Groupes et Symétries

L2 USPN

CHAPITRE 1

Structure des groupes et Groupes Symétriques

1. Introduction et motivations

La notion de groupe a déjà été introduite dans les cours de L1 (Algèbre 1 par exemple) et le cours d'arithmétique de L2.

Cette notion de groupe, 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 restes 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 bijections 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 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 transformations 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 groupe est donc très importante en mathématiques 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'aspects 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 une opération 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).

Explicitons quelques conséquences immédiates des définitions.

PROPOSITION 2.3.
(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.*
(2) Un élément g dans un groupe $(G, *)$ admet un *unique* inverse.
(3) L'inverse de g^{-1} est g.
(4) Un groupe $(G, *)$ est non vide.
(5) Pour tous $g, h \in G$, on a $(g * h)^{-1} = h^{-1} * g^{-1}$.

PREUVE. (1) 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) 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 ensemble E qui admet un élément neutre, alors tout élément admet au plus un inverse.

(3) Cela se voit immédiatement de la définition.

[1] nous utiliserons les deux terminologies pour vous habituer

(4) Il contient forcément un élément neutre par définition.

(5) 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 $(\mathbb{Z},\times)$ munis 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).

CONVENTION 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 commettront occasionnellement aussi pour vous y habituer et parce qu'ils sont bien pratiques.

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
$$(h*g = h'*g) \iff (h=h').$$

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

- *De plus, $\forall g, h, h' \in G$, on a les équivalences*

$$(g * h = h' \iff h = g^{-1} * h'), \qquad (h * g = h' \iff h = h' * g^{-1}),$$
$$g = h \iff e = g^{-1} * h \iff g * h^{-1} = e$$

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

PREUVE. 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 $f \circ \mathrm{id}_E = f$ et $\mathrm{id}_E \circ f = f$. C'est équivalent à vérifier que pour tout $x \in E$, on a $f \circ \mathrm{id}_E(x) = f(x)$ et $id_E \circ f(x) = f(x)$. Or par définition de la composée, on a

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

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 $g \circ g^{-1} = \mathrm{id}_E = g^{-1} \circ g$ 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 $f \circ g = \mathrm{id}_E$ et $g \circ f = \mathrm{id}_E$. 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 $g \circ f = \mathrm{id}_E$ 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 $\mathrm{Bij}(E)$) et que l'application réciproque d'une bijection est une bijection). Ce dernier point est du cours de L1, ce qui prouve que 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[3]. 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.

PREUVE. 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. □

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[4] 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[5].

PREUVE. 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.

[3] qui est aussi plus en phase avec la théorie des catégories

[4] un ensemble muni d'une loi de composition interne associative admettant un élément neutre

[5] 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

- Quels 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 $\mathbb{K}$, l'application $\det : GL_n(\mathbb{K}) \to (\mathbb{K}^*, \times)$ est un morphisme de groupes.
- 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 $\mathcal{B} = \{e_1, \ldots, e_n\}$ 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 $\varphi_{\mathcal{B}} : GL(E) \mapsto GL_n(\mathbb{R})$ qui à une application linéaire associe sa matrice dans la base $\mathcal{B}$ 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 complètement analogue au cas des applications linéaires.

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

Preuve. 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 seul 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 $\mathbb{R}$-espaces 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[6], 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 cardinal. 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[7].

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 raisonnements 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

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

[7]Démontrez-le; c'est assez similaire à la preuve du lemme 2.16

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 fixée au début).

EXERCICE 2.29. Démontrer le lemme.

Voici quelques exemples élémentaires à toujours garder en tête:

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.*

PREUVE. Cette preuve est faite 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.*

PREUVE. 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 montrer 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 utilisant 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 (les éléments 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 ; celle par inverse se prouve de façon 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.*

PREUVE. La preuve a été vue en cours d'arithmétique au semestre précédent. □

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. 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, les éléments du groupe 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 parfois ${}^g x$ 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 variant 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*

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

PREUVE. 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.*

PREUVE. *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 équivalents 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 $\tau \circ \tau = \mathrm{id}_X$.*

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.

