{x_0}(\varphi)}(u) = \overrightarrow{x_0(x_0 * \varphi(u))} = \varphi(u).$$

Cette formule nous montre de plus que $\overrightarrow{\gamma_{x_0}(\varphi)} = \varphi$ et on a trouvé un antécédent de φ. □

Remarque 2.43. Le théorème implique que les translations sont un sous-groupe normal de $\mathbf{Aff}(\mathscr{E})$.

Exercice 2.44. Démontrer cette affirmation.

Remarque 2.45. On a vu que le groupe $\mathbf{Tran}(\mathscr{E})$ est isomorphe au groupe additif de E, il est donc abélien contrairement à $GL(E)$ et $\mathbf{Aff}(E)$.

En pratique le théorème permet de comprendre les applications affines en utilisant les translations (qui sont très simples) et les applications linéaires (pour lesquelles on a tous les outils de l'algèbre linéaire). La raison est que l'on peut, une fois choisi un point base x_0, identifier $GL(E)$ avec un sous-groupe de $\mathbf{Aff}(E)$.

On a déjà vu cela à l'oeuvre dans l'exemple 2.36

Pour tout choix $x_0 \in \mathscr{E}$, on a obtenu une structure d'espace vectoriel sur $\mathscr{E}$ et un isomorphisme linéaire $\Gamma_{x_0}^{-1} : E \xrightarrow{\sim} \mathscr{E}$.

Notation 2.46. On note $GL_{x_0}(\mathscr{E})$ le groupe linéaire de $\mathscr{E}$ muni de cette structure d'espace vectoriel.

Lemme 2.47. *Soit* $x_0 \in \mathscr{E}$.

- *on a que* $GL_{x_0}(\mathscr{E})$ *est un sous-groupe de* $\mathbf{Aff}(\mathscr{E})$. *Il est égal à l'ensemble des* $f \in \mathbf{Aff}(\mathscr{E})$ *tels que* $f(x_0) = x_0$.

- *L'application* $\varphi \mapsto \Gamma_{x_0}^{-1} \circ \varphi \circ \Gamma_{x_0}$ *est un isomorphisme de groupes* $GL(E) \to GL_{x_0}(\mathscr{E})$. *De plus, on a* $\overrightarrow{\Gamma_{x_0}^{-1} \circ \varphi \circ \Gamma_{x_0}} = \varphi$.

Exercice 2.48. Démontrer ce lemme.

Le lemme permet d'identifier $GL(E)$ et $GL_{x_0}(\mathscr{E})$, donc $GL(E)$ avec un sous-groupe de $\mathbf{Aff}(\mathscr{E})$ et c'est ce qu'on fera dans la suite de cette partie.

Remarque 2.49. On peut remarquer que $GL(E)$ et $GL_{x_0}(\mathscr{E})$ sont en quelque sorte conjugués.

Définition 2.50. Pour $f \in \mathbf{Aff}(\mathscr{E})$, on notera $\overrightarrow{f}_{x_0}$ la composée $\mathbf{Aff}(\mathscr{E}) \to GL(E) \xrightarrow{\simeq} GL_{x_0}(\mathscr{E})$.

Autrement dit, $\overrightarrow{f}_{x_0}$ est l'application linéaire associée à f, vue dans $GL_{x_0}(\mathscr{E})$, donnée pour $x \in \mathscr{E}$ par

$$\overrightarrow{f}_{x_0}(x) = x_0 * \overrightarrow{f}(\overrightarrow{x_0x}). \tag{26}$$

Par exemple si $\mathscr{E} = \mathbb{K}^n$ et que l'on choisit 0 comme origine, $\overrightarrow{f}_0 = \overrightarrow{f}$.

Exercice 2.51. Démontrer la formule (2.50).

On peut énoncer le théorème clé de cette partie qui est la version générale de la proposition 2.37.

Théorème 2.52. *Soit* $(\mathscr{E}, E, *)$ *un espace affine et* $x_0 \in \mathscr{E}$.

- *Toute bijection affine* $f \in \mathbf{Aff}(\mathscr{E})$ *s'écrit de manière* **unique** *sous la forme*
$$f = t \circ \varphi$$
où t *est une translation et* $\varphi \in GL_{x_0}(\mathscr{E})$ *est linéaire.*
- *Toute bijection affine* $f \in \mathbf{Aff}(\mathscr{E})$ *s'écrit de manière* **unique** *sous la forme*
$$f = \psi \circ t'$$
où t' *est une translation et* $\psi \in GL_{x_0}(\mathscr{E})$ *est linéaire.*
- *Dans les deux cas précédents on a* $\varphi = \overrightarrow{f}_{x_0} = \psi$.

La proposition dit donc que toute bijection affine est la composition d'une translation et d'une bijection linéaire. **Il faut faire attention que les translations ne commutent PAS avec les applications linéaires de** GL_{x_0} **en général**.

Ce théorème généralise l'exemple 2.36.

Il est important de bien comprendre la preuve de 2.37 avant de lire la suivante qui en est simplement la réécriture dans le cadre d'une action plus générale.

Démonstration. Remarquons déjà que la troisième assertion implique l'unicité (mais pas l'existence) dans les deux premières assertions. En effet : si on a une décomposition $f = t \circ \varphi$ alors $t = f \circ \varphi^{-1}$ et donc si $\varphi = \overrightarrow{f}_{x_0}$, alors nécessairement $t = f \circ \overrightarrow{f}_{x_0}^{-1}$ et donc le couple (t, φ) est unique, égal à $(f \circ \overrightarrow{f}_{x_0}^{-1}, \overrightarrow{f}_{x_0})$.

Nous démontrons maintenant l'existence dans la première assertion. La deuxième se fait de manière similaire.

Puisque f est affine, pour $x_0 \in \mathscr{E}$ quelconque, on a, pour tout $M \in \mathscr{E}$,

$$\begin{aligned} f(M) = f(x_0) * \overrightarrow{f}(\overrightarrow{x_0M}) &= x_0 * \left(\overrightarrow{x_0f(x_0)} + \overrightarrow{f}(\overrightarrow{x_0M})\right) \text{ (car } * \text{ est une action)} \\ &= (x_0 * \overrightarrow{f}(\overrightarrow{x_0M})) * (\overrightarrow{x_0f(x_0)}) = \overrightarrow{f}_{x_0}(M) * (\overrightarrow{x_0f(x_0)}) \text{ (par le lemme 26)} \\ &= t_{\overrightarrow{x_0f(x_0)}}(\overrightarrow{f}_{x_0}(M)) \end{aligned}$$

par définition d'un translation. On a donc montré que $f = t_{\overrightarrow{x_0 f(x_0)}} \circ \vec{f}_{x_0}$. Ce qui donne l'existence de la décomposition comme voulu. Et par ailleurs, nous voyons que la translation t est juste la translation de vecteur $\overrightarrow{x_0 f(x_0)}$.

Montrons enfin la troisième assertion.

Il suffit d'appliquer la composition $\mathbf{Aff}(\mathscr{E}) \to GL(E) \to GL_{x_0}(E)$ de la définition 2.50. En effet, c'est une composition de morphismes de groupes comme on l'a vu. Et par ailleurs $\overrightarrow{t \circ \varphi} = \vec{t} \circ \vec{\varphi} = \vec{\varphi}$ car les translations sont dans le noyau de $f \mapsto \vec{f}$. Ainsi on a que $f = t \circ \varphi$, alors $\vec{f}_{x_0} = \vec{\varphi}_{x_0}$.

Or on a $\vec{\varphi}_{x_0} = \varphi$. En effet, cela provient du lemme 26 qui nous donne que

$$\vec{\varphi}_{x_0}(M) = x_0 * (\vec{\varphi}(\overrightarrow{x_0 M}) = \varphi(x_0) * (\vec{\varphi}(\overrightarrow{x_0 M}) = \varphi(M)$$

car $\varphi \in GL_{x_0}(\mathscr{E})$ et donc $\varphi(x_0) = x_0$. □

Remarque 2.53. La proposition 2.52 s'étend à toutes les applications affines mais ce n'est pas notre centre d'intérêt.

Remarque 2.54. Si $\mathscr{E}$ est euclidien, l'application $\vec{f}_{x_0}$ est une isométrie linéaire. Et donc la proposition 2.52 est vraie avec les isométries et les espaces euclidiens.

Attention, les t et t' dans la proposition ne sont en revanche *pas* les mêmes en général. Cela se voit via le lemme suivant qui établit *la formule de commutation entre translations et applications linéaires* :

Lemme 2.55. *Soit $u \in E$ et $\vec{f}_{x_0} \in GL_{x_0}(E)$. On a*

$$\vec{f}_{x_0} \circ t_u = t_{\vec{f}_{x_0}(u)} \circ \vec{f}_{x_0}.$$

Quitte à composer par $\vec{f}_{x_0}^{-1}$, le lemme est équivalent à

$$t_{\vec{f}_{x_0}(u)} = f_{x_0} \circ t_u \circ \vec{f}_{x_0}^{-1}.$$

c'est à dire au fait que la conjuguée d'une translation est une translation. De plus deux translations de vecteur non-nul sont toujours conjuguées (car on peut toujours trouver une bijection linéaire entre deux vecteurs non-nuls)

Démonstration. Par définition, pour tout $M \in \mathscr{E}$, on a

$$\begin{aligned}
&\vec{f}_{x_0} \circ t_u(M) = \vec{f}_{x_0}(t_u(M)) \\
&= \vec{f}_{x_0}(M * u) = \vec{f}_{x_0}((x_0 * \overrightarrow{x_0 M}) * u) = \vec{f}_{x_0}(x_0 * (\overrightarrow{x_0 M} + u)) \text{ (puisque } * \text{ est une action)} \\
&\qquad = x_0 * \vec{f}_{x_0}(\overrightarrow{x_0 M} + u) = x_0 * (\vec{f}_{x_0}(\overrightarrow{x_0 M}) + \vec{f}_{x_0}(u)) \text{ (par linéarité)} \\
&= x_0 * (\vec{f}_{x_0}(t_{\vec{f}_{x_0}(u)}(\overrightarrow{x_0 M})) = \vec{f}_{x_0}(t_{\vec{f}_{x_0}(u)}(\overrightarrow{x_0 M})) \text{ (par définition des translations)} \\
&\qquad = \vec{f}_{x_0} \circ t_{\vec{f}_{x_0}(u)}(M).
\end{aligned}$$

On a prouvé le résultat. □

Cette relation de commutation donnée par le lemme permet de comprendre toute la structure du groupe $\mathbf{Aff}(\mathscr{E})$ en termes de translations et applications affines

Théorème 2.56. *Soit $(\mathscr{E}, E, *)$ un espace affine et $x_0 \in \mathscr{E}$.*

(1) L'ensemble $\mathbf{Tran}(\mathscr{E}) \times GL_{x_0}(\mathscr{E})$ *muni de la loi interne*

$$(t_u, \vec{f_1}) * (t_v, \vec{f_2}) = (t_{u+\vec{f_1}(v)}, \vec{f_1} \circ \vec{f_2}) \tag{27}$$

est un groupe.

(2) L'application $(t, \vec{f_{x_0}}) \mapsto t \circ \vec{f_{x_0}}$ *est un isomorphisme de groupe de* $\mathbf{Tran}(\mathscr{E}) \times GL_{x_0}(\mathscr{E})$ *sur* $\mathbf{Aff}(\mathscr{E})$.

La proposition dit donc que $\mathbf{Aff}(\mathscr{E})$ ressemble au groupe produit des translations et du groupe linéaire, si ce n'est que l'on doit modifier le produit dans les translations par l'action de f_1 sur t_v. Ce genre de constructions arrivent souvent en théorie des groupes et leurs applications. Cela s'appelle un *produit semi-direct*.

Remarque 2.57 (**cas de** $\mathbb{K}^n$**)**. Dans le cas de $\mathscr{E} = \mathbb{K}^n$ avec sa structure canonique, ce résultat exprime juste que la composée de $f_1(X) = M_1X + B_1$ avec $f_2(X) = M_2X + B_2$ est l'applciation

$$X \mapsto M_1M_2X + (B_1 + M_1B_2).$$

Preuve du théorème 2.56. La proposition 2.52 implique immédiatement que l'application $(t, \vec{f_{x_0}}) \mapsto t \circ \vec{f_{x_0}}$ est bijective (par existence et unicité).

Par ailleurs, on a

$$\left(t_u \circ \vec{f_1}\right) \circ \left(t_v \circ \vec{f_2}\right) = t_u \circ \left(\vec{f_1} \circ t_v\right) \circ \vec{f_2} = (t_u \circ t_{\vec{f_1}(v)}) \circ \vec{f_1} \circ \vec{f_2}$$

par le lemme 2.55. Ceci prouve que l'application est un morphisme de groupes modulo le fait qu'on a pas prouvé que la multiplication sur $\mathbf{Tran}(\mathscr{E}) \times GL_{x_0}(\mathscr{E})$. L'associativité découle du fait que la composition est associative, le neutre est $(\mathrm{id}, \vec{\mathrm{id}}_{x_0})$ et l'inverse d'un élément $(t_u, \vec{f})$ est $(t_{\vec{f}^{-1}(u)}, (\vec{f})^{-1})$. On laisse la vérification de ces affirmations en exercice.

□

Remarque 2.58. Notons que l'équation (29), au vu du lemme 2.55, se traduit par

$$(t, \vec{f_1}) * (t', \vec{f_2}) = (t \circ (\vec{f_1} \circ t \circ \vec{f_1}^{-1}, \vec{f_1} \circ \vec{f_2}).$$

La proposition 2.56 permet de comprendre les bijections affines en comprenant d'une part les translations, d'autre part les applications linéaires bijectives.

Remarque 2.59 (**Équvalence des espaces affines de même dimension finie)**. Terminons par une remarque analogue aux propriétés du cas linéaire.

Proposition 2.60. *Soit* $(\mathscr{E}, E, *)$ *et* $(\mathscr{F}, F, *)$ *deux espaces affines de même dimension. Alors il existe un isomorphisme affine entre eux.*

Si par ailleurs ils sont euclidiens, on peut même trouver une isométrie entre eux.

Autrement dit, à isomorphisme près, il n'y a qu'un espace affine de chaque dimension finie. En particulier, **tout espace affine de dimension** n **est isomorphe à** $\mathbb{K}^n$ **avec sa structure canonique.** Ce qui justifie que l'on peut s'occuper en première instance que de ces derniers espaces.

3. Isométries et Similitudes

On va maintenant rajouter la notion de distance entre des points dans un espace affine. Ce qui permet donc de faire des mesures et de définir des choses comme un carré ou triangle équilatéral.

Définition 3.1. Un espace affine sera dit préhilbertien (resp. euclidien) si son espace sous-jacent est en plus muni d'une structure préhilbertienne (resp. euclidienne). Autrement dit il s'agit de la donnée de $(\mathscr{E}, E, b, *)$ telle que $(\mathscr{E}, E, *)$ est affine et (E, b) préhilbertien (resp. euclidien). C'est à dire que $b : E \times E \to E$ est un produit scalaire sur E. On notera, pour $u \in E$, $\|u\| = \sqrt{b(u,u)}$ la norme associée.

Si $M, N \in \mathscr{E}$ sont des points, on appellera *distance de M à N* la norme $\|\overrightarrow{MN}\|$.

Notation 3.2. On notera aussi $d(M,N)$ pour la norme $\|\overrightarrow{MN}\|$.

Un espace affine de dimension finie peut toujours être munie d'une structure euclidienne d'après le cours d'Algèbre 4 (on remarquera que l'on a juste besoin de rajouter une structure à notre espace vectoriel sous-jacent).

On a donc maintenant une notion d'isométrie dans les espaces affines euclidien.

Définition 3.3. Soit $\mathscr{E}$ un espace affine euclidien (ou préhilbertien).

- Une **isométrie** de $\mathscr{E}$ est une application $f : \mathscr{E} \to \mathscr{E}$ telle que, pour tout M, $N \in \mathscr{E}$, on ait
$$\|\overrightarrow{f(M)f(N)}\| = \|\overrightarrow{MN}\|.$$
- Une **isométrie** affine de $\mathscr{E}$ est une isométrie qui est aussi une application affine.
- On note $\mathbf{Iso}(\mathscr{E})$ le sous-ensemble de $\mathbf{Aff}(\mathscr{E})$ des isométries affines bijectives.

Lemme 3.4. *Soit $\mathscr{E}$ un espace affine préhilbertien ou euclidien. Alors $\mathbf{Iso}(\mathscr{E})$ est un sous-groupe de $(\mathrm{Bij}(\mathscr{E}), \circ)$. De plus, les translations sont des isométries et $\mathbf{Trans}(\mathscr{E})$ un sous-groupe normal de $\mathbf{Iso}(\mathscr{E})$.*

Démonstration. Il est facile de vérifier que la fonction identité est une isométrie affine. La condition d'être une isométrie se lit, avec la notation 3.2,
$$d(f(M), f(N)) = d(M,N).$$
Si $f, g \in \mathbf{Iso}(\mathscr{E})$, alors, pour tout $x, y \in \mathscr{E}$, on a
$$d(f \circ g(x), f \circ g(y) = d(f(g(x)), f(g(y)) = d(g(x), g(y)) = d(x,y)$$
en appliquant successivement que f puis g sont des isométries. On a donc bien que $f \circ g$ est une isométrie.

Il reste à vérifier que si f est une isométrie, alors f^{-1} aussi. Soit $x, y \in \mathscr{E}$. Alors il existe $x', y' \in \mathscr{E}$ tels que $x = f(x')$, $y = f(y')$ car f est bijective, donc surjective. On a d'une part
$$d(f^{-1}(x), f^{-1}(y)) = d(f^{-1}(f(x')), f^{-1}(f(y'))) = d(x', y')$$
car f^{-1} est l'inverse de f. D'autre part, comme f est une isométrie,
$$d(x', y') = d(f(x'); f(y')) = d(x,y).$$
Les deux égalités précédentes donnent bien $d(f^{-1}(x), f^{-1}(y)) = d(x,y)$. Donc f^{-1} est une isométrie et la première affirmation est démontrée.

Soit maintenant $u \in E$. Pour $x, y \in \mathscr{E}$, on a, par définition de $\overrightarrow{xy}$, que $y = x * \overrightarrow{xy}$. En faisant agir u sur cette égalité, en utilisant la commutativité de la somme et les propriétés d'une action, on obtient
$$y * u = (x * \overrightarrow{xy}) * u = x * (\overrightarrow{xy} + u) = x * (u + \overrightarrow{xy}) = (x * u) * \overrightarrow{xy}$$
ce qui montre que le vecteur $\overrightarrow{(x*u)(y*u)} = \overrightarrow{xy}$ par unicité dans la condition satisfaite par l'action dans un espace affine.

Alors,
$$d(t_u(x), t_u(y)) = d(x * u; y * u) = \|\overrightarrow{(x*u)(y*u)}\| = \|\overrightarrow{xy}\| = d(x,y).$$

Il suit que les translations sont incluses dans les isométries. Leur loi de groupe étant la composition, le deuxième point est prouvé. □

Exemple 3.5. La distance dans un espace affine euclidien traduit exactement l'idée intuitive que l'on a. C'est bien la longueur du segment de droite entre deux points. En effet si $x, y \in \mathscr{E}$. Soit D l'unique droite affine passant [29] par x et y. Alors cette droite D s'identifie à $x + \mathbb{R}\vec{u}$ où $\vec{u}$ est un vecteur unitaire de direction D. Soit alors t l'unique réel tel que $y = t\vec{u} + x$. On a alors que

$$d(x, y) = \|(y - x)\| = \|t\vec{u}\| = |t|\|\vec{u}\| = |t|.$$

Autrement dit, la distance euclidienne entre x et y est bien donnée par la longueur du segment les joignant.

Remarque 3.6. La définition implique facilement qu'une isométrie f est injective. En effet, soit M, N tels que $f(M) = f(N)$. Alors $\|\overrightarrow{MN}\| = \|\overrightarrow{f(M)f(N)}\| = 0$ implique que $M = N$.

En dimension finie, le théorème 3.18 implique qu'une isométrie est toujours affine d'où on en déduit [30] qu'une isométrie est toujours bijective en dimension *finie*.

On a la généralisation suivante de la notion d'isométrie.

Définition 3.7. Soit $\mathscr{E}$ un espace affine préhilbertien (ou euclidien). Une similitude de $\mathscr{E}$ est une application $f : \mathscr{E} \to cE$ qui vérifie qu'il existe un réel $r > 0$ tel que pour tous M, $N \in \mathscr{E}$ on ait

$$d(f(M), f(N)) = rd(M, N).$$

Autrement dit f multiplie les distances par r. On appelle r le rapport de la similitude.

On prendra garde que r est une constante bien sûr, c'est à dire le même quels que soient les points M et N.

Les isométries sont donc exactement les similitudes de rapport 1. Les similitudes ne sont en général pas des isométries, mais des parentes proches au sens où elles ne conservent pas forcément les distances, mais conservent les *proportions* [31], rapport entre les distances.

Lemme 3.8. *Une similitude est injective.*

Démonstration. On la laisse en exercice. C'est la même que celle pour les isométries. □

Introduisons une terminologie importante.

Terminologie 3.9. Soit $(\mathscr{E}, E, *)$ un $\mathbb{R}$-espace affine de dimension finie.

- Une application $\varphi \in GL(E)$ est dite un isomorphisme linéaire ***direct*** si $\det(\varphi) > 0$ et ***indirect*** si $\det(\varphi) < 0$.
- Un isomorphisme affine $f \in \mathbf{Aff}(\mathscr{E})$ est un isomorphisme linéaire ***direct*** si $\det(\vec{f}) > 0$ et ***indirect*** si $\det(\vec{f}) < 0$.

On étend bien sûr cette notion à tout sous-groupe de $GL(E)$ ou $\mathbf{Aff}(\mathscr{E})$: on parle donc d'isométries (in)directes, similitudes (in)directes par exemple.

Les isométries directes (resp. indirectes) sont parfois appelées positives (resp. négatives), surtout en anglais. On trouve également la terminologie de *déplacement* et anti-déplacement pour les indirects, surtout dans le plan et l'espace.

Remarque 3.10 (Déterminant d'une application affine). On pourrait définir le déterminant de toute application affine f comme étant par définiton $\det(\vec{f})$. Et les résultats usuels s'étendent à ce cadre : par exemple $\det(f) \neq 0$ si et seulement si f est un isomorphisme.