PREUVE. 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 laissent 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 de G, on appellera *points fixes* de H les éléments de $\mathrm{Fix}(H) = \{x \in X, \forall h \in H, {}^h x = x\} = \bigcap_{h \in H} \mathrm{Fix}(h)$. On le 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 $\mathrm{Stab}_Y = \{g \in G, \forall y \in Y,\, g \cdot y = y\} = \bigcap_{y \in Y} \mathrm{Stab}_y$. 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.*

PREUVE. 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. On l'appelle l'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 (justifiez-le !). 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 $\{E_1, \ldots, E_n\}$, $\mathrm{Stab}_{\{E_1, \ldots, E_n\}} = \{I_n\}$. En revanche $C_{\{E_1, \ldots, E_n\}} = B$. 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*[8]: 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 3.69), alors $\mathrm{Stab}_x = G$ et $\mathrm{Stab}_G = Z(G)$ 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.

PREUVE. 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

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

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 $\mathrm{Stab}_x = \{e\}$. 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.

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 ${}_{G,X}\mathcal{R}$ sur X par $x\,{}_{G,X}\mathcal{R}y$ si il existe $g \in G$ tel que $y = g \cdot x$.

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

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

[8]notion que l'on va voir réapparaître souvent

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

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

PREUVE. 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 $x\mathcal{R}_{H,G}x$ et donc la relation est réflexive.

La symétrie va être une conséquence de la règle de simplification du lemme 3.11: Si $x\mathcal{R}_{H,G}y$, 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 $y\mathcal{R}_{H,G}x$.

La transitivité est une conséquence de la propriété (1) d'une action. Supposons que $x\mathcal{R}_{H,G}y$ et $y\mathcal{R}_{H,G}z$; 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 $x\mathcal{R}_{H,G}z$. □

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

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

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**[9] **de** X. La proposition suivante précise un peu plus la précédente.

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

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

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

On dispose d'une application (dite canonique) $X \to X_{/\mathcal{R}}$ 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 $G/\mathcal{R}_H$ 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 $x\mathcal{R}_H y$ si et seulement si $x^{-1}y \in H$ ce qui est aussi équivalent à $y^{-1}x \in H$.*

PREUVE. La définition de $x\mathcal{R}_H y$ 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. □

[9] autrement dit une décomposition de X en sous-ensembles non vides 2 à 2 disjoints, et qui recouvrent X

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***[10] *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 ?). En fait quand on écrit coensemble ou classe à gauche de g, cela fait référence au fait que g est à gauche.

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[11] $\{gH, g \in G\}$ 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.

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 plus tard (en L3 ou en DM) que le groupe H doit être normal pour que cela soit vrai (condition toujours satisfaite lorsque G est abélien).

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

REMARQUE 3.40. 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.

[10] coset en anglais, terminologie que beaucoup de francophones utilisent sans états d'âmes

[11] que l'on peut voir comme un sous-ensemble de $P(G)$ les parties de G

Démonstration du lemme 3.39. 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 3.41. La preuve montre même plus généralement, que quels que soient le cardinal de G et H, et $x \in G$, on a une bijection entre xH et H

Théorème 3.42 (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 3.43. 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

$$\begin{aligned} \mathrm{card}(G) = \sum_{\overline{x} \in G/H} \mathrm{card}(xH) &= \sum_{\overline{x} \in G/H} \mathrm{card}(H) \text{ (par le lemme 3.39)} \\ &= \mathrm{card}(G/H) \times \mathrm{card}(H) \end{aligned}$$

ce qui conclut. □

La première importante conséquence est la suivante.

Corollaire 3.44 (Lagrange). *Soit G est un groupe fini. Pour tout sous-groupe H de G,* $\mathrm{card}(H)$ *divise* $\mathrm{card}(G)$.

Preuve. 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 3.45. 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 3.46. 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 3.47. *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 note souvent $\langle S\rangle$ *le sous-groupe engendré par* S.

PREUVE. La preuve la plus rapide est la suivante. On regarde la famille $\mathcal{F}$ de tous les sous-groupes contenant S. Alors, par le lemme 2.31, on a que l'intersection $\bigcap_{H_i\in\mathcal{F}} H_i$ 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 $K \subset \bigcap_{H_i\in\mathcal{F}} H_i$ puisque ce dernier contient S mais aussi $\bigcap_{H_i\in\mathcal{F}} H_i \subset K$ puisque K contient S. Ainsi ces deux groupes sont égaux ce qui prouve l'unicité. □

REMARQUE 3.48 (À 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 3.52). 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 langage 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 3.49 (Ordre d'un élément). Soit $g \in G$ un groupe. On note $\langle g\rangle$ le sous-groupe engendré[12] 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 3.50. *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 $g = e$.*

[12] c'est-à-dire $\langle\{g\}\rangle$ dans les notations du lemme 3.47

PREUVE. 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 $\text{card}(\langle g\rangle) = 1$, 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 3.51. Regardons quelques exemples.

- Soit $n \neq 0 \in \mathbb{Z}$, alors $\text{ord}(n) = \infty$. En effet, $n\mathbb{Z} = \langle n\rangle$ est de cardinal infini.
- 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 $\text{ord}(\overline{2}^4) = 2$.
- 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 voit 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 $\text{ord}(\overline{2}^5) = 5$.

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 3.52. *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 $\text{ord}(g) = \infty$, pour tout $n \in \mathbb{Z} \setminus \{0\}$, on a $g^{*n} \neq e$.*
(3) *Si $n = \text{ord}(g)$, le sous-groupe $\langle g\rangle$ est* égal *au sous-groupe $\{e, g, g^{*2}, \cdots, g^{*(n-1)}\}$ de $(G, *)$.*

REMARQUE 3.53 (*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 3.49).

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 3.54 ci-dessous.

DÉMONSTRATION DE LA PROPOSITION 3.52. 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 laissé 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 $n = \text{ord}(g)$. 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 $\text{ord}(g) = \infty$. 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 3.54. *Soit $(G, *)$ un groupe et $g \in G$.*

1. *Pour tout $m \in \mathbb{Z}$, si $g^{*m} = e$, alors* $\text{ord}(g)$ *divise m (autrement dit m est un multiple de* $\text{ord}(g)$*).*
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 $\langle g \rangle = \{g^{*i},\ i = 0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ 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 $\mathbb{Z}$.*

PREUVE. On peut remarquer que l'on a déjà démontré (2) dans la preuve de la proposition 3.52. 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 $r_m \in \{0, \ldots, \text{ord}(g) - 1\}$. Or on a vu dans la proposition 3.52 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 3.52).

Il reste à voir que ces morphismes sont des isomorphismes. Dans le cas fini, par égalité des cardinaux, il suffit de vérifier que ce morphisme 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 $\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z}$,
soit isomorphe à $\mathbb{Z}$ *si* $\operatorname{ord}(g) = \infty$.

Remarque 3.55. 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 $\bar{i} \mapsto g^{*i}$ (la preuve du corollaire nous assurant que ce morphisme est bien défini).

Le corollaire suivant est aussi très utile.

Corollaire 3.56. *Si G est un groupe fini, alors, pour tout $g \in G$, on a $g^{\operatorname{card}(G)} = e$. En particulier* $\operatorname{ord}(g)$ *divise* $\operatorname{card}(G)$.

Preuve. 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 $\operatorname{card}(G)$ ce qui conclut pour le premier point. Le deuxième a été vu dans le corollaire précédent. □

Exemple 3.57. 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 3.58. 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 3.59. 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 3.60 (Un groupe cyclique est abélien, isomorphe à $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}$). Le corollaire 3.54 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 3.61.

- 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 $\bar{i}$ tel que $i \wedge n = 1$; par exemple $\bar{1}$.
- 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.
- Trivialement, 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 longueur 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 !)

EXEMPLE 3.62. 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 3.50).

EXEMPLE 3.63 (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 3.50). Donc tous 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 3.54). 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 3.64 (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 3.50).

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 3.54).

Sinon, tous les éléments $\neq e$ sont d'ordre 3. Soit $a \neq e$. On a $\langle a \rangle = \{e, a, a^2\}$. Soit $b \notin \{e, a, a^2\}$, 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 $(\overline{i}, \overline{j}) \mapsto a^i b^j$. 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 3.54. Ainsi $\overline{i} = \overline{j} = \overline{0}$ 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 3.65. Si $f : G \to H$ est un isomorphisme de groupes, alors pour tout $g \in G$, on a $\mathrm{ord}(f(g)) = \mathrm{ord}(g)$.

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 3.66. *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.