29. nous vérifierons ci-dessous que c'est bien vrai
30. laissé en exercice
31. et donc les angles

Remarque 3.11. On a associé, à tout point $x_0 \in \mathscr{E}$, une structure d'espace vectoriel sur $\mathscr{E}$ isomorphe à E (cf 2.26). Si en plus E est muni d'un produit scalaire b, alors on peut définir, pour tout $x, y \in \mathscr{E}$, l'application

$$b_{x_0}(x,y) = b(\overrightarrow{x_0x}, \overrightarrow{x_0y}). \tag{28}$$

Lemme 3.12. *Soit $(\mathscr{E}, E, b, *)$ un espace préhilbertien, alors $(\mathscr{E}, +_{x_0}, *_{x_0}, b_{x_0})$ est également préhilbertien et Γ_{x_0} est une isométrie linéaire.*

De plus, l'application $\Gamma_{x_0} : \left\{ \begin{array}{ccc} E & \to & \mathscr{E} \\ u & \mapsto & x_0 * u \end{array} \right.$ *et son inverse sont des isométries.*

Démonstration. Que b_{x_0} soit un produit scalaire découle directement du fait que b l'est. Par exemple $b_{x_0}(x,x) = 0$ est équivalent à $b(\overrightarrow{x_0x}, \overrightarrow{x_0x}) = 0$ ce qui est équvalent puisque b est un produit scalaire à $\overrightarrow{x_0x} = 0$ et donc $x = x_0$ le neutre de notre espace vectoriel. On montre de même els autres propriétés. Au vu de 2.25, il reste à vérifier que Γ_{x_0} est une isométrie (linverse d'une isométrie l'étant aussi). Or pour $M, N \in \mathscr{E}$, alors il existe $u, v \in E$ uniques tels que $M = x_0 * u$, $N = x_0 * v$. Alors $N = x_0 * (v - u + u) = (x_0 * u) * (v - u) = M * (v - u)$. Il suit que $\overrightarrow{MN} = v - u$ Par conséquent, la distance entre $M = x_0 * u$ et $N = x_0 * v$ est égale à $\|\overrightarrow{MN}\| = \|v - u\| = d(u,v)$ dans E. L'application est bien une isométrie. □

Remarque 3.13 (**Similaire, isométrique...**). Étant des sous-groupes de $\mathbf{Aff}(\mathscr{E})$, qui est lui même un sous-groupe de $\mathrm{Bij}(\mathscr{E})$, les groupes des isométries $\mathbf{Iso}(\mathscr{E})$ et des similitudes $\mathbf{Sim}(\mathscr{E})$ (Définition 3.7) agissent sur $\mathscr{E}$. En effet, on déduit du lemme 4.1.

Lemme 3.14. *Soit $\mathscr{E}$ un espace affine. Alors l'application* $\begin{array}{ccc} \mathbf{Aff}(\mathscr{E}) \times \mathscr{E} & \longrightarrow & \mathscr{E} \\ (f, M) & \longmapsto & f(M) \end{array}$ *est une action à gauche de $\mathbf{Aff}(\mathscr{E})$ sur $\mathscr{E}$. Elle induit, pour tout sous-groupe H de $\mathbf{Aff}(\mathscr{E})$ une action de H sur $\mathscr{E}$ définie par la même formule.*

Exercice 3.15. Démontrer le lemme.

Puisque l'on a des actions, on a les relations d'équivalences associées. Rappelons que si G agit sur X, la relation associée est $x \mathscr{R} y \Leftrightarrow \exists g \in G,\ y = g \cdot x$. Ces relations d'équivalence sont centrales en géométrie et s'étendent facilement aux sous-ensembles de $\mathscr{E}$. D'ailleurs vous avez sans doute déjà croisés les terminologies suivantes :

- Deux sous-ensembles X, Y de $\mathscr{E}$ sont dit *isométriques* si il existe une isométrie $f \in \mathbf{Iso}(\mathscr{E})$ telle que $f(Y) = X$.
- Deux sous-ensembles X, Y de $\mathscr{E}$ sont dit *similaires* si il existe une similitude $g \in \mathbf{Sim}(\mathscr{E})$ telle que $g(Y) = X$.

Ces deux relations forment des relations d'équivalence sur les sous-ensembles de $\mathscr{E}$.

Exercice 3.16. Démontrer le !

Le théorème de structure du groupe affine se restreint aux isométries.

Corollaire 3.17. *Soit $(\mathscr{E}, E, b, *)$ un espace affine euclidien et $x_0 \in \mathscr{E}$.*

(1) L'ensemble $\mathbf{Tran}(\mathscr{E}) \times O_{x_0}(\mathscr{E})$ muni de la loi interne

$$(t_u, \overrightarrow{f_1}) * (t_v, \overrightarrow{f_2}) = (t_{u + \overrightarrow{f_1}(v)}, \overrightarrow{f_1} \circ \overrightarrow{f_2}) \tag{29}$$

est un groupe.

(2) L'application $(t, \overrightarrow{f_{x_0}}) \mapsto t \circ \overrightarrow{f_{x_0}}$ est un isomorphisme de groupe de $\mathbf{Tran}(\mathscr{E}) \times O_{x_0}(\mathscr{E})$ sur $\mathbf{Iso}(\mathscr{E})$.

Un résultat remarquable est que les isométries dans un espace euclidien sont automatiquement affines. C'est le cas affine du Théorème 1.3 que l'on précise maintenant.

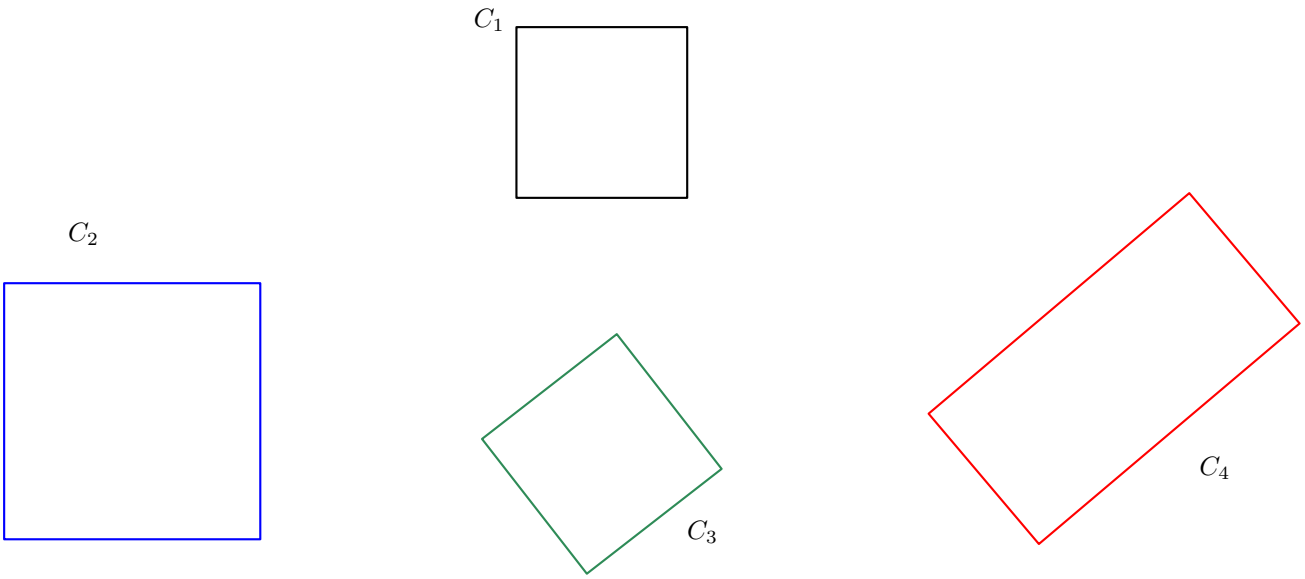


FIGURE 9. Le caré C_1 est isométrique à C_3 via, par exemple, une translation composée avec une rotation autour de son centre. Il n'est pas isométrique à C_2 mais lui est similaire. En revanche il n'est ni similaire (ni donc isométrique) à C_4 mais lui est affinement équivalent via lc composée d'une translation avec une rotation et une application de la forme $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$

Théorème 3.18 (Theorème fondamental des isométries euclidiennes)**.** *Soit $\mathscr{E}$ et $\mathscr{F}$ des espaces affines euclidiens. Alors f est une isométrie si et seulement si f est une isométrie affine.*

Le sens important est que les isométries d'un espace euclidiene $\mathscr{E}$ est en particulier des applications affines. Elles envoient en particulier des droites sur des droites, des parallélogrammes sur des parallélogrammes etc... Voir 2.41.

Remarque 3.19. Comme une application linéaire de E dans E s'identifie avec une application affine qui laisse 0 fixe, le théorème 3.18 implique l'analogue :

Soit** (E, b) **un espace vectoriel euclidien. Alors** $f : E \to E$ **est une isométrie si et seulement si c'est une isométrie linéaire.

Exercice 3.20. Démontrer le reste du lemme 2.41.

Proposition 3.21. *Soit $(\mathscr{E}, E, b, *)$ un espace affine euclidien.*

- *Toute similitude est un isomorphisme affine.*
- *Le sous-ensemble* $\mathbf{Sim}(\mathscr{E}) = \{f : \mathscr{E} \to \mathscr{E},\ \ f \text{ est une similitude}\}$ *est un sous-groupe de* $\mathbf{Aff}(\mathscr{E})$ *qui contient* $\mathbf{Iso}(\mathscr{E})$.

On notera aussi $\mathbf{Sim}_{x_0}(\mathscr{E}) \subset GL_{x_0}(\mathscr{E})$ le sous-groupes des similitudes qui laissent fixe un point x_0. Il est isomorphe au sous-groupe des similitudes de E qui sont des applications linéaire.

Là encore la preuve de cette proposition est similaire au cas des isométries.

3.1. **Exemples : réflexions, symétries et homothéties.** Il est plus que temps de faire des exemples autres que les translations. Les premiers sont des exemples que vous avez sans doute rencontré, en petite dimension du moins.

Pour commencer, précisons la notion d'*orthogonalité.* Si (E, b) est un espace vectoriel euclidien et H un sous-espace de E, alors un vecteur u est orthogonal à H si $b(u, h) = 0$ pour tout $h \in H$. Dans le cas affine, on a littéralement la même définition :

Définition 3.22. Soit $\mathscr{H}$ est un sous-espace affine d'un espace affine euclidien $\mathscr{E}$. Un vecteur $u \in E$ est dit orthogonal à $\mathscr{H}$ si il est orthogonal à H (la direction de $\mathscr{H}$).

Deux sous-espaces affines $\mathscr{H}$, $\mathscr{K}$ sont orthogonaux si leurs directions K et H sont orthogonales c'est à dire si pour tout $u \in K$, $v \in H$, on a $b(u, v) = 0$.

Remarque 3.23. Certains auteurs rajoutent la condition que $\mathscr{H}$ et $\mathscr{K}$ soient d'intersection non vide dans la définition de l'orthogonalité. Il faut donc être prudent.

Exemple 3.24 (Symétries centrales). Si x_0 est un point de $\mathscr{E}$, on a la notion de symétrie centrale de centre x_0 qui est une isométrie de $\mathscr{P}$. Elle est définie par

$$s_{x_0}(M) = x_0 * \Big(- \overrightarrow{x_0 M}\Big). \tag{30}$$

On vous invite à dessiner cette construction pour justifier que c'est bien une symétrie centrale.

Passons aux réflexions (par rapport à un hyperplan).

Définition 3.25 (Réflexion/symétrie orthogonale)**.** Soit $\mathscr{H}$ un hyperplan [32] affine d'un espace euclidien $(\mathscr{E}, E, b, *)$. La **réflexion par rapport à $\mathscr{H}$**, aussi appelée *symétrie (orthogonale) par rapport à $\mathscr{H}$*, est l'application $s_{\mathscr{H}}$ définie par

$$s_{\mathscr{H}}(M) = x_0 * \Big(\overrightarrow{x_0 M} - 2b\big(\overrightarrow{x_0 M}, \vec{v}\big)\vec{v}\Big) \tag{31}$$

où x_0 est un point quelocnque de $\mathscr{H}$ et $\vec{v}$ un vecteur de norme 1 orthogonal à $\vec{\mathscr{H}}$.

La figure (10) représente une réflexion. Notons que la formule donnée traduit juste l'idée géométrique que *l'image du point M par le point obtenu en regardant le projeté orthogonal $p(M)$ de M sur $\mathscr{H}$ et en regardant le point opposé à M sur la droite* $(p(M)M)$ c'est dire le point donné par $p(M) * \overrightarrow{Mp(M)}$.

Les réflexions (que vous appelez le droit d'appeler symétries, mais réflexion évite de confondre avec les symétries centrales) sont très importantes. Elles jouent en fait un rôle similaire aux transpositions pour le groupe symétrique, cf le lemme suivant. Nous montrerons d'ailleurs qu'avec les translations, elles engendrent $\mathbf{Iso}(\mathscr{E})$.

Exemple 3.26 (Réflexions/symétries par rapport à une droite). En particulier si $\mathscr{P}$ est un plan affine euclidien et D une droite (affine) de $\mathscr{P}$, alors la notion de réflexion 3.25 nous redonne la symétrie (orthogonale) $s_D : \mathscr{P} \to \mathscr{P}$ par rapport à D usuelle. Elle vérife que la doite D est la médiatrice du segment $[M, s(M)]$ pour tout M.

A priori, il y a une ambiguïté dans la définition 3.25 d'une réflexion, puisque la formule semble dépendre du choix d'un point x_0. Le lemme suivant garantit que non, entre autres choses.

Lemme 3.27. *Soit $\mathscr{H}$ un hyperplan affine.*

- *La réflexion par rapport à $s_{\mathscr{H}}$ est d'ordre 2 : $s_{\mathscr{H}} \circ s_{\mathscr{H}} = id_{\mathscr{E}}$.*
- *Si x_0 et x_1 sont dans $\mathscr{H}$, $\vec{v_1}$ et $\vec{v_2}$ des vecteurs unitaires orthogonaux à $\mathscr{H}$, alors*

$$x_0 * \Big(\overrightarrow{x_0 M} - 2b(\overrightarrow{x_0 M}, \vec{v_0})\vec{v_0}\Big) = x_1 * \Big(\overrightarrow{x_1 M} - 2b(\overrightarrow{x_1 M}, \vec{v_1})\vec{v_1}\Big).$$

En particulier la formule (31) *est indépendant des choix de x_0 (tant qu'il reste dans $\mathscr{H}$) et $\vec{v}$ (tant qu'il reste unitaire orthogonal).*

32. c'est à dire un sous-espace affine de dimension $\dim(\mathscr{E}) - 1$; par exemple une droite dans le plan affine, un plan dans l'espace affine de dimension 3

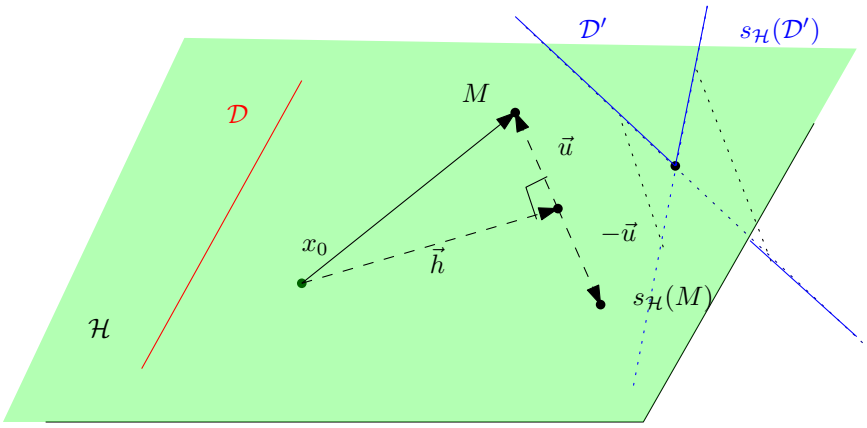


FIGURE 10. On a représenté l'image par la réflexion de plan affine $s_{\mathscr{H}}$ du point M et des droites $\mathscr{D}$ (en rouge) et $\mathscr{D}'$ (en bleu). On a que $\mathscr{D}$ est dans $\mathscr{H}$ et donc son image est-elle même. En revanche $s_{\mathscr{H}}$ n'est pas une isométrie de $\mathscr{D}'$ car $s_{\mathscr{H}}(\mathscr{D}') \neq \mathscr{D}'$.

- *Soit $M \in \mathscr{E}$ et $x_0 \in \mathscr{H}$. Si on a décomposé $\overrightarrow{x_0M} = \vec{h} + \vec{u}$ avec $\vec{h} \in H$ et $\vec{u}$ orthogonal à H, alors, on a*

$$s_{\mathscr{H}}(M) = x_0 * (\vec{h} - \vec{u}).$$

Le dernier point donne le moyen le plus facile de calculer une réflexion (et de la comprendre).

Démonstration. Remarquons tout d'abord que si $\vec{v} \neq 0$ est orthogonal à $\mathscr{H}$, alors $H \oplus \mathbb{R}\vec{v} = E$ et c'est même une somme directe orthogonale, puisque $\dim(H) = \dim(E) - 1$. On peut donc écrire tout vecteur de E de manière unique sous la forme $\vec{h} + \vec{u}$ où $\vec{u} = s\vec{v}$ et $\vec{h} \in H$.

Montrons le troisième point : On a

$$b(\overrightarrow{x_0M}, \vec{v})\vec{v} = b(\vec{h} + s\vec{v}, \vec{v})\vec{v} = \Big(b(\vec{h}, \vec{v}) + sb(\vec{v}, \vec{v})\Big)\vec{v} = 0 + s\vec{v} = \vec{u}$$

car $\vec{v}$ est orthogonal à $\vec{h}$ et de norme 1. Il suit que

$$\overrightarrow{x_0M} - 2b(\overrightarrow{x_0M}, \vec{v})\vec{v} = \vec{h} + \vec{u} - 2\vec{u} = \vec{h} - \vec{u}$$

et le dernier point est démontré.

Ce dernier point implique le premier : En effet $\vec{h} - \vec{u}$ est déjà une décomposition de $\overrightarrow{x_0 s_{\mathscr{H}}(M)}$. Il suit que

$$s_{\mathscr{H}}(s_{\mathscr{H}}(M)) = s_{\mathscr{H}}(x_0 * (\vec{h} - \vec{u})) = x_0 * (\vec{h} - (-\vec{u})) = x_0 * (\overrightarrow{x_0M}) = M.$$

Passons au deuxième. Déjà, étant deux vecteurs unitaires orthogonaux à un hyperplan H, $v_1 = \pm v_0$ où $\pm = 1$ ou -1. Notons maintenant que l'on a l'écriture $\overrightarrow{x_0M} = \overrightarrow{x_1M} + \overrightarrow{x_0x_1} + s\vec{v_0}$ où $\overrightarrow{x_0M} + \overrightarrow{x_1x_0} \in H$. Si on applique la formule du 3, on obtient donc que

$$s_{\mathscr{H}}(M) = x_0 * \Big(\overrightarrow{x_1M} + \overrightarrow{x_0x_1} - sv_0\Big) = (x_0 * \overrightarrow{x_0x_1} * (\overrightarrow{x_1M} - s \pm v_1) = x_1 * (\overrightarrow{x_1M} - s \pm v_1).$$

La preuve du troisième point nous donne

$$(\overrightarrow{x_1M} - s) \pm v_1 = 2b(\overrightarrow{x_1M}, \vec{v_1})\vec{v_1}$$

et donc les deux dernières égalités démontrent la formule annoncée. □

Remarque 3.28. Le troisième point permet en pratique de calculer/dessiner l'image d'un point par une réflexion. Cf figure 10.

Proposition 3.29. *Les réflexions par rapport à un hyperplan $\mathscr{H}$ sont des isométries affines négatives et les symétries centrales de centre x_0 sont des isométries*[33] *affines. Elles ont par ailleurs respectivement $\mathscr{H}$ et x_0 comme points fixes.*

Exercice 3.30. Prouver la proposition.

Exemple 3.31 (Homothéties et Similitudes). Les symétries centrales sont des cas particuliers d'homothéties, qui sont elles-mêmes des cas particuliers de similitudes.

Définition 3.32. Soit x_0 un point de $\mathscr{E}$ un espace affine. L'homothétie $h_{(x_0,\lambda)}$ de centre x_0 et de rapport $\lambda \in \mathbb{R} \setminus \{0\}$ est l'application définie, pour tout $M \in \mathscr{E}$, par $h_{(x_0,\lambda)}(M) = x_0 * \left(\lambda \overrightarrow{x_0 M}\right)$.

Autrement dit, pour calculer l'image de M on regarde la droite (x_0, M) et en partant de x_0 on suit le vecteur $\lambda\overrightarrow{x_0M}$ pour trouver son image.

Lemme 3.33. *Une homothétie $h_{(x_0,\lambda)}$ est une similitude laissant x_0 fixe. C'est une isométrie si et seulement si $\lambda = \pm 1$ et une symétrie centrale si et seulement si $\lambda = -1$.*

On a de plus que $\overrightarrow{h_{x,\lambda}} = \lambda id$.

Démonstration. Comme $h_{(x_0,\lambda)}(x_0) = x_0$, on vérifie que pour tout $\vec{u} \in E$, on a

$$\overrightarrow{h_{(x_0,\lambda)}(x_0)\, h_{(x_0,\lambda)}(x_0 * \vec{u})} = \overrightarrow{x_0\, x_0 * (\lambda u)} = \lambda\vec{u}$$

ce qui démontre que $\vec{u} \longmapsto \overrightarrow{h_{(x_0,\lambda)}(x_0)\, h_{(x_0,\lambda)}(x_0 * \vec{u})}$ est l'application λid qui est bien linéaire, inversible, donc une homothétie est une bijection affine. On en déduit directement que

$$\|\overrightarrow{h_{(x_0,\lambda)}(M)\, h_{(x_0,\lambda)}(N)}\| = \|\lambda\vec{MN}\| = |\lambda|\|\vec{MN}\|$$

et donc que c'est une similitude de rapport $|\lambda|$. □

Définition 3.34 (Rotation plane)**.** Une rotation *vectorielle* plane est un élément de $SO_2(\mathbb{R})$.

Si $\mathscr{P}$ est un plan affine euclidien, une *rotation affine* de centre x_0 est un élément de $\left(SO_2(\mathbb{R})\right)_{x_0}$ l'image par Γ_{x_0} de $SO_2(\mathbb{R})$ dans $\mathbf{Aff}(\mathscr{P})$. Ainsi une rotation d'un plan affine $\mathscr{P}$ de centre x_0 est une application de la forme

$$M \longmapsto x_0 * r(\overrightarrow{x_0M})$$

où $r \in SO_2(\mathbb{R})$ est quelconque.

Terminologie 3.35. On appelle parfois plus généralement rotation vectorielle tout élément de $SO_n(\mathbb{R})$.

Remarque 3.36. La (deuxième partie de la) définition signifie simplement qu'une fois qu'on a identifié un plan affine avec $\mathbb{R}^2$ en choisissant un point x_0, une rotation de centre x_0 est précisément l'image de $SO_2(\mathbb{R}) \cong SO_2(\mathbb{R}^2)$ via le plongement des applications linéaires dans les applications affines qui préservent x_0.

Proposition 3.37. *Une rotation affine plane est une isométrie directe.*

Démonstration. Soit $R(M) = x_0 * r(\overrightarrow{x_0M})$ une rotation affine de centre x_0. En choisissant x_0 comme origine, on trouve immédiatement que $\vec{R} = r$ qui est bien linéaire et une isométrie vectorielle directe puisque un élément de $SO_2(\mathbb{R})$. Voir le cours d'algèbre 4. □

33. directe si la dimension est paire, indirecte sinon

Exemple 3.38. Pour résumer, on a les exemples standards suivants :

- Une translation est une isométrie directe.
- Une rotation est une isométrie directe du plan.
- Une réflexion est une isométrie indirecte. En effet, il suffit de le vérifier pour une isométrie linéaire par définition. On a vu en TD qu'il existe une décomposition de E sous la forme $E = H \oplus D$ avec H un hyperplan et D une droite telle que la matrice de la réflexion dans une base adaptée à la décomposition est $\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix}$. Cette matrice est de déterminant $-1 < 0$ et le déterminant est indépendant du choix d'une base d'après le cours d'algèbre linéaire.
- Une homothétie $h_{x_0,\lambda}$ dans $\mathscr{E}$ de dimension n est une similitude directe si et seulement $\lambda^n > 0$. En particulier une symétrie centrale est indirecte en dimension impaire mais directe en dimension paire.