PREUVE. 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 3.67.
- 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 implique 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 $p : \begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \overline{k}^{nm} & \longmapsto & (\overline{k}^n, \overline{k}^m) \end{array}$: 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 3.68 (Il y a des produits *PAS* directs). 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[13] comme le groupe diédral.

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

DÉFINITION 3.69 (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 3.70. *Le centre d'un groupe G est un sous-groupe abélien de G.*

PREUVE. 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 simplifications successives. □

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

EXEMPLE 3.71.
- Évidement, $Z(G) = G$ si et seulement si G est abélien.
- Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Le centre $Z(GL(E))$ est égal à $\mathbb{K}\,\mathrm{id}$, c'est-à-dire les matrices d'homothéties (essayez d'en écrire une preuve, ce n'est pas du tout évident).

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 $(\mathrm{Bij}(X), \circ)$.

TERMINOLOGIE 4.2. Cette action est appelée *action canonique*.

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

PREUVE. 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 4.3. 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 $\mathrm{Bij}(X)$.

EXEMPLE 4.4. 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 l'application g.

EXERCICE 4.5. 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 4.6. *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.

PREUVE. Il faut d'abord vérifier que

$$\begin{array}{ccc} Ad_f : \mathrm{Bij}(X) & \longrightarrow & \mathrm{Bij}(Y) \\ \varphi & \longmapsto & f \circ \varphi \circ f^{-1} \end{array}$$

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

$$\begin{array}{rccc} Ad_{f^{-1}} : \mathrm{Bij}(Y) & \longrightarrow & \mathrm{Bij}(X) \\ \alpha & \longmapsto & f^{-1} \circ \alpha \circ f \end{array}$$

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 4.7 (**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.

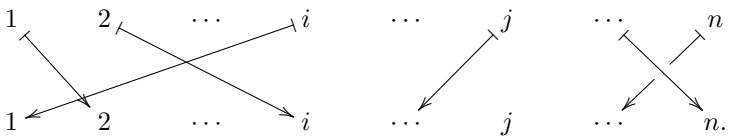
Tout d'abord ce groupe est le[14] groupe des bijections de tout ensemble à n éléments.

Corollaire 4.8. *Si X est un ensemble de cardinal n, alors $(\mathrm{Bij}(X), \circ)$ est un groupe isomorphe au groupe symétrique S_n.*

Preuve. Par définition du cardinal (voir le cours de L1 d'algèbre et structures), on a qu'il existe une bijection $f : X \to \{1, , \ldots, n\}$. La proposition 4.6 nous fournit un isomorphisme de groupes explicite entre $\mathrm{Bij}(X)$ et $S_n = \mathrm{Bij}(\{1, \ldots, n\}$. □

Terminologie 4.9. On appelle un élément de S_n une *permutation*.

Pourquoi cette terminologie ? Tout simplement parce qu'une bijection de $\{1, \ldots, n\}$ est une façon de réordonner[15] 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.

[14]à isomorphisme de groupes près bien sûr

[15]Rappelons qu'une bijection de $\{1, \ldots, n\}$ 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...

NOTATION 4.10. 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 $\sigma(i)$. Attention, il ne faut pas y penser comme des matrices d'algèbre linéaire.

LEMME 4.11. *On a* $\operatorname{card}(S_n) = n! = \prod_{i=1}^{n} i = n \cdot (n-1) \cdots 2 \cdot 1$.

PREUVE. 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 4.12. Puisque S_n est fini, par le Théorème de Lagrange, tout élément de S_n est d'ordre fini.

EXEMPLE 4.13 (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 4.14 (Le groupe S_2). En utilisant la notation 4.10, 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 4.15 (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. 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:

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

Cet algorithme marche évidemment pour tout entier n !

REMARQUE 4.16 (**Inverse**). Avec l'écriture de la notation 4.10, 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 4.10 ce qui justifie l'algorithme ci-dessus.