Exercice 3.39. Vérifier les affirmations de ces exemples.

Exemple 3.40. On a vu que les similitudes contiennent les isométries. Réciproquement, étant donné une similitude linéaire, autrement dit un élément de $\mathbf{Sim}_0(E)$, on peut construire une isométrie linéaire. En effet, soit $f : \mathscr{E} \to \mathscr{E}$ une telle similitude de rapport r. Comme $r > 0$, il admet une racine carrée $\sqrt{r}$. On a alors $\dfrac{f}{\sqrt{r}} : \mathscr{E} \to \mathscr{E}$ est une isométrie linéaire. En effet

$$d\left(\frac{f(x)}{\sqrt{r}}, \frac{f(y)}{\sqrt{r}}\right) = \frac{1}{r} d(f(x), f(y)) = d(x, y)$$

où on a utilisé que $d(a, b)$ provient de la norme et donc $d(\lambda a, \lambda b) = \lambda d(a, b)$ pour $\lambda \geq 0$.

La fin de cette section est hors programme. Elle est culturelle
L'étude précédente des homothéties nous donne

Lemme 3.41. *Le groupe* $\mathbf{Sim}_{x_0}(\mathscr{E})$ *est isomorphe au groupe produit* $]0, +\infty[\times\mathbf{Iso}_{x_0}(\mathscr{E})$.

Remarque 3.42. Il est indispensable de fixer x_0 ici, sinon on ne peut pas multiplier par un scalaire. En effet, avant de fixer x_0, on a pas de structure vectorielle sur $\mathscr{E}$.

Démonstration. Soit f une similitude linéaire de rapport r. Alors f s'écrit $\sqrt{r}\,\mathrm{id} \circ \dfrac{f}{\sqrt{r}}$. On en déduit facilement que l'application $\begin{array}{ccc}]0, +\infty[\times\mathbf{Iso}_{x_0}(\mathscr{E}) & \longrightarrow & \mathbf{Sim}_{x_0}(\mathscr{E}) \\ (s, f) & \longmapsto & sf \end{array}$ est bijective. Et on vérifie que c'est un morphisme de groupe en remarquant que $s\mathrm{id}$ commute avec toute application linéaire. □

On en déduit comme dans les propositions 2.52 que $\mathbf{Sim}(\mathscr{E})$ est isomorphe au produit semi-direct $\mathbf{Tran}(\mathscr{E})\times]0, +\infty[\times\mathbf{Iso}_{x_0}(\mathscr{E})$ muni d'une relation similaire à (29).

Le résultat ci-dessus nous dit qu'en fait la classification des similitudes se ramène à celle des isométries ou presque en vertu du théorème suivant.

Théorème 3.43. *Soit* $f : \mathscr{E} \to \mathscr{E}$ *une similitude de rapport* $r \neq 1$. *Alors* f *admet un unique point fixe* C *et* f *s'écrit de manière unique comme la composée* $h_{C,r} \circ \varphi_f$ *où* $\varphi_f \in \mathbf{Iso}_C(\mathscr{E})$ *et* $h_{C,r}$ *est l'homothétie de centre* C *et de rapport* r.

Autrement dit, une similitude qui n'est pas une isométrie est la composée d'une homothétie et d'une isométrie linéaire. La preuve sera basée sur le lemme suivant, qui est vrai pour *tout espace affine de dimension finie.*

Lemme 3.44. *Si* $f : \mathscr{E} \to \mathscr{E}$ *est un isomorphisme affine et que* 1 *n'est pas vecteur propre de* $\vec{f}$, *alors* f *a un unique point fixe.*

Démonstration. Soit $M \in \mathscr{E}$. Nous allons essayer de résoudre l'équation $f(M) = M$, et montrer qu'elle a une unique solution. Le point clé sera qu'une application linéaire $\vec{f}$ n'admet pas 1 comme valeur propre si et seulement si $\vec{f} - \mathrm{id}$ est bijective (ce qui découle du théorème du rang puisque nous sommes en dimension finie).

Pour pouvoir utiliser l'application linéaire $\vec{f}$, nous allons utiliser la définition d'une application affine et pour cela on introduit donc un point $x_0 \in \mathscr{E}$ différent de M. L'équation $f(M) = M$ est équivalente à l'équation $\overrightarrow{x_0 f(M)} = \overrightarrow{x_0 M}$, qui est une équation entre vecteurs de E, par l'unicité dans les axiomes définissant un espace affine.

Pour introduire $\vec{f}$, on introduit maintenant le vecteur $\overrightarrow{f(x_0)f(M)} = \vec{f}(\overrightarrow{x_0 M})$. Par la relation de Chasles,

$$\overrightarrow{x_0 f(M)} = \overrightarrow{x_0 f(x_0)} + \overrightarrow{f(x_0)f(M)} = \overrightarrow{x_0 f(x_0)} + \vec{f}(\overrightarrow{x_0 M}).$$

On obtient que M est un point fixe si et seulement si

$$\overrightarrow{x_0 f(x_0)} + \vec{f}(\overrightarrow{x_0 M}) = \overrightarrow{x_0 M} \iff (\vec{f} - \mathrm{id})(\overrightarrow{x_0 M}) = \overrightarrow{x_0 f(x_0)}. \tag{32}$$

Il nous faut donc montrer qu'il existe un unique vecteur $u = \overrightarrow{x_0 M}$ dans E tel que $(\vec{f} - \mathrm{id})(u) = \overrightarrow{x_0 f(x_0)}$. Or par hypothèse 1 n'est pas valeur propre de $\vec{f}$. Donc $(\vec{f} - \mathrm{id})$ est bijective. Ce qui assure l'existence et l'unicité de u. □

Remarque 3.45. La réciproque du lemme est vraie. Si 1 a un unique point fixe, alors 1 n'est pas valeur propre de $\vec{f}$. Sinon, l'espace affine $C + \ker(\vec{f} - \mathrm{id})$ (où C est le point fixe de f) serait un espace de points fixes, de dimension ≥ 1 et donc infini. En fait, l'argument montre essentiellement que si $\vec{f}$ a 1 pour valeur propre, alors soit f n'a pas de points fixes (par exemple une symétrie glissée 3.56), soit f a un sous-espace affine de dimension > 0 comme points fixes.

Preuve du Théorème 3.43. Le premier est point de voir qu'on peut appliquer le lemme 3.44. Comme $\vec{f}$ est une similitude linéaire de rapport r, ses valeurs propres sont de module r puisque $|\vec{f}(x)| = r|x|$ ce qui assure que si $f(x) = \lambda x$, alors $|\lambda| = r$. Comme $r \neq 1$, les hypothèse du lemme 3.44 sont vérifiées et f a un unique point fixe C. Donc f est un élément de $\mathbf{Sim}_C(\mathbb{C})$ le groupe des similitudes linéaires en $\mathbb{C}$. Le résultat découle alors du lemme 3.41 et que les homothéties linéaires sont précisément les applications de la forme $r\mathrm{id}$. □

3.2. **Rotations affines planes.** Nous allons maintenant nous concentrer sur le cas d'un plan affine euclidien. D'après la proposition 2.60, on peut supposer que ce plan est $\mathbb{R}^2$ muni de sa structure affine canonique et du produit vectoriel canonique. On peut identifier $\mathbb{R}^2$ avec $\mathbb{C}$ et la strucure de corps de $\mathbb{C}$ va nous aider à décrire les similitudes comme nous allons le voir.

On rappelle qu'une base de $\mathbb{C}$ est donnée par $\{1, i\}$. De manière standard nous avons identifié 1 avec les vecteurs $(1, 0)$ et i avec le vecteur $(0, 1)$ de $\mathbb{R}^2$ et donc avec les vecteurs colonnes $\begin{pmatrix}1\\0\end{pmatrix}$ et $\begin{pmatrix}0\\1\end{pmatrix}$ respectivement.

Ces identifications *nous donnent un isomorphisme "canonique"*

$$\Psi : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{C} \\ \begin{pmatrix}x\\y\end{pmatrix} & \longmapsto & x + iy. \end{array} \tag{33}$$

où on a noté les éléments de $\mathbb{R}^2$ comme des vecteurs colonnes.

Remarque 3.46 (*Quelle est la différence entre* $\mathbb{C}$ *et* $\mathbb{R}^2$ *ou un autre* $\mathbb{R}$*-espace vectoriel de dimension 2 ?).* D'abord $\mathbb{C}$ est bien un $\mathbb{R}$-espace vectoriel de dimension deux. Cependant lorsque on définit [34] $\mathbb{C}$, on choisit une racine carrée de -1, que l'on nomme i la plupart du temps. ***Ceci nous donne une base de*** $\mathbb{C}$ comme $\mathbb{R}$-espace vectoriel ; la base $(1, i)$; d'ailleurs on en profite pour écrire les nombres complexes sous la forme $z = x + iy$. Donc $\mathbb{C}$ arrive avec une base préférentielle tout comme $\mathbb{R}^2$ (avec la base canonique $\Big((1,0),(0,1)\Big)$). Ils ont par ailleurs tous deux une structure euclidienne canonique (donnée par le module dans $\mathbb{C}$).

Mais cependant il y a encore une différence : $\mathbb{C}$ ***est muni d'une structure de corps****, c'est à dire que l'on a fixé une multiplication compatible avec l'action de* $\mathbb{R}$ *sur* $\mathbb{C}$, précisément donnée par $i^2 = -1$. C'est là la différence principale avec $\mathbb{R}^2$. Cette structure va en fait nous permettre de représenter efficacement toutes les similitudes du plan euclidien.

L'isomorphisme Ψ (cf (33)))permet d'identifier tout sous-groupe de $GL_2(\mathbb{R})$ avec un sous-groupe de $GL(\mathbb{C})$ via le morphisme de groupes bijectif :

$$\tilde{\Psi} : \begin{array}{ccc} GL_2(\mathbb{R}) & \xrightarrow{\simeq} & GL(\mathbb{C}) \\ M & \longmapsto & \Big(z \mapsto \Psi\big(M(\Psi^{-1}(z))\big)\Big). \end{array}$$

Exercice 3.47. Vérifier que ceci est bien un isomorphisme de groupes.

Rappelons enfin que tout nombre complexe non-nul s'écrit sous la forme

$$z = x + iy = re^{i\theta} = f\cos(\theta) + ir\sin(\theta)$$

où $\theta \in \mathbb{R}$ est défini modulo 2π et $r > 0$. On a dans cette écriture que le module $|z| = r$. En particulier les nombres complexes de module 1 sont ceux de la forme $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

On va identifier $SO_2(\mathbb{R})$ et les nombres complexes de module 1 ci-dessous. Pour cela, rappelons du cours d'algèbre 4 qqu'un élément de $SO_2(\mathbb{R})$ s'écrit sous la forme d'une matrice $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. Cette matrice est celle de l'application appelée rotation vectorielle d'angle θ et est égale à $\begin{pmatrix} u & u^\perp \end{pmatrix}$ où $(u, u^\perp)$ sont des vecteurs colonnes orthogonaux et unitaires (et $u = \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix}$ et donc on peut identifier u avec $e^{i\theta}$ et $u^\perp$ avec $ie^{i\theta}$.

Proposition 3.48. *L'image par l'isomorphisme* Ψ *ci-dessus du sous-groupe des rotations vectorielles est le sous-groupe des applications* $\mathbb{C} \to \mathbb{C}$ *donné par* $z \mapsto e^{i\theta}z$*. Cette application correspond précisément à celle donnée par la matrice* $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

Autrement dit, une rotation vectorielle est simplement donnée par la multiplication par un nombre complexe de module 1.

Avec l'écriture $z = re^{i\alpha}$ d'un nombre complexe quelconque, on obtient que la rotation *vectorielle* d'angle θ est donnée par la formule

$$re^{i\alpha} \longmapsto re^{i(\alpha+\theta)}$$

Démonstration. Soit $M = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. On peut identifier M avec $\begin{pmatrix} \Psi^{-1}(z) & \Psi^{-1}(iz) \end{pmatrix}$ par définition (33) de Ψ, avec $z = e^{i\theta}$.

Soit maintenant $N = \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \in SO_2(\mathbb{R})$. Alors $MN = \begin{pmatrix} \cos(\theta)u - \sin(\theta)v & -u\sin(\theta) - \cos(\theta)v \\ \sin(\theta)u + \cos(\theta)v & \cos(\theta)u - \sin(\theta)v \end{pmatrix}$. D'un autre côté

$$e^{i\theta}(u + iv) = \cos(\theta)u - s \in (\theta)v + i(\sin(\theta)u + \cos(\theta)v)$$

34. en tout cas dans ce cours ou en algèbre ou analyse

ce qui est exactement le premier vecteur colonne de MN. Ainsi $M \mapsto e^{i\theta}$ est bien un morphisme de groupes.

Le même calcul appliqué à un vecteur colonne donne la fin du résultat :

$$\Psi\left(\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}\right) = \cos(\theta)x - \sin(\theta)y + i(\sin(\theta)x + \cos(\theta)y) = e^{i\theta}(x+iy)$$

ce qui démontre la formule annoncée. □

Le corollaire à retenir est le suivant.

Corollaire 3.49. *Les rotations affines dans $\mathbb{C}$ sont exactement les applications de la forme*

$$z \mapsto a(z - z_0) + z_0$$

où $a = \exp(i\theta)$ est de module 1 et z_0 est un nombre complexe.

Remarquons que si $a = 1$, alors l'application $z \mapsto a(z - z_0) + z_0 = z - z_0 + z_0 = z$ est l'identité.

Démonstration. Rappelons d'abord qu'une translation t_z de vecteur $z \in \mathbb{C}$ est donnée par $t_z(u) = z+u$ (d'après la structure affine de $\mathbb{C}$ associée à sa structure de $\mathbb{R}$-espace vectoriel). En particulier, si $z, z' \in \mathbb{C}$, on a $\overrightarrow{zz'} = z' - z$ puisque $z' = z + (z - z')$ (et par unicité de ce vecteur).

Soit maintenant un isomorphisme linéaire $\vec{f} : \mathbb{C} \to \mathbb{C}$ et $z_0 \in \mathbb{C}$. Alors $\vec{f}_{z_0} \in GL_{z_0}(\mathbb{C})$ l'application linéaire associée fixant z_0 est donnée, pour tout $z \in \mathbb{C}$, par

$$\vec{f}_{z_0}(z) = z_0 + \vec{f}(\overrightarrow{z_0 z}) = z_0 + \vec{f}(z - z_0).$$

En appliquant cela à une rotation, la proposition 3.48, nous donne qu'une rotation s'écrit $r_{z_0}(z) = z_0 + a(z - z_0)$ pour un certain $z_0 \in \mathbb{C}$ et $a \in S^1$. □

Lemme 3.50. *Une rotation affine (plane) différente de id a un* unique *point fixe, appelé son centre. Dans la formule du corollaire 3.49, c'est précisément le point z_0.*

Démonstration. Si z est un point fixe d'une rotation affine, alors $z = a(z - z_0) + z_0$ d'après le corollaire précédent. Il suit que $z(1 - a) = z_0(1 - a)$. Si la rotation est différente de l'identité alors $a \neq 1$, donc on peut simplifier par $1 - a$ et on obtient $z = z_0$. □

Nous venons de voir comment coder et calculer facilement des rotations avec des nombres complexes, en utilisant leur multiplication. Nous allons généraliser cela à toutes les similitudes.

3.3. **Étude des isométries et similitudes planes via les nombres complexes.** Nous allons généraliser notre étude des rotations via les nombres complexes à toutes les isométries et même similitudes.

Le résultat principal est le théorème suivant qui montre que les similitudes s'écrivent très simplement si on les écrit avec l'écriture en complexe. On rappelle que les nombres complexes de module 1 sont exactement les $\exp(i\theta)$ ($\theta \in \mathbb{R}$)

Théorème 3.51. *Dans le plan euclidien $\mathbb{C}$, on a que*

- *les **similitudes directes** sont exactement les applications de la forme*

  $$z \mapsto az + b$$

  avec $a \in \mathbb{C}^*$, $b \in \mathbb{C}$ quelconques.
- *Les **similitudes indirectes** sont exactement les applications de la forme*

  $$z \mapsto a\overline{z} + b$$

  avec $a \in \mathbb{C}^*$, $b \in \mathbb{C}$ quelconques.

- *les* ***isométries directes*** *sont exactement les applications de la forme*
$$z \mapsto \exp(i\theta)z + b$$
avec $\exp(i\theta) \in S^1$, $b \in \mathbb{C}$ *quelconques.*
- *Les* ***isométries indirectes*** *sont exactement les applications de la forme*
$$z \mapsto \exp(i\theta)\overline{z} + b$$
avec $\exp(i\theta) \in S^1$, $b \in \mathbb{C}$ *quelconques.*

Les écritures ci-dessus sont ***uniques****.*

Avant de donner la preuve, nous allons expliciter des exemples. C'est les exemples qu'il faut comprendre en priorité ; pas la preuve.

Exemple 3.52 (**Translations**). La translation de vecteur $\vec{u} \in \mathbb{C}$ est l'application $z \mapsto z + \vec{u}$. En effet, la structure affine de $\mathbb{C}$ est donnée par l'action de $\mathbb{C}$ sur lui-même par addition, c'est l'exemple canonique 2.36. Ainsi pour toute paire de points z, $z' \in \mathbb{C}$, on a $\overrightarrow{zz'} = z' - z$ car $z' = z + (z' - z)$ et donc $z' - z$ est le vecteur qui fait passer de z à z'. Il suit que $t_{\vec{u}}(z) = z + \vec{u}$.

Exemple 3.53 (**Réflexions par rapport aux axes réels et imaginaires**). On note $z = x + iy$ un nombre complexe.

- La réflexion par rapport à l'axe des réels est l'application :
$$\Sigma : z \mapsto \overline{z}.$$
En effet prenons 0 comme point dans la droite $\mathbb{R}$. Alors, pour tout vecteur $z = x + iy$, on a que $x \in \mathbb{R}$ et iy est orthogonal à $\mathbb{R}$. Par suite (voir le lemme 3.27), la réflexion par rapport à $\mathbb{R}$ se lit donc
$$\Sigma(z) = 0 + (x - iy) = x - iy = \overline{z}.$$
- La réflexion par rapport à l'axe des imaginaires est :
$$z \mapsto -\overline{z}.$$
En effet prenons 0 comme point dans la droite imaginaire $i\mathbb{R}$. Alors, pour tout vecteur $z = x + iy$, on a que $iy \in i\mathbb{R}$ et x est orthogonal à $i\mathbb{R}$. Par suite (voir le lemme 3.27), la réflexion par rapport à $i\mathbb{R}$ se lit donc
$$z \mapsto 0 + (-x + iy) = -x + iy = -\overline{z}.$$
- La réflexion τ par rapport à la première diagonale $\Delta := \{y = x\}$ est l'application
$$\tau : z \mapsto i\overline{z}.$$
En effet prenons encore 0 comme point sur la droite. Soit $z = x + iy \in \mathbb{C}$ et décomposons le vecteur $\overrightarrow{0z} = z$ sous la forme de la somme d'un vecteur $s(1 + i)$ de Δ et d'un vecteur $t(1 - y)$ orthogonal à Δ (où s, $t \in \mathbb{R}$). On doit résoudre $x + iy = s(1 + i) + t(1 - i)$ ce qui donne $z = \dfrac{x + y}{2}(1 + i) + \dfrac{x - y}{2}(1 - i)$. On en déduit
$$\tau(z) = 0 + (\frac{(x + y)}{2}(1 + i) - \frac{x - y}{2}(1 - i)) = y + ix = i(x - iy) = i\overline{z}.$$

Preuve du Théorème 3.51. On fixe 0 comme point base de $\mathbb{C}$. Notons que si v est un vecteur, alors $t_v(z) = z + v$ pour tout $z \in \mathbb{C}$ (vu comme un point affine). En effet, l'action de $\mathbb{C}$ (vu comme espace vectoriel) sur lui-même vu comme espace affine est celle par addition (c'est la structure affine canonique 2.36).

Par le théorème de structure des applications affines, il existe une translation t_b et une similitude linéaire de $f \in \mathbb{C}$ uniques tels que l'isométrie s'écrive $t_b \circ f$ et donc la similitude

s'écrit $z \mapsto f(z) + b$. Il suffit donc de répondre dans le cas linéaire maintenant (qui revient à avoir $b = 0$).

On conseille maintenant de reprendre la preuve de la proposition 3.48, nous allons l'imiter dans le cas indirect ; la seule différence sera que z deviendra $\overline{z}$.

On traite le cas des isométries. La proposition 3.48 nous dit précisément que si f est une isométrie directe, alors $f(z) = az$ avec $a \in S^1$ ce qui termine ce cas. Si f est indirecte, alors $f \in O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$.

Rappelons que nous avons l'isomorphisme $\Psi : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{C} \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & x + iy \end{array}$ où on a noté les éléments de $\mathbb{R}^2$ comme des vecteurs colonnes.

Une telle matrice $M \in O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$ s'écrit $M = \begin{pmatrix} a & -\epsilon b \\ b & \epsilon a \end{pmatrix}$ où $\epsilon \in \{\pm 1\}$ avec $a^2 + b^2 = 1$ (car c'est une matrice orthogonale). Comme $\det(M) < 0$, on a que $-1 = \det(M) = \varepsilon(a^2 + b^2) = \varepsilon$. Donc $\varepsilon = -1$. Donc cette matrice est déterminée par son premier vecteur colonne $\begin{pmatrix} a \\ b \end{pmatrix}$. En écrivant $z = a + ib$, on obtient que Ψ se réécrit $M = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \longmapsto z = a + ib$. Rappelons que $|z| = \sqrt{a^2 + b^2} = 1$, donc $z \in S^1$.

Soit maintenant $X = \begin{pmatrix} u \\ v \end{pmatrix}$. Alors $MX = \begin{pmatrix} au + bv \\ bu - av \end{pmatrix}$. D'un autre côté

$$(a + ib)\overline{(u + iv)} = au + bv + i(bu - av)$$

ce qui est exactement le vecteur colonne de MX. Ainsi l'action de M sur $\mathbb{R}^2$ se traduit via l'isomorphisme avec $\mathbb{C}$ par $z \mapsto a\overline{z}$. Et ceci conclut donc le cas des isométries indirectes.

Pour les similitudes, il suffit de se rappeler qu'une similitude linéaire est la composée d'une homothétie de rapport $r \in]0, +\infty[$ avec une isométrie, voir le lemme 3.41.

Comme $]0, +\infty[\times S^1$ est isomorphe en tant que groupe à $\mathbb{C}^*$ (via l'isomorphisme $(r, u) \mapsto ru$ de réciproque $z \mapsto \left(|z|, \frac{z}{|z|}\right)$), on en déduit le résultat. □

Remarque 3.54 (**Classification géométrique**). Le théorème 3.51 nous dit comment écrire les isométries planes. Mais il ne nous dit pas directement quels sont les différents types "géométriques" d'isométries possibles. C'est ce qu'on va élucider complétement dans la partie 3.4, mais nous commençons par en donner un aperçu

Par type géométrique, on veut signifier que les isométries ont des caractéristiques géométriques différentes : en particulier des points fixes différents ou bien sont directes/indirectes.

On a une première réponse facile qui vient du fait qu'on sait exactement à qoi correspondent les rotations affines grace au corollaire 3.49. En comparant cette écriture avec celle donnée par le théorème 3.51, on voit que les **isométries directes du plan sont les translations** (pour $a = 1$) **et les rotations** différentes de l'identité (pour $a \neq 1$) en vertu d

Exercice 3.55. Démontrer le. (Indications : 1) Si $a = 1$, c'est facile. 2) si $a \neq 1$, vérifier que f a un unique point fixe $z_0 = \dfrac{b}{1 - a}$. 3) vérifier que $az + b = a(z - z_0) + z_0$ pour le z_0 trouvé).

On a donc déjà vu que

- l'identité, les translations de vecteur non nul, les rotations non-triviales sont les différents types d'isométries directes.
- Les réflexions sont des isométries indirectes

Il y a encore un autre type d'isométrie indirecte. Voir l'exemple ci-dessous.

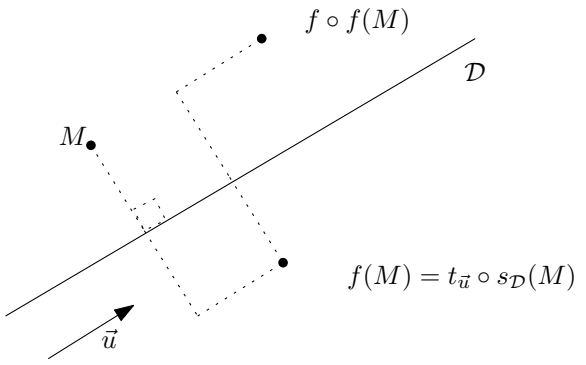


FIGURE 11. Une symétrie glissée $f = t_{\vec{u}} \circ s_{\mathscr{D}}$ de droite $\mathscr{D}$ et de vecteur $\vec{u} \in D$. On a représenté l'image de M par f et son image itérée $f^2(M)$

Exemple 3.56 (**Réflexions/Symétries glissées**). Soit $\mathscr{D}$ une droite de $\mathbb{C}$, de direction D. Notons $s_{\mathscr{D}}$ la symétrie orthogonale par rapport à $\mathscr{D}$ et soit $\vec{u} \in D$. Alors la composée $t_{\vec{u}} \circ s_{\mathscr{D}}$ est une isométrie indirecte. Voir figure (11)

Lemme 3.57. *Si $\vec{u} \in D$, alors $t_{\vec{u}}$ commute avec $s_{\mathscr{D}}$*

Démonstration. Il suffit d'appliquer le lemme 3.27 en prenant un point x_0 quelconque de $\mathscr{D}$. Pour tout $M \in \mathbb{C}$, on écrit la décomposition $\overrightarrow{x_0M} = \vec{a} + \vec{b}$ avec $\vec{a} \in D$ et $\vec{b} \in D^\perp$. On a alors

$$t_{\vec{u}} \circ s_{\mathscr{D}}(M) = t_{\vec{u}}(x_0 + (\vec{a} - \vec{b})) = \vec{a} - \vec{b} + \vec{u}.$$

On a $t_{\vec{u}}(M) = m + \vec{u}$ et donc $\overrightarrow{x_O t_{\vec{u}}(M)} = \vec{a} + \vec{b} + \vec{u}$. Comme $\vec{u} \in D$, on a que la décomposition de $\overrightarrow{x_0 t_{\vec{u}}(M)} = (\vec{a} + \vec{u}) + \vec{b}$ et il suit que

$$s_{\mathscr{D}} \circ t_{\vec{u}}(M) = x_0 + \vec{a} + \vec{u} - \vec{b}$$

ce qui est bien la même formule que ci-dessus. □

Exercice 3.58. Démontrer ces affirmations.

Terminologie 3.59. Une telle isométrie s'appelle une ***symétrie orthogonale glissée*** *ou réflexion glissée.*

Cette construction peut évidemment se faire en toute dimension tant qu'on prend un vecteur de direction l'hyperplan définissant la réflexion. Notons qu'une symétrie est un cas particulier de symétrie glissée (celle de vecteur $u = 0$). En général lorsque l'on dit symétrie glissée, on sous-entend que le vecteur u est non-nul.

Le lemme suivant permet de retrouver le vecteur de la translation.

Lemme 3.60. *Soit $f = t_u \circ s_{\mathscr{D}}$ une symétrie glissée dans $\mathbb{C}$. Alors, quel que soit $z \in \mathbb{C}$, on a*

$$u = \frac{f^2(z) - z}{2}.$$

Démonstration. Comme $\vec{f} = \mathrm{id} \circ \vec{s_{\mathscr{D}}} = s_D$ est une symétrie orthogonal linéaire, on a que $\vec{f} \circ \vec{f} = \vec{f} \circ \vec{f} = \mathrm{id}$. Donc $f^2 = f \circ f$ est bien une translation (puisque l'application linéaire associée est l'identité). Donc $f^2(z) - z$ est constante, égale à un vecteur de $\mathbb{C}$.

Pour trouver ce vecteur il suffit de regarder l'image par f^2 d'un point $x_0 \in \mathscr{D}$. Alors

$$\begin{aligned} f \circ f(x_0) &= f \circ t_u(s_{\mathscr{D}}(x_0)) = f \circ t_u(x_0) \text{ car } x_0 \in \mathscr{H}, \\ &= f(x_0+u) = t_u\big(s_{\mathscr{D}}((x_0+u)\big) = t_u(x_0+u) \text{ car } x_0+u \in \mathscr{H} \text{ puisque } u \in H, \\ &= x_0 + 2u. \end{aligned}$$

Ceci nous donne l'équation du lemme. □

Remarque 3.61. Il est ***indispensable*** de faire un dessin en dimension 2 (au minimum) pour comprendre ce résultat et voir une preuve géométrique à la main.

Rappelons qu'**un point fixe de** $f : \mathbb{C} \to \mathbb{C}$ **est un** $z \in \mathbb{C}$ **tel que** $f(z) = z$.

Lemme 3.62. *Une symétrie glissée (de translation non-triviale) n'a aucun point fixe. Une symétrie orthogonale a exactement une droite comme points fixes.*

Démonstration. Une symétrie orthogonale par rapport à $\mathscr{D} = x_0 + D$ s'écrit sous la forme $s(h+u-x_0)+x_0 = h-u+x_0$ où $x_0 \in \mathscr{D}$, $h \in D$ et u est orthogonal à D. Il suit que $s_{\mathscr{D}}(h+u-x_0) = h-u+x_0$ si et seulement si $u = 0$. Ce qui donne que les points fixes sont ceux de la droite $\mathscr{D}$.

Pour une symétrie glissée de vecteur $v \in D$ avec $v \neq 0$, on obtient $s_{\mathscr{D},v}(h+u-x_0)+x_0 = h-u+x_0+v$. Un point fixe doit donc vérifier que $u+v = -u$ ce qui est impossible car u et v sont orthogonaux, donc en somme directe (la seule possibilité serait u et $v = 0$ ce qu'on a exclu). □

3.4. **Classification géométrique des isométries planes.** Nous allons nous intéresser à déterminer toutes les isométries planes en fonction de leur nature géométrique (et pas de leur équation sous forme complexe). Continuant ainsi ce que nous avons commencé dans la remarque 3.54.

Théorème 3.63. *Soit $\mathscr{P}$ un plan affine euclidien.*

- *Les seules isométries directes sont l'identité, les translations et les rotations (non-triviales). Une isométrie directe non-triviale s'écrit sous la forme $z \mapsto az+b$ avec $a \in S^1$ qui est différent de 1 si et seulement si c'est une rotation non-triviale. Une translation non-triviale n'a pas de points fixes et une rotation non-triviale a un unique point fixe.*
- *Les seules isométries indirectes sont les réflexions et les réflexions glissées (non-triviales). Les réflexions ont exactement une droite comme points fixes, alors que les réflexions glissées non-triviales n'en ont aucun.*
- *Chacune de ces 4 catégories sont stables par conjugaison par une isométrie.*

Démonstration. Tout d'abord nous avons déjà remarqué le premier énoncé. Voir l'exercice 3.55. Il reste à voir le cas des isométries indirectes. Soit f une telle isométrie. On veut montrer qu'elle s'écrit $f = t_u \circ s_{\mathscr{D}}$ où $u \in D$ est possiblement nul et $\mathscr{D}$ est une droite affine de direction D.

D'après le théorème 3.51, on a que $f(z) = a\overline{z}+b$ avec a de norme 1.

En raison du lemme 3.60, on commence par chercher l'éventuel vecteur u d'un symétrie glissée. C'est à dire que l'on calcule

$$\frac{f^2(z)-z}{2} = \frac{a\,\overline{a\overline{z}+b}+b}{2} = \frac{a\bar{a}z+a\bar{b}+b-z}{2} = \frac{a\bar{b}+b}{2} \tag{34}$$

car $a\bar{a} = |a| = 1$. Ayant trouvé le candidat pour u, on regarde $t_{-u} \circ f$ car $f = t_u \circ s_{\mathscr{D}} \Leftrightarrow t_{-u} \circ f = s_{\mathscr{D}}$. Il reste donc à prouver que $t_{-u} \circ f$ est une symétrie orthogonale par rapport à une droite $\mathscr{D}$. Cette droite doit être les points fixes de $t_{-u} \circ f$. On cherche donc à résoudre :

$$z = t_{-u} \circ f(z) = a\overline{z}+b-\frac{a\bar{b}+b}{2} \iff z-a\overline{z} = \frac{b-a\bar{b}}{2}. \tag{35}$$

Écrivons $\tilde{a}$ pour une racine carrée de $\overline{a}$. Explicitement si $a = \exp(i\theta)$, on prend $\tilde{a} = \exp\left(\frac{-i\theta}{2}\right)$. On a alors $\tilde{a}a = \exp(i\theta)$ qui est une racine carrée de a. L'équation (35) devient alors équivalente (en multipliant chaque membre par $\tilde{a} \neq 0$) à

$$\tilde{a}z - \overline{\tilde{a}z} = \frac{\tilde{a}b - \overline{\tilde{a}b}}{2} \iff \mathrm{Im}(\tilde{a}z) = \mathrm{Im}\left(\frac{\tilde{a}b}{2}\right). \tag{36}$$

Ceci est bien l'équation d'une droite, il s'agit précisément d'une droite qui fait un angle $\theta/2$ avec l'axe des réels (et passe par $b/2$). On a donc que sa direction D est la droite $\mathrm{Im}(\tilde{a}z) = 0$.

On note que le vecteur $u = \frac{a\overline{b} + b}{2}$ qu'on a trouvé vérifie que $\mathrm{Im}(\tilde{a}u) = \mathrm{Im}\left(\frac{\tilde{a}b + \overline{\tilde{a}b}}{2}\right) = 0$ et donc vérifie l'équation de la droite vectorielle.

Il suffit maintenant de vérifier que $t_{-u} \circ f$ est la symétrie orthogonale par rapport à cette droite.

Nous pouvons écrire $z - b/2 = \overline{\tilde{a}}x + i\overline{\tilde{a}}y$ avec $x, y \in \mathbb{R}$ car l'équation $\mathrm{Im}(\tilde{a}z) = 0$ est équivalente à $\tilde{a}z = x \in \mathbb{R}$ qui comme $\tilde{a}^{-1} = \overline{\tilde{a}}$, nous donne $z = \overline{\tilde{a}}x$; et de même pour y.

C'est une décomposition avec $\overline{\tilde{a}}x$ dans D et $i\overline{\tilde{a}}y$ orthogonal à D.

Il nous suffit donc de démontrer que

$$t_{-u} \circ f(\overline{\tilde{a}}x + i\overline{\tilde{a}}y + b/2) = \overline{\tilde{a}}x - i\overline{\tilde{a}}y + b/2$$

pour conclure (puisque c'est exactement l'écriture de la symétrie orthogonale cherchée.

Or

$$\begin{aligned} t_{-u} \circ f(\overline{\tilde{a}}x + i\overline{\tilde{a}}y + b/2) &= a\overline{(\overline{\tilde{a}}x + i\overline{\tilde{a}}y + b/2)} + b/2 - \frac{a\overline{b}}{2} \\ &= a\tilde{a}x - ia\tilde{a}y + \frac{a\overline{b}}{2} + b/2 - \frac{a\overline{b}}{2} = \overline{\tilde{a}}x - i\overline{\tilde{a}}y + b/2 \end{aligned}$$

ce qui est exactement le résultat cherché. □

Remarque 3.64 (**Que faut-il retenir ?**). Il est important de connaître le résultat du théorème. Pas sa preuve. En pratique, pour trouver la symétrie ou symétrie glissée correspondant à une isométrie indirecte, il nous suffit de calculer le vecteur u en calculant f^2. Puis de calculer $t_{-u} \circ f$ pour retrouver la symétrie qui est caractérisée par sa droite de points fixes. Voir l'exemple ci-dessous et les TDs.

L'exemple suivant est **fondamental**. Voir la figure (12).

Exemple 3.65 (**Composées de deux symétries**). Que se passe-t-il si on compose deux symétries $s_{\mathscr{D}}$ et $s_{\mathscr{D}'}$? Dans tous les cas on a une isométrie directe, donc une translation ou une réflexion.

Les deux cas sont possibles et dépendent de savoir si $\mathscr{D}$ et $\mathscr{D}'$ sont parallèles.

(1) Si $\mathscr{D}$ et $\mathscr{D}'$ sont parallèles, alors $s_{\mathscr{D}} \circ s_{\mathscr{D}'}$ est la translation de vecteur $2\vec{w}$ où $\mathscr{D} = \mathscr{D}' * \vec{w}$, c'est à dire que $\vec{w}$ est le vecteur qui par translation envoie $\mathscr{D}'$ sur $\mathscr{D}$.
(2) Si $\mathscr{D}$ et $\mathscr{D}'$ se coupent en un point z_0, alors c'est une rotation de centre z_0 de la forme $z \mapsto \exp(2i\theta)(z - z_0) + z_0$ où $D = \exp(i\theta)D'$. Autrement dit θ est l'angle entre les deux droite $\mathscr{D}'$ et $\mathscr{D}$.

Exemple 3.66. Regardons les rotations $u : z \mapsto e^{i\theta}z$ et $v : z \mapsto e^{-i\theta}(z - z_0) + z_0$ où $\theta \notin 2\pi\mathbb{Z}$ et $z_0 \neq 0$. Alors la composée $u \circ v$ est une isométrie directe car composée d'isométries directes (on rappelle qu'elles forment un sous-groupe). C'est donc soit une rotation, soit une translation. Il est facile de voir que ce n'est pas une rotation non-triviale : en effet, la composée des applications linéaires associées $\vec{u} \circ \vec{v}(x) = e^{i\theta}(e^{-i\theta}(x)) = x$ est l'identité.

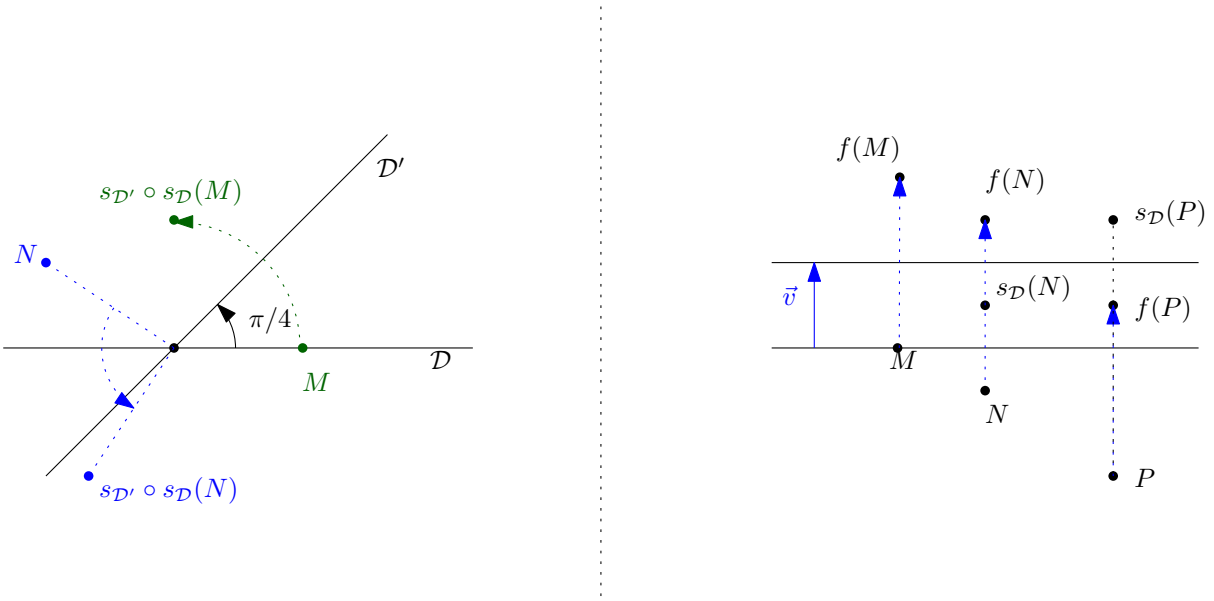


FIGURE 12. À gauche, la composée de deux symétries de droites se coupant et faisant un angle de $\pi/4$ qui est une rotation d'angle $\pi/2$. À droite, la composée de deux symétries de droites parallèles qui est la transalation de vecteur $\vec{v}$

Il suit que cette composée est donc une translation. Comme le vecteur z_0 est envoyé sur $e^{i\theta}(z_0)$, c'est une translation de vecteur $e^{i\theta}(z_0) - z_0$.

Exemple 3.67. Soit $f : \mathbb{C} \to \mathbb{C}$ l'application définie par $f(z) = -\overline{z}+1+i$. C'est une isométrie indirecte. Ainsi c'est donc une symétrie glissée. Déterminons le vecteur de glissement. D'après le lemme 3.60, on calcule

$$f(f(z)) - z = -\overline{-\overline{z} + 1 + i} + 1 + i - z = -1 + i + 1 + i = 2i.$$

D'où le vecteur de glissement est i. Pour trouver la symétrie $s_{\mathscr{D}}$ telle que $f = t_i \circ s_{\mathscr{D}}$ il suffit de remarquer que $t_{-i} \circ f = s_{\mathscr{D}}$. Il nous reste plus qu'à trouver $\mathscr{D}$ qui sont les points fixes de $t_{-i} \circ f = s_{\mathscr{D}}$. On résout $t_{-i} \circ f(z) = z$. Cela donne

$$-\overline{z} + 1 + i - = z \iff z + \overline{z} = 1 \iff \Re(z) = \frac{1}{2}$$

où $\Re(z)$ désigne la partie réelle de z. Donc $\mathscr{D}$ est l'axe vertical d'équation $x = \dfrac{1}{2}$.

Exemple 3.68. Considérons la composée f de la rotation d'angle $\pi/2$ de centre 0 et de la symétrie glissée de droite $\mathrm{Im}(z) = 1$ et de vecteur 1.

- La rotation s'écrit $z \mapsto iz$;
- la symétrie glissée s'écrit $z \mapsto \overline{z} + i + 1$ (voir l'exemple précédent).

Leur composée est donc : $f : z \mapsto z \mapsto i\overline{z} - 1 + i$ qui est indirecte car : car on a $\overline{z}$ dans l'écriture. Est-ce une symétrie ou une rélfexion glissée ? On calcule f^2

On a $f^2(z) = i\overline{i\overline{z} - 1 + i} - 1 + i = z - i + 1 - 1 + i = z$ qui est une translation de vecteur nul ; donc f est une réflexion non-glissée (d'après le lemme 3.60).

Pour trouver la droite définissant la symétrie, on cherche les points fixes : $f(z) = z$. C'est à dire les z tels que

$$z = i\overline{z} - 1 + i \iff z - i\overline{z} = i - 1.$$

En se rappelant que $i = \exp(i\pi/2)$, on obtient en multipliant par $\exp(-i\pi/4)$ que l'équation devient

$$e^{\frac{-i\pi}{4}}z - e^{\frac{i\pi}{4}}\overline{z} = e^{\frac{i\pi}{4}} - e^{\frac{-i\pi}{4}} \iff e^{\frac{-i\pi}{4}}z - \overline{e^{\frac{-i\pi}{4}}z} = e^{\frac{i\pi}{4}} - e^{\frac{-i\pi}{4}} \iff \mathrm{Im}(e^{\frac{-i\pi}{4}}z) = \frac{1}{\sqrt{2}}.$$

On a donc que f est la symétrie orthogonale par rapport à la droite $\mathrm{Im}(e^{\frac{-i\pi}{4}}z) = \frac{1}{\sqrt{2}}$, c'est à dire la droite passant par i et de pente $e^{\frac{i\pi}{4}}$. *Faire impérativement un dessin.*

En revanche si on avait pris la symétrie glissée même droite et de vecteur 2, les mêmes calculs auraient montré que sa composée par la rotation précédente était $g(z) = i\overline{z} - 1 + 2i$. C'est une symétrie glissée de même droite que f et de vecteur $\dfrac{1+i}{2}$.

Résumons la classification des isométries du plan euclidien ;

(1) Une isométrie directe est soit une translation, soit une rotation différente de l'identité. Elle s'écrit sous la forme $z \mapsto az + b$ avec $a \in S^1$ qui est différent de 1 si et seulement si c'est une rotation non-triviale. Une translation n'a pas de points fixes (à part l'identité) et une rotation non-triviale a un unique point fixe.
(2) Une isométrie indirecte est une réflexion ou une réflexion glissée (de translation non-triviale), elle s'écrit sous la forme $z \mapsto a\overline{z} + b$ ($a \in S^1$). Dans le premier cas, elle a exactement une droite comme points fixes, dans le deuxième elle n'en a aucun.

En vertu du théorème 3.43, on a une classification similaire des similitudes.

3.5. **Isométries d'un polygone : les groupes diédraux.** Très souvent en géométrie on s'intérèsse à certaines figures particulières et leurs isométries. C'est à dire les isométries qui laissent la figure stable globalement, mais pas point par point.

Un exemple important est donné par les symétries d'un polygone régulier. Leurs groupes d'isométrie sont appelés les groupes diédraux. Ils vont aussi nous servir d'exemple pour étudier les groupes d'isométries de figure.

(R)appelons d'abord la définition suivante : *un **polygone** d'un plan affine est un sous-ensemble de points dont trois points quelconques ne sont jamais colinéaires* (c'est à dire ne sont pas sur une même droite, ou dit autrement, forment un triangle non-plat).

Remarque 3.69. Notre définition correspond à ce que certains auteurs appellent polygone non-dégénéré.

*Définition informelle : Un **polygone régulier** est un polygone du plan affine dont tous les côtés et tous les angles sont égaux.* Cette définition est informelle au sens où on a pas vraiment dit ce qu'est un côté, ni des angles égaux. Mais vous en avez une idée intuitive, donc il faut la garder en tête.