EXEMPLE 4.17. 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:

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

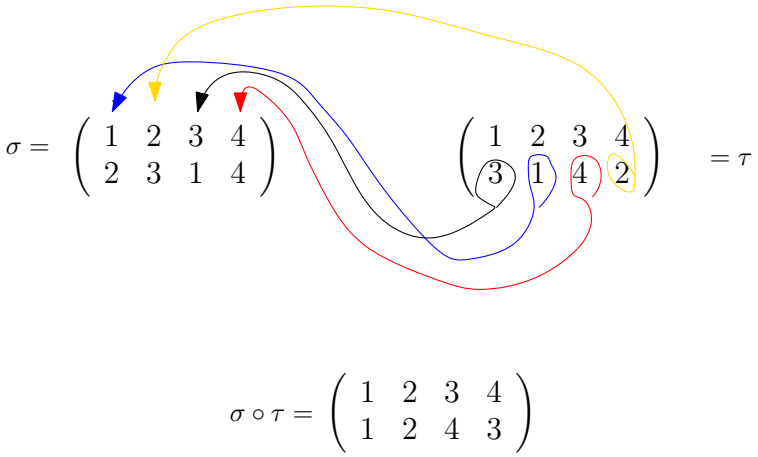


FIGURE 1. Composition de deux permutations

REMARQUE 4.18 (**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 4.10, 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 4.19. 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 4.20 (S_n est un sous-groupe de S_{n+1} canoniquement). Il est souvent pratique d'identifier à 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 4.21 (**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 4.22. On a $\mathrm{Supp}(\sigma) = \emptyset \iff \sigma = \mathrm{id}$.

EXEMPLE 4.23. 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 4.24. 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 point fixe. Précisément, on a l'*important lemme suivant.*

LEMME 4.25. *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 $\mathrm{Supp}(\sigma \circ \tau) \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$.*

PREUVE. 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, on a 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 troisième point, soit $i \in \mathrm{Supp}(\sigma \circ \tau)$. Alors $\sigma \circ \tau(i) \neq i$. On en déduit que, ou bien $\tau(i) \neq i$ ou bien $\tau(i) = i$ et $\sigma(i) \neq i$. En d'autres termes, ou bien $i \in \mathrm{Supp}(\tau)$, ou bien $i \in \mathrm{Supp}(\sigma)$. De manière équivalente $i \in \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$.

□

En général, le troisième point n'est pas une égalité (par exemple si on prend $\tau = \sigma^{-1}$). On a cependant le Lemme suivant.

LEMME 4.26. *Si σ et τ sont à support* disjoints[16]*, alors* $\mathrm{Supp}(\sigma \circ \tau) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$.

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

PREUVE. Une inclusion découle du Lemme précédent. Inversement, 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 $i \in \mathrm{Supp}(\tau)$.

[16] c'est à dire $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$

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 4.25, 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 $\sigma \circ \tau = \tau \circ \sigma$. De plus, pour tout $n \in \mathbb{N}$, on a*

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

PREUVE. 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 $i \notin \mathrm{Supp}(\tau)$;
(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 4.25.(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 être 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

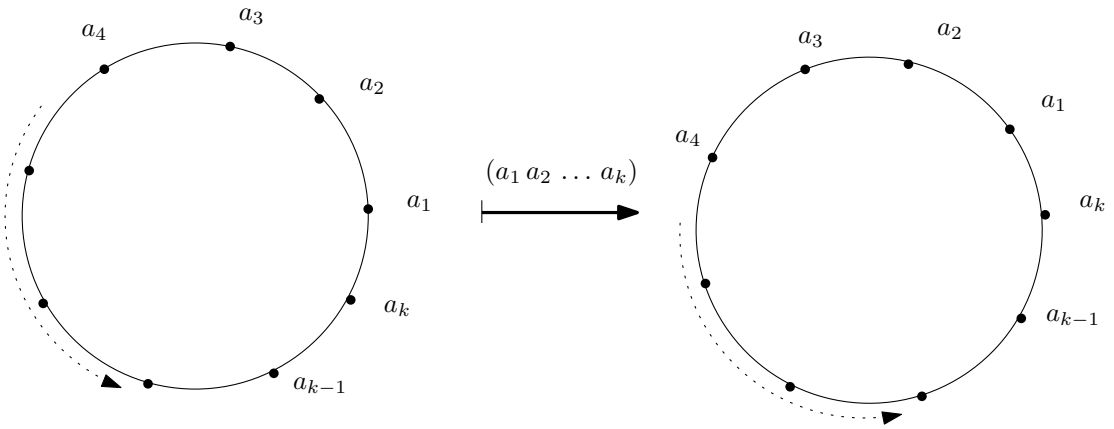
- $\sigma(i) = i$ si $i \notin \{a_1, \ldots, a_k\}$;
- $\sigma(a_j) = a_{j+1}$ si $1 \leq j \leq k-1$;
- $\sigma(a_k) = a_1$.