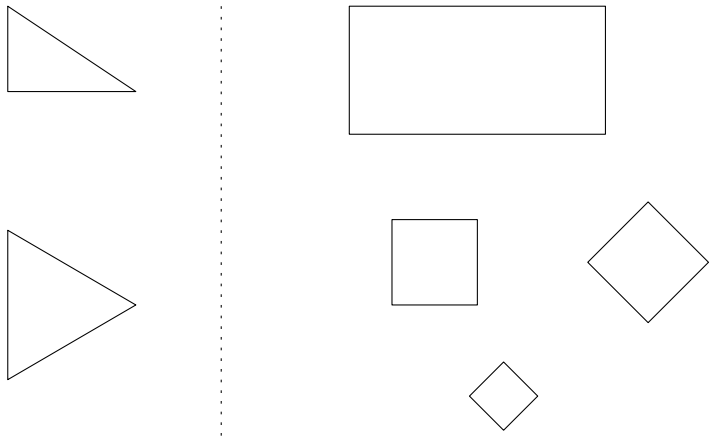
Par côté on entend les segments reliant un point à ses deux points les plus proches que l'on pourra tracer ou pas en représentant une figure. Les angles sont ceux déterminés par ces segments.

Exemple 3.70. Un triangle équilatéral ou un carré sont des polygones réguliers à 3 et 4 sommets respectivement. Un triangle isocèle (non équilatéral) ou un losange (non carré) ne le sont pas.

On peut regarder la figure 13 pour d'autres exemples.

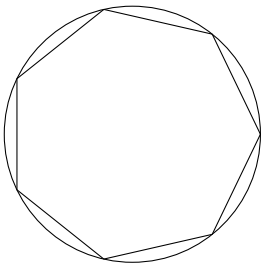
On va préciser cette définition. À isomorphisme affine près, on peut se ramener au cas où $\mathscr{E}$ est isomorphe à $\mathbb{C}$ le plan complexe (cf la proposition 2.60).

Définition 3.71. Un **polygone régulier** (à $n \geq 3$-côtés) de $\mathbb{C}$ est un ensemble de points de la forme $\{z_0 + r\exp\left(i\varphi + \dfrac{2ik\pi}{n}\right),\ k = 0, \dots n-1\}$ (avec $n \geq 3$).

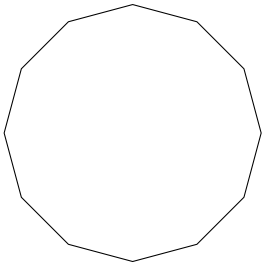


En haut un triangle qui n'est pas un polygone régulier.
En bas un triangle qui est un polygone régulier: c'est dire un triangle isocèle.

En haut un rectange non carré qui n'est pas un polygone régulier 4 côtés.
En dessous trois carrés qui sont des polygones réguliers. Les deux premiers sont isométriques mais ne sont pas isométrique à celui du bas.



Un hexagone régulier inclus dans le cercle unité.



Un polygone régulier à 12 côtés (appelé dodécagone).

FIGURE 13. Des polygones réguliers et non réguliers dans le plan de la feuille

Remarque 3.72. En vertu de l'isomorphisme rappelé ci-dessus, on appellera polygone régulier d'un (sous-)espace $\mathscr{P}$ euclidien de dimension 2, tout ensemble de points $P = \{P_1, \dots, P_n\} \subset \mathscr{P}$ tel qu'il existe une isométrie affine $f : \mathscr{E} \to \mathbb{C}$ telle que $f(P)$ est un polygone régulier de $\mathbb{C}$.

Terminologie 3.73. Un *côté* d'un polygone régulier de la forme donné par la définition 3.71 est un segment $\left[z_0 + r\exp\left(i\varphi + \frac{2ik\pi}{n}\right),\ z_0 + r\exp\left(i\varphi + \frac{2i(k+1)\pi}{n}\right)\right]$ où $k \in \{1, \dots, n\}$ (en identifiant $k+1$ et 1). Un *sommet* est un des points du polygone.

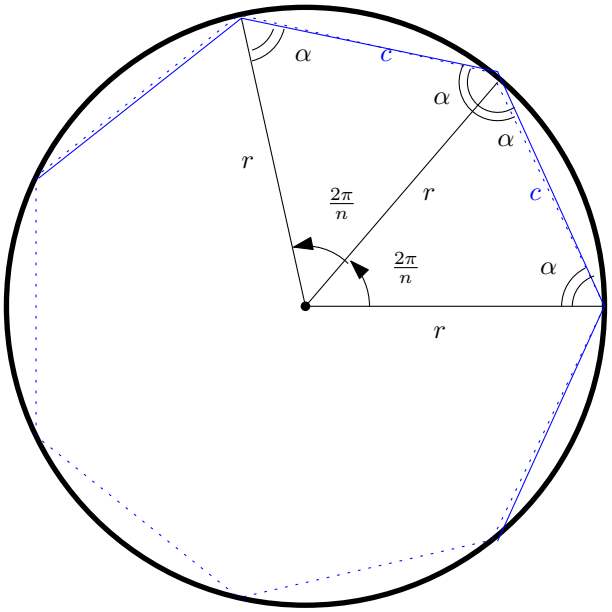
Remarque 3.74 (Le polygone c'est les sommets, les côtés, le polygone plein ?). En pratique, la réponse à cette question ne sera pas importante pour nous. On pourra, lorsque on parle du polygone le voir comme les sommets, ou la réunion des côtés, voir un polygone plein (c'est à dire avec l'intérieur de la région délimitée par les côtés). Cela ne change *rien* aux isométries, car une isométrie du polygone de $\mathscr{E}$ va préserver les segments de droites et le centre de gravité du polygone (ou s'étendre de manière unique en une telle isométrie).

Lemme 3.75. *Soit P un polygone régulier d'un plan affine euclidien. Alors, les côtés sont tous de de même longueur et les angles entre deux côtés consécutifs sont tous égaux.*

Démonstration. La preuve est explicitée dans la figure (14). Plus précisément elle montre que deux angles consécutifs sont les mêmes, de valeur égale à 2α et que les côtés consécutifs sont égaux (et donc tous les côtés sont égaux par une récurrence facile). □

Le lemme suivant caractérise simplement les polygones réguliers à similitude près.

Lemme 3.76. *Soit P un ensemble de n-points de $\mathbb{C}$. Les propriétés suivantes sont équivalentes :*



Notons que les deux triangles représentés sont isocèles: ils ont deux côtés égaux à r. Par suite les angles des triangles formés par les côtés bleus ont les mêmes angles α (qui vaut $\beta = \frac{(n-2)\pi}{2n}$).

Il suit que les angles formés par les côtés sont les mêmes. Par la loi d'Al Kashi, aussi appelée loi des sinus, on a que les deux côtés bleus ont mme longeur car on a $\frac{r}{\sin(\alpha)} = \frac{c}{\sin(\beta)}$. Ceci nous donne que les côtés sont de même longueur.

FIGURE 14. La preuve que les côtés consécutifs et angles entre sommets sont les mêmes.

- *Le polygone P est régulier à n-sommets.*
- *Le polygone P est isométrique à un polygone dont les sommets sont exactement les points* $\left\{ r\exp\left(\frac{2ik\pi}{n}\right), k = 0, \dots n-1 \right\}$ *où* $r \in]0, +\infty[$.
- *Le polygone P est similaire à un polygone dont les sommets sont exactement les points* $\left\{ \exp\left(\frac{2ik\pi}{n}\right), k = 0, \dots n-1 \right\}$.

Démonstration. Il suffit de remarquer que la rotation d'angle φ et de centre 0 envoie $r\exp\left(\frac{2ik\pi}{n}\right)$ sur $r\exp\left(i\varphi + \frac{2ik\pi}{n}\right)$. Ainsi la composée $t_{z_0} \circ r_{0,\varphi} \circ h_{0,r}$ de l'homothétie de centre 0 et de rapport r avec la rotation précédente et la translation de vecteur z_0, n obtient une similitude (directe) car composée de similitudes. Elle envoie les racines de l'unité sur le polygone $\{z_0 + r\exp\left(i\varphi + \frac{2ik\pi}{n}\right), k = 0, \dots n-1\}$. Et son inverse est aussi une similitude puisque les similitudes forment un groupe. Ceci donne l'équivalence entre 1 et 3. Celle entre 1 et 2 est obtenue de même (mais sans avoir besoin d'utiliser l'homothéte, ce qui donne bien des isométries). □

Autrement dit, **un polygone est régulier à n-sommets si et seulement si il est *similaire* à l'ensemble des *racines n-ièmes de l'unité***. Ces dernières vont être notre polygone régulier de base.

Démonstration. Soit t_{-z_0} la translation de vecteur $-z_0$ et soit r la rotation d'angle $-\varphi$ et de centre z_0 (cf définition 3.34). Alors, $t_{-z_0} \circ r$ envoie le polygone

$$\left\{ z_0 + r\exp\left(i\varphi + \frac{2ik\pi}{n}\right), z_0 + r\exp\left(i\varphi + \frac{2i(k+1)\pi}{n}\right) \right\}$$

sur le polygone $\left\{ r\exp\left(\frac{2ik\pi}{n}\right), k = 0, \dots n-1 \right\}$. On laisse le calcul en exercice.

Soit maintenant $h_{\frac{1}{r},0}$ l'homothétie de centre 0 et de rayon $1/r$. Alors les racines n-ièmes de l'unité sont l'image par $h_{\frac{1}{r},0}$ du polygone $\left\{r\exp\left(\frac{2ik\pi}{n}\right),\ k=0,\dots n-1\right\}$. Ce qui conclut. □

Nous allons maintenant introduire le groupe des isométries des polygones réguliers (à $n \geq 3$ sommets).

On commence par une notion générale que nous allons spécifier aux polygones réguliers.

Définition 3.77. Soit X un sous-ensemble de $\mathscr{E}$ un espace affine euclidien. On note

$$\mathbf{Iso}(P) := \{f \in \mathrm{Bij}(X),\ \exists \tilde{f} \in \mathbf{Iso}(\mathscr{E}) \text{ telle que } \tilde{f}_{|X} = f\}$$

le sous-ensemble des bijections de X qui sont des restrictions d'isométries (affines). ON appelle $\mathbf{Iso}(X)$ le sous-groupe des isométries de X.

Lemme 3.78. *Soit $\mathscr{E}$ affine euclidien de dimension n. On a que $\mathbf{Iso}(X)$ est un sous-groupe de $(\mathrm{Bij}(X), \circ)$.*

Exercice 3.79. Démontrer le lemme.

Soit $\tilde{f} \in \mathbf{Iso}(\mathscr{E})f$ telle que $\tilde{f}(X) = X$. alors la restriction à X de $\tilde{f}$ est une bijection de P sur lui-même donc un élément de $\mathbf{Iso}(X)$. La restriction à X est donc une application du sous-groupe des isométries de $\mathscr{E}$ qui envoient X sur X vers $\mathbf{Iso}(X)$ qui est surjetive par définition de ce dernier. En toute généralité cette application n'est pas injective. Mais elle l'est dés que *X engendre $\mathscr{E}$. C'est à dire si le plus petit sous espace affine de $\mathscr{E}$ qui contient X est $\mathscr{E}$ lui-même.*

Lemme 3.80. *Si X engendre $\mathscr{E}$ alors la restriction $\{f \in \mathbf{Iso}(\mathscr{E}) \,/\, f(P) = P\} \to \mathbf{Iso}(X)$ est un isomorphisme.*

Remarque 3.81. Une condition nécéssaire et suffisante pour que X engendre $\mathscr{E}$ est que X contienne $n+1$ points $x_0, \dots, x_n$ tels que les vecteurs $\overrightarrow{x_0x_i}$ $(i = 1 \dots n)$ forment une base de E.

Notons que la dernière condition est vérifiée pour tout polygne régulier à au moins 3 côtés. *En pratique, pour un tel polygône régulier, on identifiera $\mathbf{Iso}(P)$ avec le sous-groupe des isométries affines de $\mathscr{E}$ qui envoient P sur P bijectivement.*

Définition 3.82. Le groupe diédral d'ordre $2n$ est le groupe des isométries du polygone régulier à n-sommets dont les sommets sont $\left\{\exp\left(\frac{2ik\pi}{n}\right),\ k=0,\dots n-1\right\}$. On le notera D_n

Remarque 3.83. Attention, dans la littérature on l'appelle parfois groupe diédral d'orde n (ce qui est confusant...). Et parfois D_n est noté D_{2n}, ce qui est également confusant...

Le choix du polygone régulier n'est pas important car :

Proposition 3.84. *Si P et Q sont deux polygones réguliers à n-sommets alors $\mathbf{Iso}(P)$ et $\mathbf{Iso}(Q)$ sont des groupes isomorphes.*

Avant de démontrer cette proposition, notons le lemme suivant.

Lemme 3.85. *Soit P et Q deux polygones réguliers. Alors il existe une similitude f telle que $f(P) = Q$.*

Démonstration. Par le lemme 3.76 on a qu'il existe des similitudes $h : P \cong \mu_n$ et $g : Q \cong \mu_n$ où μ_n est le polygone des racines n-ièmes de l'unité. Mais alors $g^{-1} \circ h$ est une similitude (car les similitudes forment un groupe) et envoie P sur Q. □

Démonstration du corollaire 3.84. On utilise une similitude $f : P \cong Q$ donnée par le lemme 3.85. Alors on a $\mathbf{Iso}(Q) = f \circ \mathbf{Iso}(P) \circ f^{-1}$. La seule difficulté c'est que f n'est pas une isométrie, donc il n'est pas aussi claire que si $\varphi \in \mathbf{Iso}(P)$, $f \circ \varphi \circ f^{-1}$ est une isométrie. Or si f est une similitude de rapport r, alors f^{-1} est de rapport $1/r$. Et on obtient, pour tout $x, y \in \mathbb{C}$,

$$d\Big(f \circ \varphi \circ f^{-1}(x), f \circ \varphi \circ f^{-1}(y)\Big) = rd\Big(\varphi \circ f^{-1}(x), \varphi \circ f^{-1}(y)\Big)$$
$$= r\Big(f^{-1}(x), f^{-1}(y)\Big) = \frac{r}{r} d(x, y) = d(x, y).$$

C'est donc bien une isométrie. □

Exemple 3.86. On voit facilement que la rotation de centre 0 et d'angle $\dfrac{2\pi}{n}$ est un élément de D_n et qu'elle génère un sous-groupe d'ordre n.

On peut aussi vérifier que la symétrie par rapport à toute droite passant par un des sommets et 0 est un élément de D_n.

Ces deux éléments engendrent tout le groupe D_n.

Théorème 3.87. *Le groupe diédral D_n est un groupe non-commutatif fini avec $2n$ éléments. Il est engendré par un élément r d'ordre n et un élément s d'ordre 2. On a*

$$D_n := \big\{s^\epsilon r^i, \epsilon \in \{0, 1\}, i \in \{0, \dots n-1\}\big\}$$

et la structure de groupe est donnée par la relation

$$srs = srs^{-1} = r^{-1}$$

qui implique

$$s^\epsilon r^i s^\tau r^j = s^{\epsilon+\tau} r^{j-i}. \tag{37}$$

Démonstration. La preuve du théorème est similaire à celle fait en TD dans les cas $n = 3$ et $n = 4$. Rappelons les points essentiels. Notons $A_k = \exp(\frac{2ik\pi}{n})$ les sommets de P_n. La propriété d'isométrie fait qu'un élément $f \in D_n$ envoie un sommet sur un sommet et 0 sur 0. En particulier, on a au plus n possibilités pour l'image $f(A_0)$ de A_0.

Par ailleurs, tout sommet A_i a exactement deux sommets qui sont à distance minimale de lui parmis tous les sommets : il s'agit de A_{i+1} et A_{i-1} (on regarde les indices modulo n bien sûr). Ainsi, comme f est une isométrie, il suit que si $f(A_0) = A_i$, $f(A_1)$ est soit A_{i+1} soit A_{i-1}. On a donc plus que deux choix pour $f(A_1)$. Maintenant $f(A_2)$, par argument de minimalit de la distance est forcé : c'est l'autre sommet voisin de $f(A_1)$ qui n'est pas $f(A_0)$ et de proche en proche, l'image de tout sommet est fixée.

On a donc au plus $2n$ éléments dans D_n. On vérifie que les rotations donnent n valeurs différentes (en effet la rotation r est d'ordre n). Les composées sr^i donnent également n isométries distinctes qui réalisent les n possibilités manquantes du coup. Ce qui donne que D_n est de cardinal $2n$ et s'écrit comme énoncé dans le théorème. Un calcul explicite donne la formule énoncée pour le produit. □

Remarque 3.88. Il suit qu'en tant qu'*ensemble* $D_n = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mais en tant que *groupe* ce n'est *PAS* le produit direct de ces groupes. Il s'agit encore d'un produit semi-direct (comme pour le groupe affine vis à vis des groupes linéaires et translation).

Remarque 3.89. En particulier, on vient de voir qu'il existe un groupe d'ordre $2n$ non-abélien pour tout $n \geq 3$.

Pour $n = 3$, on peut montrer que $D_3 \cong S_3$. En revanche ce n'est pas vrai pour $n > 3$ (ne serait-ce que pour des raisons de cardnal). par ailleurs D_4 n'est pas isomorphe au groupe (vu en devoir maison) Q_8 non plus.

Remarque 3.90. La description de D_n donnée dans le théorème 3.87 le caractérise complètement : on a donné ses éléments et la loi de groupe est définie par l'égalité (37). Et on peut vérifier facilement que ceci définit bien une structure de groupes. Il n'est pas complètement évident si on part de cette définition algébrique de voir que ce groupe est isomorphe à un sous-groupe de $\mathbf{Aff}(\mathbb{R}^2) \cong \mathbf{Aff}(\mathbb{C})$ et a un sens géométrique précis. Ceci illustre qu'on peut définir et voir des groupes avec des points de vue différents de manière générale.

III. Appendice : compléments hors-progamme

Nous donnons dans les pages suivantes quelques résultats et remarques supplémentaires qui ne sont pas au programme du cours. Mais pourront être utile comme référence plus tard ou pour les élèves curieux. On commencera par la classification des isométries en dimension 3.

1. Aperçu des isométries en dimension supérieure

1.1. **Cas de la diemnsion 3.** En dimension 3, nous avons par le théorème 1.13 que toute isométrie affine est un produit d'au plus 4 réflexions. On peut classifier toutes les isométries de l'espace en fonction du nombre minimum de réfélexions requises pour les décrire. De manière analogue à ce qu'on a vu dans le cas plan.

On dispose bien entendu des cas suivants que nousa vons déjà vu :

- des réflexions,
- des composée de deux réflexions qui sont directes : ce qui nous donne, comme dans le cas plan, soit une translation, si les plans des réflexions sont parallèles, soit une rotation de l'espace comme nous l'explicitons ci-dessous.

En dimension 3, nous avons la définition suivante analogue à celle de la dimension 2.

Définition 1.1 (rotations dans l'espace)**.** Une rotation vectorielle d'un espace euclidien E de dimension 3 est un élément de $SO(E)$.

Soit $\mathscr{E}$ un espace *affine* euclidien de dimension 3. Une rotation de $\mathscr{E}$ est un élément r de $\mathbf{Iso}(\mathscr{E})$ tel qu'il existe $x_0 \in \mathscr{E}$ tel que $r \in SO_{x_0}(\mathscr{E})$.

Autrement dit une rotation affine dans l'espace est l'image d'une rotation vectorielle (identifiée avec une application affine préservant un point arbitraire de l'espace affine).

Lemme 1.2. *Une isométrie r est une rotation si et seulement si il existe deux plans $\mathscr{H}$, $\mathscr{H}'$ qui s'intersectent tels que $r = s_{\mathscr{H}} \circ s_{\mathscr{H}'}$.*

Démonstration. Un élément de $SO(E) \cong SO_{x_0}(\mathscr{E})$ peut s'écrire comme un produit de deux réflexions (d'hyperplans H, H' non égaux sauf si la rotation est l'identité) d'après le théorème 1.13 (en effet toute isométrie linéaire est le produit d'au plus 3 réflexions. Mais le cas de 3 réflexions est une isométrie indirecte (car si on a trois siométries indirectes s, s', s", alors $\det(s \circ s' \circ s'') = \det(s)\det(s')\det(s") = (-1)^3 = -1$). Donc une rotation s'écrit bien sous la forme annoncée (avec $\mathscr{H} = x_0 * H$, $\mathscr{H}' = x_0 * H'$).

Réciproquement, si on prend $x_0 \in \mathscr{H} \cap \mathscr{H}'$, alors, par définition, x_0 est un point fixe de $s_{\mathscr{H}}$, $s_{\mathscr{H}'}$ et donc $s_{\mathscr{H}} = \overrightarrow{s_{\mathscr{H}}}_{x_0}$ est dans $SO_{x_0}(\mathscr{E})$. Et de même pour $s_{\mathscr{H}'}$. La composée de ces symétries linéaires $\overrightarrow{s_{\mathscr{H}}} \circ \overrightarrow{s_{\mathscr{H}'}}$ est donc un élément de $SO(E)$ (car composée de deux isométries indirectes). Et donc r est dans l'image dans $SO_{x_0}(\mathscr{E})$. □

Notons que comme ces deux plans s'intersectent, ils sont donc soit égaux, auquel cas la composée est id, soit leur intersection est une unique droite $\mathscr{D}$, qui est constituée de points fixes de la rotation (puisque fixe pour chaque symétrie orthogonale).

Exemple 1.3 (**Comment décrire géométriquement une rotation dans l'espace)**. L'intersection de deux plans $\mathscr{H}$, $\mathscr{H}'$ est une droite $\mathscr{D}$ fixe par la rotation. Si $M \in \mathscr{E} \setminus \mathscr{D}$, alors la rotation se restreint au plan orthogonal $\mathscr{P}$ à $\mathscr{D}$ passant par M qui est une rotation plane. L'image de M par cette rotation (plane) est précisément $r(M)$!

Autrement dit une rotation de l'espace est la donnée d'une droite-*son axe*-et d'une rotation plane fixée qui agit sur chaque plan orthogonal (avec son centre précisément sur la droite)

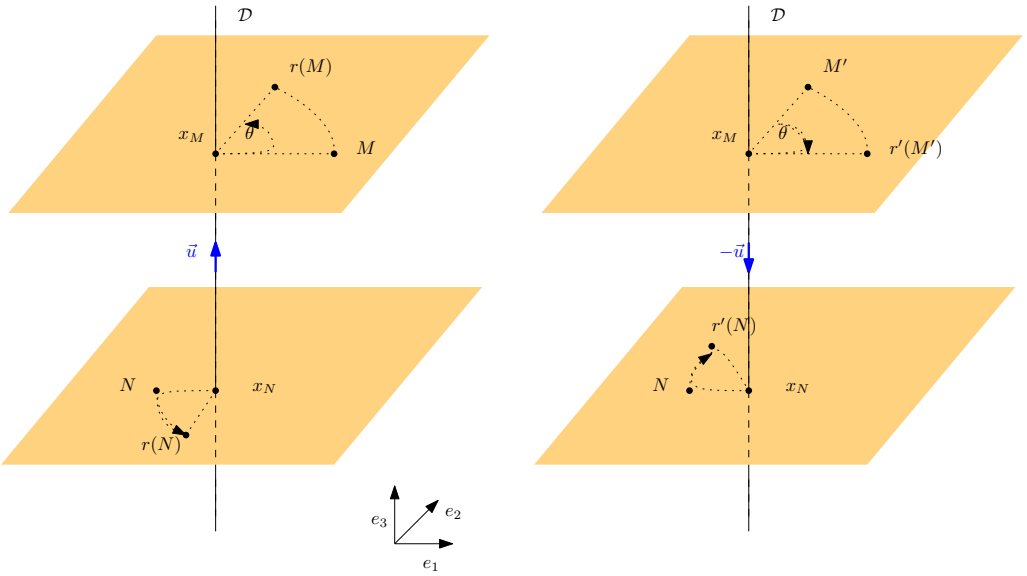


FIGURE 15. À gauche, la rotation $r = r_{\mathscr{D},\vec{u},\theta}$ d'axe $\mathscr{D}$ et à droite la rotation $r' = r_{\mathscr{D},-\vec{u},\theta}$ de même axe $\mathscr{D}$ et même angle mais vecteur directeur opposé. On a dessiné la base canonique (e_1, e_2, e_3) de $\mathbb{R}^3$ utilisée pour définir les bases directes.

Plus précisément, une rotation différente de l'identité dans l'espace se décrit comme suit. Soit $\mathscr{D} = \mathscr{H} \cap \mathscr{H}'$ la droite d'intersection des deux plans. Cette droite est évidemment fixe puisque chaque réfléxion la laisse fixe. Si maintenant M est un point de $\mathscr{E}$ qui n'est pas dans $\mathscr{D}$, alors on dispose du plan $\mathscr{P} = M * D^{\perp}$ orthogonal à $\mathscr{D}$ passant par M. L'image d'un point de $\mathscr{P}$ par $s_{\mathscr{H}}$ et $s_{\mathscr{H}'}$ est dans $\mathscr{P}$ (par orthogonalité). Il suit que cette composée se restreint à ce plan et y est une rotation plane. Autrement dit l'image de M est l'image par une rotation plane de plan $\mathscr{P}$, précisément la rotation donnée par la composée des réflexions $s_{\mathscr{H}\cap\mathscr{P}} \circ s_{\mathscr{H}'\cap\mathscr{P}}$ dans $\mathscr{P}$. Voir la figure (15) et la figure (17)

Nous allons voir comment décrire cela en termes de vecteur et d'angle θ. Pour faire celà il y a une subtilité.

A priori $\mathscr{P}$ n'est pas canoniquement isomorphe à $\mathbb{C}$ ou toute orientation de $\mathbb{R}^2$ (et donc on ne sait pas dire dans quel sens tourner lorsqu'on parle de l'angle d'une rotation). On y remédie de la façon suivante :

Fixons un vecteur unitaire $\vec{u}$ de $\mathscr{D}$ et une orientation de $\mathscr{E}$, c'est à dire le choix d'une notion de base directe de E.

Notons que ceci donne une orientation de tout plan orthogonal $\mathscr{P}$ à $\mathscr{D}$ en décidant qu'une base (p_1, p_2) de P est directe si la base $(p_1, p_2, \vec{u})$ est directe dans E. Comme $\mathscr{P}$ est orienté, on peut définir sans ambiguïté ce que signifie une rotation d'angle θ dans $\mathscr{P}$.

Définition 1.4. La rotation $r_{\mathscr{D},\vec{u},\theta}$ *d'axe* $\mathscr{D}$ est l'application définie, pour tout $M \in \mathscr{E}$, par

$$r_{\mathscr{D},\vec{u},\theta}(M) = x_M * \left(r_\theta(\overrightarrow{x_M M})\right) \tag{38}$$

où x_M est le point de $\mathscr{D}$ tel que $\overrightarrow{x_M M}$ est orthogonal à $\mathscr{D}$ et r_θ) est la rotation d'angle θ dans le plan orthogonal à $\mathscr{D}$ passant par M.

Noter que $r_{\mathscr{D},-\vec{u},\theta} = r_{\mathscr{D},\vec{u},-\theta}$.

Lemme 1.5. *Une rotation différente de id d'un espace (affine) euclidien de dimension 3 admet exactement une droite de points fixes, appelée* **l'axe de la rotation**.

Si $\mathscr{P}$ est un plan orthogonal à l'axe d'une rotation r ($\neq id$), alors $s_{\mathscr{P}}$ commute avec r.

Démonstration. On utilise la description explicite de l'exemple 1.3 ci-dessus (après avoir fixée une orientation de l'espace et de l'axe bien sûr). Le résultat est alors une conséquence de la formule (38) que si $M \notin \mathscr{D}$, alors $r_\theta(\overrightarrow{x_M M}) \neq \overrightarrow{x_M M}$ et donc M n'est pas fixe. On sait déjà que les points de $\mathscr{D}$ sont fixes ce qui conclut.

Pour la deuxième assertion, on utilise que si on écrit $\overrightarrow{x_0 M} = h + w$ avec $h \in P$ (la direction de $\mathscr{P}$ et $w \in D$ (la direction de l'axe de r), alors on a pour tout $M \in \mathscr{E}$ et $x_0 \in \mathscr{P}$ que

$$r \circ s_{\mathscr{P}}(M) = x_0 * \Big(r\big(w - h\big)\Big) = x_0 * \Big(\overrightarrow{r_\theta}(w) - h\Big)$$

où $\overrightarrow{r_\theta} : P \to P$ est la rotation d'angle θ linéaire du plan (pour l'orientation induite sur P).

Comme le vecteur $\vec{r_\theta}(w)$ est dans P, on a que $s_P(\vec{r_\theta}(w)) = \vec{r_\theta}(w)$. On en déduit que

$$s_{\mathscr{P}} \circ r(M) = s_{\mathscr{H}}\Big(x_0 * \big(\overrightarrow{r_\theta}(w) + h\big)\Big) = x_0 * \Big(\overrightarrow{r_\theta}(w) - h\Big) = r \circ s_{\mathscr{P}}(M).$$

□

Exemple 1.6. Si on compose trois réflexions, on a forcément une isométrie indirecte.

- On peut donc retrouver une *réflexion ou une réflexion glissée* comme en dimension 2 : c'est le cas d'une isométrie qui s'écrit comme composée d'une réflexion de plan $\mathscr{H}$ et de deux plans parallèles et orthogonaux à $\mathscr{H}$.
- Mais on a aussi le cas du composée de trois réflexions d'hyperplans orthogonaux deux à deux. Dans ce cas là l'application linéaire associée est $-I_3$. On a une homothétie de rapport -1. Autrement dit une symétrie centrale !

Enfin le dernier cas (pour les composées de 3 réflexions) possible est celui d'une anti-rotation.

Exemple 1.7 (**anti-rotation)**. Une anti-rotation est une isométrie a indirecte de l'espace obtenue comme la composée d'une rotation non-triviale d'axe $\mathscr{D}$ et d'une réflexion d'axe orthogonale à $\mathscr{D}$. Son application linéaire associée s'écrit $\overrightarrow{a} = P \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix} {}^tP$ où P est orthogonale où θ est une mesure de l'angle de la rotation.

L'intersection de l'axe et de l'hyperplan est l'unique point fixe de l'anti-rotation.

Il existe aussi des isométries qui *nécessitent* d'être obtenue comme la *composée de 4 réflexions*, qui sont forcément directes (puisque on a un nombre pair de telles réflexions). C'est le cas maximal et analogue du cas des réflexions glissées de la dimension 3.

Exemple 1.8 (**Vissage)**. Un vissage non-trivial [35] est la composée $t_{\overrightarrow{v}} \circ r$ d'une rotation d'axe $\mathscr{D}$ (non-triviale) de l'espace et d'une translation de vecteur $\overrightarrow{v} \in D \setminus \{0\}$ (la direction de $\mathscr{D}$) . Elle s'obtient donc comme la composée de 4 réflexions, dont deux des réflexions sont orthogonales à l'intersection des deux autres (en utilisant le deuxième point de 1.5). Voir la figure (17).

Le théorème suivant récapitule la liste de toutes les isométries du plan et de l'espace.

Théorème 1.9. *Les isométries d'un plan affine euclidien et d'un espace affine euclidien de dimension 3 sont exactement données par le tableau suivant et l'identité.*

35. on peut étendre la définition en incluant des rotations ou translations triviales mais on retombe alors dans une catégorie précédente et on a plus la nécessité de 4 réflexions

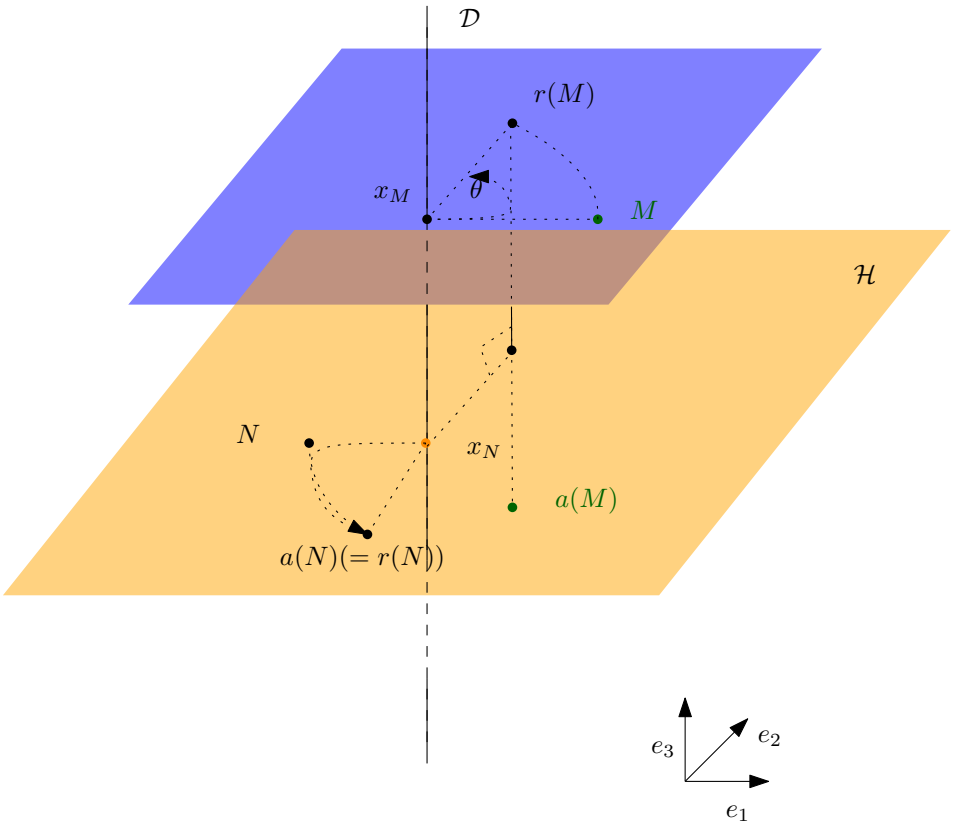


FIGURE 16. une antirotation a obtenue comme la composée d'une rotation d'axe $\mathscr{D}$ et angle θ et de la réflexion d'hyperplan orthogonal $\mathscr{H}$. On a représenté en verts un point M et son image $a(M)$. Ainsi que l'image d'un point N dans $\mathscr{H}$

Dim 2	**Nombre minimal de réflexions**	**Points fixes**	**Points fixes de l'application linéaire associée** [36]**.**
Réflexions	*1*	*1 droite*	*1 droite*
Translations	*2 réflexions de droites parallèles*	*Aucun point fixe*	*Toute droite*
Rotations	*2 réflexions de droites sécantes*	*1 seul point fixe*	*Aucune*
Symétrie glissée	*3 réflexions*	*Aucun*	*une droite*
Dim 3			
Réflexions	*1*	*1 plan*	*1 plan*
Translations	*2 plans parallèles*	*aucun*	*1 droite*
Rotations	*2 de plans se coupant*	*1 droite*	*1 droite*
Réflexions glissées	*3*	*aucun*	*1 plan*
Anti-rotations	*3 dont une de plan orthogonal aux deux autres*	*1 point*	*aucune*
Vissage	*4*	*aucun*	*1 droite*

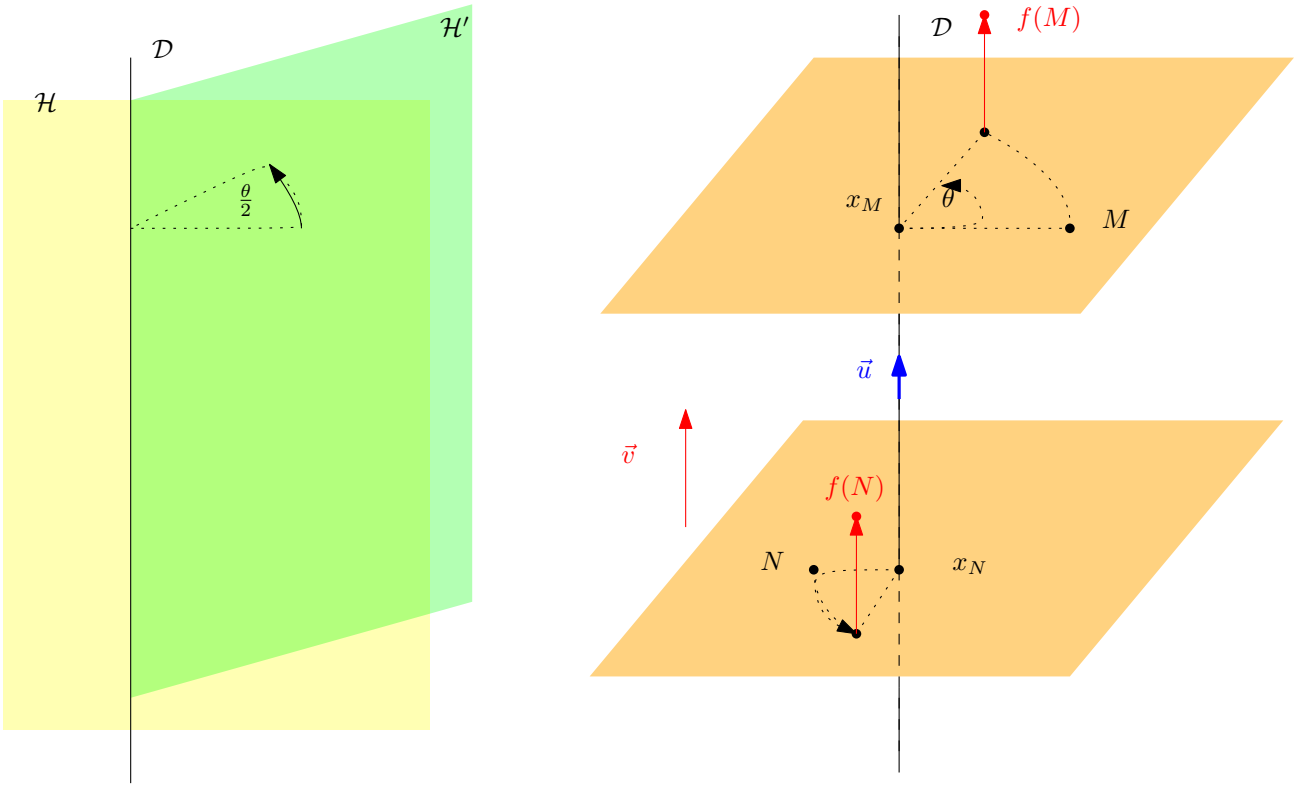


FIGURE 17. Deux réflexions engendrant la rotationd d'axe $\mathscr{D}$ de la figure (38). À droite un vissage f de vecteur $\vec{v}$ obtenu comme la composée de la rotation avec la translation de vecteur $\vec{v}$

Exemple 1.10. Un cas particulier d'anti-rotation est la symétries centrale [37]. Elle s'obtient comme composée de 3 de plans orthogonaux et c'est une anti-rotation d'angle π. Elle n'a qu'un seul point fixe et aucune direction fixe.

Démonstration. On a déjà vu le cas plan. Pour le reste la preuve est basée sur le théorème 1.13 et la proposition 1.16. En effet ce dernier donne la forme de toutes les isométries linéaires. À isomorphisme euclidien affine près, il suffit de considérer le cas de l'espace affine $\mathbb{R}^3$. Et par ailleurs, le théorème de structure nous dit que toute isométrie affine ψ est la composée

$$\psi = t_u \circ f$$

avec f isométrie linéaire (fixant 0).

D'après la proposition 1.16, on a 4 forme possibles (à conjugaison près) pour la matrice de f. Ci-dessous, P sera une matrice orthogonale.

(1) Soit $f = \mathrm{id}$, auquel cas ψ est une translation, et le reste des affirmations est facile.

(2) Soit $f = P \begin{pmatrix} -1 & 0 \\ 0 & I_2 \end{pmatrix} {}^tP$, alors f est une réflexion linéaire. On note H son espace propre associé à 1. Alors en décomposant $u = h + v$ avec $v \in H^\perp$, $h \in H$ on obtient que $\psi = t_h \circ (t_v \circ s_H)$. Or si v est orthogonal à H, on a que $t_v \circ s_H = s_{v/2+H}$. C'est donc une symétrie orthogonale de plan affine $v/2 + H$ et de direction H. En effet, pour tout $z = h' + v'$ avec $h' \in H$, $v' \in H^\perp$, on a

$$t_v \circ s_H(z) = t_v(h' - v') = h' + v - v' = h' - (v' - v/2) + v/2 = s_{v/2+H}(z).$$

37. = homothétie de rapport -1

Il suit que $\psi = t_h \circ s_{v/2+H}$ est une symétrie glissée (possiblement une symétrie si $h = 0$).

(3) Soit $f = P \begin{pmatrix} 1 & 0 & \\ 0 & 0 & \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix} {}^tP$ où $\theta \notin 2\pi\mathbb{Z}$ (on a donc inclus le cas de la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -I_2 \end{pmatrix}$ dans cette étude). Alors $f \in SO_3(\mathbb{R})$ et est une rotation d'axe D et d'angle θ (pour l'orientation fixée par le changement de base donné par la matrice de passage orthogonale P). On peut alors écrire $u = h + v$ avec $v \in D$ et $h \in D^\perp$ de manière unique. Et on a $\psi = t_v \circ (t_h \circ r_{0+D,\theta})$. Or $t_h \circ r_{D,\theta} = r_{(\mathrm{id}-r_\theta)^{-1}(h)+D,\theta}$ est encore une rotation. En effet pour tout $z = h' + v'$ avec $h' \in D^\perp$, $v' \in D$, on a

$$t_h \circ r_{0+D,t\theta}(z) = r_\theta(h') + u' + h = r_\theta(h') + u' - (r - \mathrm{id})(\mathrm{id} - r)^{-1}(h) = r_\theta(h' - (\mathrm{id} - r)^{-1}(h)) + (\mathrm{id} - r)^{-1}(h).$$

On obtient donc que $\Psi = t_u \circ r_{(\mathrm{id}-r_\theta)^{-1}(h)+D,\theta}$ est un vissage d'axe $(\mathrm{id} - r_\theta)^{-1}(h) + D$ (ou une rotation si $v = 0$).

(4) Le dernier cas est $f = P \begin{pmatrix} 1 & 0 & \\ 0 & 0 & \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix} {}^tP$ où $\theta \notin 2\pi\mathbb{Z}$ (on a donc inclus le cas de la matrice $-I_3$ dans cette étude). Cette matrice est la composée de la réflexion s_H d'hyperplan H (qui est l'espace propre associé à la valeur propre 1 de f) et la rotation d'axe $H^\perp$ et d'angle θ. C'est une anti-rotation de cente 0 donc. Pour trouver ψ, on écrit encore $u = h + v$ avec $h \in H$ et $v \in H^\perp$. On a que

$$\Psi = t_u \circ f = t_v \circ t_h \circ s_H \circ r_{H^\perp,\theta} = (t_v \circ s_H) \circ (t_h \circ r_{H^\perp,\theta}$$

en utilisant que t_h et s_H commutent. D'après les calculs dans les deux derniers cas ci-dessus, on obtient que

$$\Psi = s_{v/2+H} \circ r_{(\mathrm{id}-r_\theta)^{-1}(h)+H^\perp,\theta}$$

qui est bien une anti-rotation.

Les propriétés d'invariance sont des corollaires des formes des matrices.

Notons que pour la minimalité, on a d'une part que les isométries données se décomposent sous la forme donnée. D'autre part, si Ψ se décompose en deux réflexions, alors soit elles sont parallèles et on a vu qu'on a une translation soit elles se coupent et on a vu qu'on avait une rotation. Si on a un minimum de 4 réflexions, alors on est une isométrie positive, et pas une rotation (car sinon 2 symétries suffiraient).Dans la description ci-dessus, le seul cas restant est un vissage (non-trivial). De même si on se décompose en trois symétries au minimum, alors on est une isométrie indirecte et l'étude des cas ci-dessus montre qu'on est soit une anti-rotation, soit une réflexion glissée non-triviale (sinon on aurait une réflexion). □

1.2. **Rotations vectorielles, dimension n, $SO_n(\mathbb{R})$.** On donne ici quelques résulats sur les isométries en dimension quelconque.

Commençons par des (r)appels du cours d'algèbre linéaire et euclidienne.

Lemme 1.11. *Le sous-ensemble $SO_n(\mathbb{R}) := \{M \in O_n(\mathbb{R}),\ \det(M) = 1\} = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$ est un sous-groupe normal de $O_n(\mathbb{R})$. On l'appelle le groupe* spécial orthogonal. *Le quotient $O_n(\mathbb{R})/SO_n(\mathbb{R})$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}$.*

Démonstration. On a que $O_n(\mathbb{R})$ est un groupe d'après le cours d'algèbre linéaire et $SL_n(\mathbb{R}) = \ker(\det)$ en est un aussi. Leur intersection [38] est donc un sous-groupe en vertu du

38. on peut aussi directement vérifier les propriétés de sous-groupes. Ce n'est pas très dur ici

résultat général sur les intersections de groupes. Qu'il soit normal provient du fait que c'est le noyau de la restriction du morphisme de groupes det à $O_n(\mathbb{R})$. Par le premier théorème d'isomorphisme des groupes (cf le corrigé du TD5), on a que $O_n(\mathbb{R})/SO_n(\mathbb{R}) \cong \mathrm{Im}(\det)$. Mais le déterminant d'une matrice orthogonale est dans $\{\pm 1\}$ (et les deux cas sont possibles). Donc $O_n(\mathbb{R})/SO_n(\mathbb{R})$ est de cardinal 2 et donc forcément isomorphe à $\mathbb{Z}/2\mathbb{Z}$. □

On a la caractériation suivante des éléments de $O_n(\mathbb{R})$.

Proposition 1.12. *Une matrice $M \in M_n(\mathbb{R})$ est un élément de $O_n(\mathbb{R})$ si et seulement si ses vecteurs colonnes forment une base orthonormée*[39].

Démonstration. Voir le cours d'algèbre 4. □

On rappelle que la proposition est vraie pour $O(E)$ avec E euclidien plus généralement.

1.3. **Décomposition des isométries.** Les isométries d'un espace affine euclidien quelconques sont engendrées par les réflexions (tout comme les permutations sont engendrées par les transpositions).

Le nombre minimal de réflexons nécessaire dépend de la dimension par une formule très simple :

Théorème 1.13. *Soit $(\mathscr{E}, E, *)$ un espace affine euclidien de dimension n.*

- *Toute isométrie linéaire non-triviale $f \in O(E)$ peut s'écrire comme une composée d'au plus n réflexions (linéaires).*
- *Toute isométrie non-triviale $\varphi \in \mathbf{Iso}(\mathscr{E})$ peut s'écrire comme une composée d'au plus $n+1$ réflexions.*

On notera la **différence de** 1 **entre le cas affine et le cas linéaire**, qui est essentiellement due aux translations !

Remarque 1.14. Le théorème dit en particulier que les réflexions sont une famille de générateurs des isométries : $\langle s,\ s \text{ réflexion}\rangle = \mathbf{Iso}(\mathscr{E})$. Il donne en plus une borne précise sur le nombre maximal de réflexions nécessaires.

Exemple 1.15. En dimension 2, on voit qu'il suffit d'au maximum 3 réflexions. Ce qui permet de retrouver la classification des isométries que l'on a vu (théorème 3.63). En effet, nous avons vu ci-dessus que la composée de deux symétries est une rotation si les droites se coupent et une translation sinon. Pour la composée de 3 symétries, il faut distinguer si deux d'entre elles sont parallèles ou pas. On laisse le lecteur faire des essais et réflèchir aux différents cas.

On (r)appelle du cours d'algèbre linéaire que par ailleurs, on a la forme suivante pour les matrices orthogonales.

Proposition 1.16. *Soit $M \in O_n(\mathbb{R})$. Alors, M est* conjuguée par une matrice orhtogonale *à une unique matrice de la forme* $\begin{pmatrix} I_p & 0 & 0 & 0 & 0 \\ 0 & -I_q & 0 & 0 & 0 \\ 0 & 0 & C_1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & C_k \end{pmatrix}$ *où les C_i sont des matrices blocs de $SO_2(\mathbb{R})$, de la forme* $\begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$, *avec $\theta_i \neq 0 + \pi\mathbb{Z}$.*

39. évidement par rapport à al structure euclidienne usuelle de $\mathbb{R}^n$

Preuve du théorème 1.13. Il suffit de démontrer le résultat pour chaque $\mathbb{R}^n$ car tout espace euclidien affine de dimension n est isomorphe à $\mathbb{R}^n$.

On peut le faire par récurrence forte. Le résultat est trivial pour $n = 0$. Regardons l'initialisation pour $n = 1$ également. On a que $O_1(\mathbb{R}) = \{\mathrm{id}, s\}$ où s est la symétrie centrale par rapport à 0 qui est aussi la réflexion par rapport au (seul) hyperplan $\{0\}$ dans $\mathbb{R}$. On a donc qu'il suffit d'au plus 1 réflexion...

Dans le cas affine, nous avons uniquement deux types d'isométries affines f. Soit $\overrightarrow{f} = s$, auquel cas on a une réflexion par rapport à un point x_0 (notons qu'on a forcément un point fixe dans ce cas puisque s n'a pas un comme valeur propre, ce qui permet de démontrer ce résultat). Sinon $\overrightarrow{f} = \mathrm{id}$ auquel cas f est une translation de vecteur $\overrightarrow{u}$ et s'obtient donc comme une composée de deux réflexions par rapport à deux points x_0, $x_1 \in \mathbb{R}$ tels que $\overrightarrow{x_0x_1} = \frac{1}{2}\overrightarrow{u}$.

Supposons avoir démontré le résultat en dimension $\leq n$. Et démontrons le en dimension $n + 1$.

Prenons f une isométrie. Si $\overrightarrow{f}$ admet 1 ou -1 comme valleur propre, alors il existe une droite vectorielle D stable par $\overrightarrow{f}$ et notons $D^\perp$ l'hyperplan orthgonal à D. Quitte à composer $\overrightarrow{f}$ par la réflexion d'hyperplan $D^\perp$, on est ramené au cas d'une isométrie linéaire (soit f, soit $s_{D^\perp} \circ f$) telle que D est une droite propre associée à la valeur propre 1. Auquel cas dans une base adaptée à la décomposition $D \bigoplus D^\perp = \mathbb{R}^{n+1}$, on a que $\overrightarrow{f}$ (ou $s_{D^\perp} \circ \overrightarrow{f}$) s'écrit $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$ où A est la matrice d'une isométrie de $\mathbb{R}^n$. par hypothèse de récurrence c'est le produit d'au plus n réflexions linéaires (par rapport à disons $H_1, \dots H_i$). Et il suit que $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} = s_{H_1 \oplus D} \circ \cdots \circ s_{H_i \oplus D}$. Ainsi on a bien obtenu que $\overrightarrow{f}$ ou au pire $s_{D^\perp} \circ \overrightarrow{f}$ est un produit d'au plus n réflexions. Comme $\overrightarrow{f} = s_{D^\perp} \circ (s_{D^\perp} \circ \overrightarrow{f})$, on a au final que $\overrightarrow{f}$ est le produit d'au plus $n + 1$ réflexions. L'hypothèse de récurrence est démontrée dans ce cas.

Pour finir le cas linéaire, il faut vérifier ce qui se passe s'il n'y a aucune valeur propre réelle. Par la proposition 1.16, on obtient qu'il existe un plan stable P tel que $\overrightarrow{f}_{|P}$ est une rotation plane et donc la composée de deux réflexions $s_D \circ s_{D'}$ par rapport à des droites D et D' de P. Soit alors $H = D \oplus P^\perp$ et $H' = D' \oplus P^\perp$ qui sont des hyperplans. On obtient que $(s_{H'} \circ s_H \circ \overrightarrow{f})_{|P} = \mathrm{id}$ par un calcul direct. Ainsi dans une base adaptée à la décomposition $P \bigoplus P^\perp = \mathbb{R}^{n+1}$, on a que $s_{H'} \circ s_H \circ \overrightarrow{f}$ s'écrit $\begin{pmatrix} I_2 & 0 \\ 0 & B \end{pmatrix}$ où B est la matrice d'une isométrie de $\mathbb{R}^{n-1}$. Donc B s'écrit comme un produit de $n - 1$ réflexions au plus, et comme dans le cas précédent on obtient que $\begin{pmatrix} I_2 & 0 \\ 0 & B \end{pmatrix}$ est aussi un produit d'au plus $n - 1$ réflexions et finalement $\overrightarrow{f} = s_H \circ s_{H'} \circ (s_{H'} \circ s_H \circ \overrightarrow{f})$ est un produit d'au plus $n + 1$ réflexions.

Le cas linéaire est démontré. Pour le cas affine. Notons que si $\overrightarrow{f}$ n'a pas 1 pour valeur propre, alors le lemme 3.44 nous assure que f a un point fixe x_0 et donc $f \in O_{x_0}$ et on est ramené au cas linéaire. Ce qui conclut.

Sinon, f s'écrit $t_{\overrightarrow{u}} \circ \varphi$ avec $\varphi \in O_{x_0}$ d'après le théorème de structure 3.17. Comme $T_{\overrightarrow{u}}$ est une composée de deux réflexions, on est ramené à montrer que $\varphi = s \circ s' \circ f$ est une composée d'au plus $n + 2 - 2 = n$ réflexions. On est ramené au cas linéaire puisque φ a un point fixe et donc s'identifie à $\overrightarrow{\varphi}$ via l'isomorphisme $\mathbf{Iso}_{x_0}(\mathscr{E}) \cong O_{n+1}(\mathbb{R})$. Or $\overrightarrow{\varphi} = \overrightarrow{f}$ (toujours d'après le théorème de structure 2.52) et donc on est dans le cas linéaire

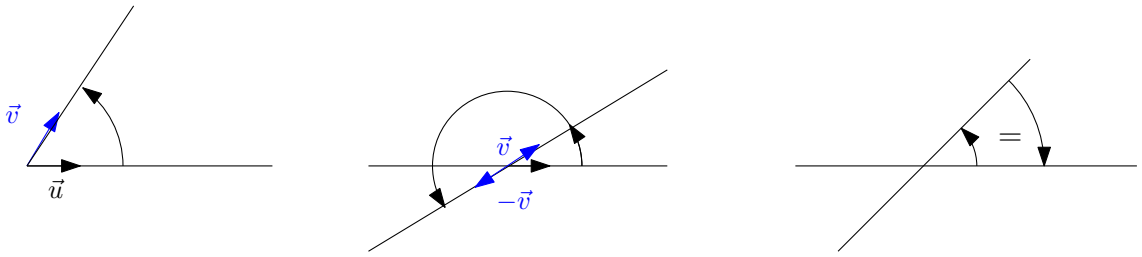


FIGURE 18. À gauche un angle orienté représenté par le couple de vecteurs $(\vec{u}, \vec{v})$; au milieu un angle orienté de droites et à droite un angle géométrique entre deux droites

précédent ou $\vec{f}$ avait 1 comme valeur propre. On a vu que dans ce cas, ce dernier était bien la composée d'au plus n-réflexions. Ce qui conclut ! □

2. Supplément 2 : la notion d'angle via les actions de groupes

On va revenir sur les rotations et la notion d'angle. Notamment autour de la relation (intuitive) entre cela et la notion et nécessité d'orientation que nous avons vu en décrivant les rotations en dimension 3. Vous avez évidemment une notion d'angle intuitive depuis au moins le collège, en tout cas de leur mesure. Ils existent par ailleurs trois notions d'angles :

- angles orientés de vecteurs,
- angles orientés de droites,
- angles non-orientés (aussi appelés géométriques).

Voir figure 18.

La définition intuitive (et qu'il faut garder en tête bien-sûr) est qu'un angle orienté de vecteurs est déterminé par l'intersection de deux demi-droites ou de manière équivalente par leurs deux vecteurs unitaires directeurs ; un angle orienté de droites est déterminé par l'intersection d'un couple de deux droites alors qu'un angle géométrique est déterminé par l'intersection d'un ensemble de deux droites (c'est à dire sans les ordonner ou décider laquelle est la première).

2.1. **Angles orientés et nombres complexes.** Pour être plus précis, on va introduire des actions de groupe et des quotients (comme d'habitude !). Dans toute la suite on considéra en général des vecteurs unitaires. Si un vecteur v n'est pas unitaire, le lecteur pourra lui associer le vecteur $\dfrac{v}{\|v\|}$ qui lui est unitaire.

Notation 2.1.
- On note $\mathscr{R}$ la relation, définie sur $S^1 \times S^1$, c'est à dire les couples de vecteurs de norme 1 de $\mathbb{C}$, donnée par $(x_1, y_1)\mathscr{R}(x_2, y_2)$ si il existe un élément $f \in SO_2(\mathbb{R})$ tel que $x_2 = f(x_1)$ et $y_2 = f(y_1)$.
- Plus généralement si P est un espace vectoriel euclidien de dimension 2, on note $\mathscr{R}$ la relation définie sur l'ensemble des couples de vecteurs *unitaires* de P par $(x_1, y_1)\mathscr{R}(x_2, y_2)$ si il existe un élément $f \in SO(\mathscr{P})$ tel que $x_2 = f(x_1)$ et $y_2 = f(y_1)$ (avec x_1, y_1, x_2, y_2 *unitaires*). Autrement dit on demande que les couples de vecteurs unitaires soit *directement isométriques*.
- On définit aussi la relation $\mathscr{R}_d$ sur les couples de vecteurs de norme 1 de P (et en particulier de $\mathbb{C}$) par

$$(x_1, y_1)\mathscr{R}_d(x_2, y_2) \text{ si } \begin{cases} (x_1, y_1)\mathscr{R}(x_2, y_2) \\ \text{ou} \\ (x_1, y_1)\mathscr{R}(-x_2, y_2) \end{cases}$$

Exercice 2.2. Vérifier que $\mathscr{R}$ et $\mathscr{R}_d$ sont des relations d'équivalence.

Définition 2.3. Un angle (orienté) de vecteur est une classe d'équivalence de la relation $\mathscr{R}$. Un angle orienté de droites est une classe d'équivalence de la relation $\mathscr{R}_d$.

Noter que cette définition a du sens dans tout plan euclidien (pas seulement $\mathbb{C}$ ou $\mathbb{R}^2$). Il est sous-entendu que les vecteurs sont évidemment des vecteurs du plan que l'on regarde.

À un couple de vecteur unitaires on peut donc associer l'angle $\overline{(u,v)}$ et à un couple de droites $\mathscr{D}$, $\mathscr{D}'$, on peut associer l'angle de droite $\overline{(u_{\mathscr{D}}, v_{\mathscr{D}'})}^d$ où $u_{\mathscr{D}}, v_{\mathscr{D}'}$ sont des vecteurs directeurs unitaires des droites. A bijection près, cet ensemble est indépendant du choix de P.

Lemme 2.4.
- *L'ensemble $\mathscr{A} = (S^1 \times S^1)/_{\mathscr{R}}$ des angles orientés est en bijection avec $SO_2(\mathbb{R})$ et donc aussi avec S^1.*
- *L'ensemble $\mathscr{A}_d = (S^1 \times S^1)/_{\mathscr{R}_d}$ des angles orientés de droites est le quotient $\mathscr{A}/\mathbb{Z}/2\mathbb{Z}$ où $\mathbb{Z}/2\mathbb{Z}$ agit sur $\mathscr{A}$ par $\overline{1}^2 * \overline{(u,v)} = \overline{(u,-v)}$.*
- *En particulier, $\mathscr{A}$ et $\mathscr{A}_d$ ont des structures de groupes abéliens tels que les bijections ci-dessus soient des isomorphismes de groupes.*
- *Les ensembles $\mathscr{A}(P)$ et $\mathscr{A}_d(P)$ des angles et angles orientés d'un plan euclidien P ont des structures de groupes isomorphes à celles de $SO(P)$ et du groupe quotient $SO(P)/\{\pm \mathrm{Id}\}$.*
- *Si $f : P \to \mathbb{C}$ est un isomorphisme euclidien, alors l'application $\overline{(u,v)} \mapsto \overline{(f(u), f(v)}$ est bien définie sur les quotients et est un isomorphisme de groupes $\mathscr{A}(P) \cong \mathscr{A}$ (ainsi que de $\mathscr{A}_d(P) \cong \mathscr{A}_d$.*

Autrement dit, *les angles forment naturellement un groupe* qui est (à isomorphisme près) *indépendant du plan euclidien choisi* ! Et on peut en particulier prendre la représentation que l'on préfère dans $\mathbb{C}$ ou $\mathbb{R}^2$.

Remarque 2.5. Le point clé est le fait qu'en dimension 2, pour tous vecteurs unitaires u, v, il existe une *unique* isométrie directe qui transforme u en v. C'est *FAUX* en plus grande dimension.

Maintenant qu'est ce que la *mesure d'un angle* ? C'est donné par la proposition suivante (que vous connaissez déjà en partie).

Proposition 2.6. *L'application* $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ \theta & \longmapsto & \exp(i\theta) \end{array}$ *est un morphisme de groupes de noyau $2\pi\mathbb{Z}$ qui induit par passage au quotient un isomorphisme de groupes $\mu : \mathbb{R}/2\pi\mathbb{Z} \cong S^1$ et la composée $\mathbb{R}/2\pi\mathbb{Z} \to S^1 \to \mathscr{A}$ est une bijection.*

On a de même un isomorphisme de groupes $\mathbb{R}/\pi\mathbb{Z} \cong \mathscr{A}_d$.

La proposition établit donc que à tout angle on peut associer un θ, bien défini modulo 2π uniquement, que l'on appelle sa mesure.

Terminologie 2.7. Une **mesure d'un angle** (orienté de vecteur) $a \in \mathscr{A}$ est la donnée d'un réel θ tel que $\mu(\theta) = a \in \mathscr{A}$. En général, on notera simplement θ cette mesure. On l'appelle souvent simplement *angle* ce qui ne pose aucun problème une fois une orientation du plan choisie (mais elle dépend du choix de cette orientation).

On définit de même une mesure d'angle orientée de droites.

Remarque 2.8. Dans l'identification du lemme 2.4, on a jamais besoin d'écrire explicitement les nombres complexes dans leur base $(1, i)$. On a juste besoin de vecteurs unitaires dans $\mathbb{C}$ et de la compréhension de $SO_2(\mathbb{R})$. En revanche dans la proposition 2.6, il faut avoir choisi une base de orthonormée de $\mathbb{C}$ (c'est à dire une orientation de $\mathbb{C}$) pour pouvoir écrire un nombre complexe sous la forme $\exp(i\theta) = \cos(\theta) + i\sin(\theta)$. En effet si on échange i et $-i$ on échange θ en $-\theta$.

En particulier une fois choisie une orientation de $\mathbb{C}$ (en général celle du sens trigonométrique), on peut écrire que

Lemme 2.9. *Tout élément de $SO_2(\mathbb{R})$ s'écrit $\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}$ où θ est unique modulo 2π.*

Les angles sont laissés fixes par les similitudes directes. C'est même une propriété qui les caractérise en dimension 2...

Proposition 2.10. *Les similitudes directes préservent les angles orientés. Le similitudes indirectes inversent les angles orientés.*

2.2. **Angles non-orientés.** On fait une parenthèse culturelle sur les angles non-orientés, appelés aussi géométriques, même si ne nous en servirons pas.

Pour définir les angles géométriques, on oublie l'ordre des deux droites.

Notation 2.11. Dans $\mathscr{A}$, on définit la relation $\overline{(u,v)} \sim \overline{(x,y)}$ si $\begin{cases} \overline{(u,v)} = \overline{(x,y)} \\ \text{ou} \\ \overline{(u,v)} = \overline{(y,x)} \end{cases}$

Autrement dit on identifie les angles associés aux couples (u,v) et (v,u).

Lemme 2.12. *La relation $\sim$ est une relation d'équivalence sur $\mathscr{A}$. Elle définit également ne relation d'équivalence sur $\mathscr{A}_d$.*

Définition 2.13. Un angle géométrique entre deux vecteurs est une classe d'équivalence pour la relation $\sim$ sur $\mathscr{A}$. Un angle géométrique entre deux droites est une classe d'équivalence pour la relation $\sim$ sur $\mathscr{A}_d$.

Remarque 2.14. Les ensembles quotients $\mathscr{A}/_\sim$ et $\mathscr{A}_d/_\sim$ n'ont plus de structure de groupes compatibles avec la projection canonique (on ne quotiente plus par un sous-groupe normal malheureusement).

La proposition 2.10 a l'analogue suivant.

Proposition 2.15. *Une similitude préserve les angles géométriques.*

Remarque 2.16. On peut définir la mesure d'un angle géométrique de la même façon que pour les angles orientés. Il suffit de prendre un antécédent dans $\mathbb{R}$ de l'application composée $\mathbb{R} \to S^1 \to \mathscr{A} \to \mathscr{A}/_\sim$ ce qui revient simplement à prendre la mesure de l'angle $\overline{(u,v)}$ ou de l'angle $\overline{(v,u)}$. Attention, on ne peut plus vraiment sommer ces angles puisque il n'y a plus de structures de groupes.

3. Supplément 3 : Isométries de figures géométriques - Symétries de figures

On va s'intéresser maintenant aux **symétries** d'objets géométriques. Ce que l'on encodera par des (quotients de) sous-groupes de $\mathbf{Iso}(\mathscr{E})$ (ou $\mathbf{Aff}(\mathscr{E})$...). Précisément, il s'agit des transformations isométriques (ou affines...) qui préserve une figure géométrique. Il y a de nombreuses symétries que l'on peut considérer ; les plus courantes et importantes seront celles données par ce que nous noterons $\mathbf{Iso}(X)$ dans la définition ci-dessous. On commence donc par le "catalogue" de groupes de symétrie suivant.

3.1. Groupes de symétrie de figures.

Définition 3.1 (Symétries d'un sous-ensemble affine)**.** Soit X un sous-ensemble d'un espace préhilbertien[40] $\mathscr{E}$. On lui associe les groupes de symétries suivants :

- Le groupe des isométries de X est $\mathbf{Iso}(X) := \{f \in \mathrm{Bij}(X),\ \exists \tilde{f} \in \mathbf{Iso}(\mathscr{E}),\ f = \tilde{f}_{|X}\}$.
- Le groupe des symétries affines de X est $\mathbf{Aff}(X) = \{f \in \mathrm{Bij}(X),\ \exists \tilde{f} \in \mathbf{Aff}(\mathscr{E}),\ f = \tilde{f}_{|X}\}$, c'est à dire les bijections de X qui sont les restrictions d'isomorphismes affines de l'espace.
- Le groupe des similitudes de X est $\mathbf{Sim}(X) := \{f \in \mathrm{Bij}(X),\ \exists \tilde{f} \in \mathbf{Sim}(\mathscr{E}),\ f = \tilde{f}_{|X}\}$.

On appelle aussi parfois $\mathbf{Iso}(X)$ le groupe des symétries (orthogonales) de X. Le lemme 3.2 garantit que ce sont bien des groupes.

Lemme 3.2. *Soit X un sous-ensemble d'un espace affine préhilbertien*[41] *$\mathscr{E}$. On a que $\mathbf{Iso}(X)$ est un sous-groupe de $\mathbf{Sim}(X)$ qui est un sous-groupe de $\mathbf{Aff}(X)$ qui est un sous-groupe de $(\mathrm{Bij}(X), \circ)$.*

Démonstration. Les inclusions $\mathbf{Iso}(X) \hookrightarrow \mathbf{Sim}(X) \hookrightarrow \mathbf{Aff}(X) \hookrightarrow \mathrm{Bij}(X)$ sont par définition (puisque une isométrie bijetcive est a fortiori une similitude bijective etc...). La preuve que ce sont des sous-groupes est la même pour les 3. On ne détaille que le cas $\mathbf{Iso}(X)$. Tout d'abord, $\mathrm{id} \in \mathbf{Iso}(X)$ puisque $\mathrm{id}(X) = X$ et que c'est la restriction de l'identité $\mathrm{id} : \mathscr{E} \to \mathscr{E}$. Soit $\tilde{f} \mapsto f$ l'application qui envoie un isométrie de $\mathscr{E}$ sur sa restriction $f = \tilde{f}_{|X}$ à X. Par hypothèse on ne s'intérèsse qu'aux isométries telles que cette restriction soit injective, d'image X (c'est à dire une bijection de X dans lui-même). On a par définition de la composée et de la restriction que

$$\left(\tilde{f} \circ \tilde{g}\right)_{|X} = \tilde{f}_{|X} \circ \tilde{f}_{|X} \tag{39}$$

Ceci prouve que si $f, g \in \mathbf{Iso}(X)$, alors leur composée aussi. En effet la composée de bijections est une bijection et si $\tilde{f}$, $\tilde{g}$ sont des isométries de $\mathscr{E}$ dont les restrictions sont f et g, alors leur composée est encore une isométrie de $\mathscr{E}$ dont la restriction (d'après la formule) est bien $f \circ g$; donc $f \circ g \in \mathbf{Iso}(X)$. De même

$$(\tilde{f}^{-1})_{|X} = (\tilde{f}_{|X})^{-1}$$

et on déduit similairement que si $f \in \mathbf{Iso}(X)$, $f^{-1} \in \mathbf{Iso}(X)$. □

Exemple 3.3 (Groupe diédral). Si X est un polygone régulier P_n à n-cotés, le groupe $\mathbf{Iso}(P_n)$ s'appelle le groupe diédral d'ordre $2n$. Il sera étudié en détail dans la partie 3.5.

Exemple 3.4 (Isométries d'une droite). Soit une droite $\mathscr{D}$ dans un espace euclidien $\mathscr{E}$. Choisissons x_0 quelconque dans $\mathscr{D}$. Si ψ est une isométrie de $\mathscr{E}$ qui préserve $\mathscr{D}$, alors, par le théorème 2.52 de structure ψ s'écrit comme la composée $t_{\vec{u}} \circ f$ où $f \in O_{x_0}(\mathscr{E})$ est une isométrie linéaire en x_0. En appliquant cette décomposition en x_0, on obtient que pour

40. pour $\mathbf{Aff}(X)$, il suffit que l'espace soit affine
41. là encore, la dernière inclusion est un sous-groupe dés que l'espace soit affine

que $\mathscr{D}$ soit stable il faut que u soit un vecteur de D (la direction de $\mathscr{D}$). De plus, pour que $\mathscr{D}$ soit stable il faut aussi que D soit une droite propre de f (sinon son image est une droite de direction différente de D). Ainsi, elle est donnée matriciellement dans une base orhtonormée de premier vecteur un vecteur de D par une matrice de la forme $\begin{pmatrix}\mu & 0\\ 0 & A\end{pmatrix}$. De plus deux matrices $\begin{pmatrix}\mu & 0\\ 0 & A\end{pmatrix}$ et $\begin{pmatrix}\lambda & 0\\ 0 & B\end{pmatrix}$ définissent la même restriction à D si et seulement si $\lambda = \mu$.

Ainsi les éléments $\mathbf{Iso}(\mathscr{D})$ à $\mathscr{D}$ est un élément de $O_{x_0}(\mathscr{D}) \cong O(\mathbb{R}) = \{\pm 1\}$.

Il suit que $\mathbf{Iso}(\mathscr{D}) \cong \mathbb{R} \times \{\pm 1\}$ est bien le même groupe que celui des isométries de l'espace euclidien $\mathscr{D}$ de dimension 1.

Cette remarque se généralise évidemment à tout sous-espace affine à la place de $\mathscr{D}$. Autrement dit la notation $\mathbf{Iso}(\mathscr{P})$ n'est pas ambigue pour un sous-espace $\mathscr{P}$ de $\mathscr{E}$.

Remarque 3.5 (Autres groupes de symétries naturels). Dans la définiton de $\mathbf{Iso}(X)$ (et de ses deux cousins dans la définition 3.1), on considère des bijections de X qui sont des restrictions d'isométrie globales (nécessairement affines) de $\mathscr{E}$. En particulier, on identifie dans $\mathbf{Iso}(X)$ des isométries qui sont *égales* sur X (mais pas forcément en dehors de X) ; ce ne sont pas forcément les mêmes groupes en général, par exemple voir 3.8. D'un autre côté, on peut aussi considérer des bijections de X dans lui même qui sont des isométries du sous-espace X (c'est à dire que pour tout $x, y \in X$, on a $\|\overrightarrow{f(x)f(y)}\| = \|\overrightarrow{xy}\|$) mais ne s'étendent pas forcément en des isométries affines globales de $\mathscr{E}$. Nous récapitulons ces groupes dans la définition suivante 3.6. Dans les exemples géométriques de figure que nous considérons ces groupes seront en fait souvent isomorphes, voir proposition 3.10.

Définition 3.6 (Variantes des groupes de symétrie)**.** Soit X un sous-ensemble d'un espace préhilbertien [42] $\mathscr{E}$. On dispose des groupes de "symétries" suivants :

- le groupe $\mathbf{Iso}_{|X}(\mathscr{E}) := \{f \in \mathbf{Iso}(\mathscr{E}),\ f(X) = X\}$ des isométries de $\mathscr{E}$ qui envoient X sur X (surjectivement) ;
- le sous-groupe $\mathrm{Bij}^{\mathbf{Iso}}(X) = \{f \in \mathrm{Bij}(X),\ /\ \forall x, y \in X, \text{ on a } \|\overrightarrow{f(x)f(y)}\| = \|\overrightarrow{xy}\|\}$ des isométries du sous-espace X ;
- le groupe $\mathbf{Aff}_{|X}(\mathscr{E}) := \{f \in \mathbf{Aff}(\mathscr{E}),\ f(X) = X\}$ des bijection affines de $\mathscr{E}$ qui envoient X sur X (surjectivement) ;
- le groupe $\mathbf{Sim}_{|X}(\mathscr{E}) := \{f \in \mathbf{Aff}(\mathscr{E}),\ f(X) = X\}$ des similitudes de $\mathscr{E}$ qui envoient X sur X (surjectivement).

Lemme 3.7. *On a que* $\mathbf{Iso}_{|X}(\mathscr{E})$, $\mathbf{Aff}_{|X}(\mathscr{E})$ *et* $\mathbf{Sim}_{|X}(\mathscr{E})$ *sont des sous-groupes de* $\mathbf{Iso}(\mathscr{E})$, $\mathbf{Aff}(\mathscr{E})$ *et* $\mathbf{Sim}(\mathscr{E})$ *respectivement. De plus* $\mathrm{Bij}^{\mathbf{Iso}}(X)$ *est un sous-groupe de* $(\mathrm{Bij}(X), \circ)$.

Démonstration. La preuve est similaire à celle de 3.2. □

Exemple 3.8 (isométries d'un point). Soit x_0 un point de $\mathscr{E}$ euclidien. Il y a une unique bijection de $\{x_0\}$ sur lui-même, qui est l'identité et est donc une isométrie. On en déduit que

$$\mathbf{Iso}(x_0) = \mathrm{Bij}^{\mathbf{Iso}}(x_0) = \{\mathrm{id}_{\{x_0\}}\}.$$

En revanche, on a vu (lemme 2.47) que l'ensemble des isométries qui laissent x_0 fixe est précisément $O_{\{x_0\}}(\mathscr{E}) \cong O(E)$. Ainsi

$$\mathbf{Iso}_{|x_0}(\mathscr{E}) = O_{\{x_0\}}(\mathscr{E})$$

est beaucoup plus gros que $\mathbf{Iso}(x_0)$ (sauf si $\dim(\mathscr{E}) = 1$). De même $\mathbf{Aff}_{|x_0}(\mathscr{E}) = GL_{x_0}(\mathscr{E})$ et $\mathbf{Aff}(x_0) == \{\mathrm{id}_{\{x_0\}}\}$.

Exemple 3.9. Si X et inclus dans un hyperplan $\mathscr{H}$ de $\mathscr{E}$, alors le noyau du

42. pour les variantes affines, il suffit encore une fois que l'espace soit affine

Proposition 3.10. *Soit X un sous-ensemble d'un espace préhilbertien*[43] $\mathscr{E}$.

- *L'application de restriction $f \mapsto f_{|X}$ d'une application au sous-ensemble X induit des morphismes de groupes surjectifs*
$$\mathbf{Iso}_{|X}(\mathscr{E}) \to \mathbf{Iso}(X), \quad \mathbf{Aff}_{|X}(\mathscr{E}) \to \mathbf{Aff}(X), \quad \mathbf{Sim}_{|X}(\mathscr{E}) \to \mathbf{Sim}(X).$$
- *De plus* $\mathbf{Iso}(X)$ *est un sous-groupe de* $\mathrm{Bij}^{\mathbf{Iso}}(X)$.
- *Supposons que X ne soit inclus dans aucun hyperplan de $\mathscr{E}$. Alors, les morphismes* $\mathbf{Iso}_{|X}(\mathscr{E}) \to \mathbf{Iso}(X)$ *et* $\mathbf{Iso}(X) \hookrightarrow \mathrm{Bij}^{\mathbf{Iso}}(X)$ *sont des isomorphismes. Autrement dit, tous ces groupes sont les mêmes*[44].

Démonstration. Comme la distance induite sur X est celle donnée par la distance préhilbertienne, le deuxième pint découle des défintions directement. Comme on l'a dit la preuve du lemme 3.2 nous assure que $\mathbf{Iso}_{|X}(\mathscr{E})$ et les autres variantes sont bien des sous-groupes. De plus la formule (39) nous assure que l'application de restriction $\tilde{f} \mapsto \tilde{f}_{|X} = f$ est un morphisme de groupes surjectif (ce dernier point étant par définition). Cela prouve la proposition modulo le fait de prouver que la restriction de tout élément de $\mathbf{Iso}_{|X}(\mathscr{E})$ à X est une bijection de X. Or une telle restriction de $\mathbf{Iso}(\mathscr{E})$ est injective puisque restriction d'une application injective. De plus l'image de X par f est X par hypothèse. Donc $f : X \to X$ est à la fois injective et surjective ce qui conclut pour les deux premiers points.

Le dernier point sera vu en TD. □

Remarque 3.11. La proposition 3.10 (et le premier theorème d'isomorphisme des groupes) nous dit donc que $\mathbf{Iso}(X)$ est le groupe quotient de $\mathbf{Iso}_{|X}(\mathscr{E})$ par le noyau de la restriction $f \mapsto f_{|X}$, c'est à dire le sous-groupe stab_X ((nécessairement normal) des isométries f de $\mathscr{E}$ telles que, pour tout $x \in X$, $f(x) = x$.

Remarque 3.12. Évidemment, on peut étendre les constructions $\mathbf{Iso}(X)$, $\mathbf{Iso}_{|X}(\mathscr{E})$ etc à tout type de sous-groupes. Par exemple on peut s'intéresse aux translations qui préservent une figure etc..

Exemple 3.13. Si X est inclus dans un hyperplan $\mathscr{H}$, alors le noyau du morphisme $\mathbf{Iso}_{|X}(\mathscr{E}) \to \mathbf{Iso}(X)$ est nécessairement non-trivial. En effet, on a que la réflexion $s_{\mathscr{H}} \in \mathbf{Iso}_{|X}(\mathscr{E})$ est différente de l'identité, mais sa restriction à X est l'identité.

En particulier les exemples 3.8 et 3.18 montrent que pour une droite$\mathscr{D}$ dans un espace affine euclidien $\mathscr{E}$ de dimenson ≥ 2, $\mathbf{Iso}_{|\mathscr{D}}(\mathscr{E})$ est ben différent de $\mathbf{Iso}(\mathscr{D})$.

Remarque 3.14 (*Inclusion ou égalité ?).* Si X est un sous-espace **affine** alors, on peut montrer les égalités :

- $\mathbf{Iso}_{|X}(\mathscr{E}) = \{f \in \mathbf{Iso}(\mathscr{E}),\ \forall x \in X,\ f(x) \in X\}$,
- $\mathbf{Aff}_{|X}(\mathscr{E}) = \{f \in \mathbf{Aff}(\mathscr{E}),\ \forall x \in X,\ f(x) \in X\}$.

En particulier, il suffit d'exiger que l'on a une bijection telle que l'image de X est dans X pour être sur que $f(X) = X$ (c'est à dire que l'image de X est X tout entier).

Exercice 3.15. Démontrer cette propriété. (Indication : commencer par se ramener au cas linéaire en choisissant un point dans X. Puis utiliser le théorème du rang).

Mais en général ce n'est pas vrai. Par exemple si $X = [0, +\infty[\times\{0\}$ est le demi-axe des réels positifs dans $\mathbb{R}^2$. Alors la translation $t_{(1,0)}$ envoie bien X dans X, mais son image est $[1, +\infty[\times\{0\}$ qui n'est évidemment pas X. En particulier, son inverse, la translation $t_{(-1,0)}$, ne préserve pas X ! Ce qui montre que $\{f \in \mathbf{Iso}(\mathscr{E}),\ \forall x \in X,\ f(x) \in X\}$ n'est pas un sous-groupe en général sans hypothèses sur X.

Exercice 3.16. Chercher d'autres contre-exemples.

43. pour les variantes affines, il suffit encore une fois que l'espace soit affine

44. autrement dit, dans ce cas à, toute isométrie de l'espace métrique X s'étend en une application affine de $\mathscr{E}$ tout entier qui est forcément une isométrie, et ceci de manière unique

3.2. **Que se passe-t-il pour les groupes d'isométrie de deux objets géométriques qui se ressemblent ?** La réponse va être qu'**ils sont conjugués**, ce qui fait réapparaitre cette notion en géométrie, qu'on appelle parfois *principe de conjugaison.*

Voyons le dans un cas particulier. pour commencer, ce qui va nous permettre de détailler un exemple non-trivial de symétries de figure géométriques.

Lemme 3.17. *Soit $\mathscr{D}$ et $\mathscr{D}'$ deux droites affines d'un espace affine $\mathscr{E}$.*

- *Il existe un isomorphisme affine f tel que $f(\mathscr{D}) = \mathscr{D}'$. On peut même choisir f de sorte que ce soit une isométrie.*
- *On a $\mathbf{Iso}(\mathscr{D}') = f_{|X} \circ \mathbf{Iso}(\mathscr{D}) \circ f_{|X}^{-1}$. Autrement dit le groupe des isométries de $\mathscr{D}'$ est conjugué (par f) aux isométries de $\mathscr{D}$. De même*
  - $\mathbf{Aff}(\mathscr{D}') = f_{|X} \circ \mathbf{Aff}(\mathscr{D}) \circ f_{|X}^{-1}$
  - $\mathbf{Iso}_{|\mathscr{D}'}(\mathscr{E}) = f \circ \mathbf{Iso}_{|\mathscr{D}}(\mathscr{E}) \circ f^{-1}$
  - $\mathbf{Aff}_{|\mathscr{D}'}(\mathscr{E}) = f \circ \mathbf{Aff}_{|\mathscr{D}}(\mathscr{E}) \circ f^{-1}$

  autrement ces groupes sont isomorphes via une conjugaison par f.

Dans le lemme ci-dessus, on note bien-sûr $f_{|X}$ la restriction de f $\mathscr{D}$.

Démonstration. Notons D, D' les directions des droites (c'est à dire leur droite vectorielle sous-jacente) et x_0, x_0' des points de $\mathscr{D}$ et $\mathscr{D}'$ respectivement.

L'idée est qu'il existe un isomorphisme linéaire de E qui envoie D sur D' car ce sont deux droites vectorielles : il suffit pour ça de prendre deux bases commençant l'une par un vecteur directeur u de D et l'autre par un vecteur directeur u' de D'. Alors l'isomorphisme linéaire envoyant la première base sur la deuxième convient. Si en plus on choisit les vecteurs des bases unitaires, cet isomorphisme est orthogonal. Notons $\vec{f} \in GL(E)$ cet isomorphisme et $\vec{f}_{x_0} \in GL_{x_0}(\mathscr{E})$ l'isomorphisme affine associé qui laisse x_0 fixe. On a alors que $\vec{f}_{x_0}(\mathscr{D}) = x_0 * (\mathbb{R}u')$ est une droite passant par x_0 et parallèle à $\mathscr{D}'$ (elles sont de même direction. Soit alors $f = t_{\overrightarrow{x_0x_0'}} \circ \vec{f}_{x_0}$: c'est une isométrie affine (si on a choisit u, u' unitaire ci-dessus, sinon juste un isomorphisme affine) et on a que $f(\mathscr{D}) = \mathscr{D}'$. En effet elle envoie $\mathscr{D}$ sur l'unique droite passant par x_0' et de direction D'.

Passons au deuxième point : Montrons tout d'abord que $\mathbf{Iso}(\mathscr{D}') \supset f_{|X} \circ \mathbf{Iso}(\mathscr{D}) \circ f_{|X}^{-1}$. Comme f est une isométrie affine, f^{-1} aussi et donc leurs restrictions à $\mathscr{D}$ et $\mathscr{D}'$ sotn aussi des isométries. Ainsi, pour tout $\varphi \in \mathbf{Iso}(\mathscr{D})$, on a que $f_{|X} \circ \varphi \circ f_{|X}^{-1}$ est une isométrie. De plus $f(\mathscr{D}) = \mathscr{D}'$ implique, en appliquant f^{-1} que $\mathscr{D} = f^{-1}(\mathscr{D}')$. Ainsi

$$f_{|X} \circ \varphi \circ f_{|X}^{-1}(\mathscr{D}') = f_{|X}(\varphi(\mathscr{D})) = f_{|X}(\mathscr{D}) = \mathscr{D}'$$

et donc $f_{|X} \circ \varphi \circ f_{|X}^{-1} \in \mathbf{Iso}(\mathscr{D}')$. Ce qui montre l'inclusion voulue. L'autre inclusion se montre en inversant les rôles de $\mathscr{D}$ et $\mathscr{D}'$ et en conjuguant par $f_{|X}^{-1}$.

Le cas des trois autres groupes est similaire. □

En particulier, les groupes d'isométrie de toute droite affine sont isomorphes puisque la conjugaison est un isomorphisme de groupes.

Autrement dit on peut parler du groupe abstrait d'isométrie d'une droite dans $\mathscr{E}$, car à isomorphisme près, ils sont tous égaux.

On peut déterminer explicitement ce groupe.

Exemple 3.18. Soit une droite $\mathscr{D}$ dans $\mathscr{E}$ et choisissons x_0 quelconque dans $\mathscr{D}$. Nous avons vu $\mathbf{Iso}(\mathscr{D})$ dans l'exemple 3.4.

En appliquant les idées de cet exmeple, on trouve que le groupe $\mathbf{Iso}_{|\mathscr{D}}(\mathscr{E})$ des isométries de $\mathscr{E}$ préservant $\mathscr{D}$ est le sous-groupe de tous les isomorphismes affines qui s'écrivent comme la composée $t_{\vec{u}} \circ f$ où $t_{\vec{u}}$ est une translation de vecteur un élément quelconque de D (la

direction de $\mathscr{D}$) et $f \in O_{x_0}(\mathscr{E})$ est une isométrie linéaire en x_0 telle que D est une droite propre de f.

Le même résultat est vrai pour $\mathbf{Aff}(_{|\mathscr{D}}(\mathscr{E})$ en remplaçant isométrie par isomorphismes linéaires.

D'après les résultats d'algèbre linéaire, on peut choisir une base orthonormée $\mathscr{B} = (e_1, \dots, e_n)$ de E telle que $\mathbb{R}e_1 = D$. Dans cette base, les applications linéaires (resp. isomorphismes) s'identifient au matrice par blocs de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & A \end{pmatrix}$ où $\lambda \in \mathbb{R}$ et A est dans $M_{n-1}(\mathbb{R})$ (resp. $\lambda \neq 0$ et $A \in GL_n(\mathbb{R})$). Les isométries linéaires s'écrivent $\begin{pmatrix} \pm 1 & 0 \\ 0 & A \end{pmatrix}$ où $A \in O_{n-1}(\mathbb{R})$.

En combinant ce qu'on vient de dire on peut déduire :

Proposition 3.19. *Soit $\mathscr{E}$ un espace affine de dimension n. Soit $\mathscr{D}$ une droite quelconque.*

- *Le groupe $\mathbf{Aff}_{|\mathscr{D}}(\mathscr{E})$ des isomorphismes affines globaux qui préservent D est isomorphe au groupe $\mathbf{Tran}(\mathbb{R}) \times \mathbb{R}^* \times GL_{n-1}(\mathbb{R})$ muni de la loi de composition donnée par la formule*

$$(t_{u_1}, \lambda_1, A_1) \cdot (t_{u_2}, \lambda_2, A_2) \;=\; (t_{u_1 + \lambda u_2}, \lambda_1 \lambda_2, A_1 A_2) \tag{40}$$

- *Le groupe $\mathbf{Iso}_{|\mathscr{D}}(\mathscr{E})$ des isométries globales qui préservent D est isomorphe au groupe produit $\mathbf{Tran}(\mathbb{R}) \times \{1, -1\} \times O_{n-1}(\mathbb{R})$ muni de la loi de composition donnée par la formule* (40).
- *Le groupe $\mathbf{Aff}(\mathscr{D})$ est isomorphe au groupe $\mathbf{Tran}(\mathbb{R}) \times \mathbb{R}^*$ muni de la loi de composition donnée par la formule*

$$(t_{u_1}, \lambda_1,) \cdot (t_{u_2}, \lambda_2) \;=\; (t_{u_1 + \lambda u_2}, \lambda_1 \lambda_2) \tag{41}$$

- *Le groupe $\mathbf{Iso}_{|\mathscr{D}}(\mathscr{E})$ des isométries globales qui préservent D est isomorphe au groupe $\mathbf{Tran}(\mathbb{R}) \times \{1, -1\}$ muni de la loi de composition donnée par la formule* (41).

Démonstration. Sera vue en TD. □

Le même principe marche avec les carrés, cubes, disques de même rayon etc... Nous verrons des exemples en TD. Énonçons un résultat général de conjugaison une bonne fois pour toutes.

Proposition 3.20 (Principe de conjugaison)**.** *Soit X, Y deux sous-ensembles de $\mathscr{E}$.*

- *Si $f : \mathscr{E} \to \mathscr{E}$ est une isométrie telle que $f(X) = Y$, alors $\mathbf{Iso}(X)$ et $\mathbf{Iso}(Y)$ sont conjugués dans $\mathbf{Iso}(\mathscr{E})$ et on a plus précisément*

$$\mathbf{Iso}(Y) = f \circ \mathbf{Iso}(X) \circ f^{-1}.$$

  En particulier ces deux groupes sont isomorphes. De même pour $\mathbf{Iso}_{|cX}(\mathscr{E})$ et $\mathbf{Iso}_{|Y}(\mathscr{E})$.
- *Si $f : \mathscr{E} \to \mathscr{E}$ est un isomorphisme affine tel que $f(X) = Y$, alors $\mathbf{Aff}(X)$ et $\mathbf{Aff}(Y)$ sont conjugués dans $\mathbf{Aff}(\mathscr{E})$ et on a plus précisément*

$$\mathbf{Aff}(Y) = f \circ \mathbf{Aff}(X) \circ f^{-1}.$$

  En particulier ces deux groupes sont isomorphes. De même pour $\mathbf{Aff}_{|cX}(\mathscr{E})$ et $\mathbf{Aff}_{|Y}(\mathscr{E})$.

Démonstration. On raisonne par double inclusion pour vérifier que $\mathbf{Iso}(Y) = f_{|X} \circ \mathbf{Iso}(X) \circ f_{|X}^{-1}$. La preuve est exactement la même que dans le cas des droites ci-dessus. En effet, une composition d'isométrie est une isométrie. Il suffit donc de vérifier que si $\psi \in \mathbf{Iso}(X)$, alors $f_{|X} \circ \Psi \circ f_{|X}^{-1}(Y) = Y$ pour avoir que $f_{|X} \circ \Psi \circ f_{|X}^{-1} \in \mathbf{Iso}(Y)$. Or

$$f_{|X} \circ \Psi \circ f_{|X}^{-1}(Y) = f_{|X}(\Psi(f^{-1}(Y))) = f_{|X}(\Psi(X)) = f_{|X}(X) = Y$$

en utilisant que $f(X) = Y \Leftrightarrow x = f^{-1}(Y)$ puisque f est bijective. Ensuite, nous avons, par le même argument que $f_{|X}^{-1} \circ \mathbf{Iso}(Y) \circ f_{|X} \subset \mathbf{Iso}(X)$. En conjuguant par $f_{|X}$, cela nous donne

$$f_{|X} \circ f_{|X}^{-1} \circ \mathbf{Iso}(Y) \circ f_{|X} \circ f_{|X}^{-1} \subset f_{|X} \circ \mathbf{Iso}(X) \circ f_{|X}^{-1}$$

et comme $f_{|X}$ et $f_{|X}^{-1}$ sont inverses l'une de l'autre on retrouve bien $\mathbf{Iso}(Y) \subset f_{|X} \circ \mathbf{Iso}(X) \circ f_{|X}^{-1}$.

Les autres cas sont évidemment les mêmes. □