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 $i \in \{1, \ldots, n\}$.

PROPOSITION 4.31. *Les propriétés suivantes découlent directement de la définition.*

- *Par définition,* $\mathrm{Supp}(a_1\, a_2\, \ldots\, a_k) = \{a_1, \ldots, a_k\}$.



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

- *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 de 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.

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 4.20.

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.

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

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

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

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

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

ce qui conclut. □

Notons qu'une preuve "graphique" découle facilement de l'étude de la figure du cycle avec ses flèches 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* $\mathrm{ord}(\sigma) = k$.

PREUVE. 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 3.52 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 puissances d'un élément non-fixe quelconque.

PREUVE. 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 supports *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 4.25, 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 4.25). 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 complètement 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 3.52, 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).
- $\mathrm{Supp}(\sigma) \setminus \mathrm{Supp}(\sigma_1)$ 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 4.25) 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 $\sigma = \tau_1 \circ \cdots \circ \tau_\ell$: le cycle $\tau_j = (y\,\sigma(y)\,\ldots\,\sigma^{d_y-1}(y))$ 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

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

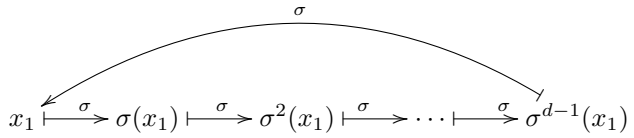
Par conséquent pour chaque élément du support on détermine exactement un des cycles de la famille des σ_i et un de la famille des τ_j qui sont égaux (et donc ont le même support et la même contribution au support de σ). En faisant ça pour tous les éléments du support de σ on établit exactement l'unicité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



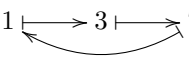
  On peut "barrer" les éléments utilisés dans σ pour éviter de les réutiliser.
- S'il n'y a plus d'éléments dans le support de σ qui ne soit pas dans celui de σ_1, on s'arrête là. Sinon, on prend un x_2 dans le support de σ qui n'est pas dans celui de x_1 et on refait l'opération ci-dessus pur avoir $\sigma_2 = (x_2\,\sigma(x_2)\,\cdots\,\sigma^{d_2-1}(x_2))$. 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

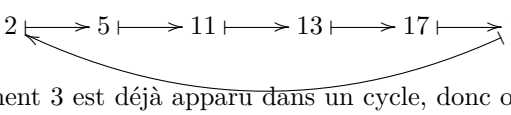
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 3 & 5 & 7 & 10 & 11 & 8 & 1 & 6 & 4 & 16 & 13 & 12 & 17 & 2 & 15 & 9 & 14 \end{pmatrix}.$$

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



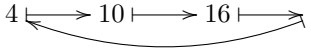
cela nous donne $\sigma_1 = (1\,3\,7)$.

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



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



cela donne $\sigma_3 = (4\,10\,16\,9)$.

L'élément 5 est déjà apparu avant donc on ne le regarde pas. On passe à $6 \overset{\curvearrowright}{\longmapsto} 8$ 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 $\tau \circ \sigma \circ \tau^{-1} = \circ \cdots \circ \left(\tau \circ \sigma_k \circ \tau^{-1}\right)$ où les $\left(\tau \circ \sigma_1 \circ \tau^{-1}\right)$ sont des cycles à supports disjoints de même ordre que σ_k.*

Preuve. 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 $(a_1 \ \dots \ a_k)$ un k-cycle de S_n. Alors on a l'égalité:*

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

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.

PREUVE. 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 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*

DÉFINITION 4.57. Ce nombre est appelé ***la signature de*** σ. Il sera noté $\mathrm{sgn}(\sigma)$ ou $(-1)^\sigma$.

Autrement dit $\mathrm{sgn}(\sigma) = (-1)^k$ 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 4.58. *La signature vérifie les propriétés suivantes:*

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

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

PREUVE. Tout d'abord, une transposition est le produit d'une transposition (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 $\mathrm{sgn}(\mathrm{id}) = (-1)^2 = 1$ (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

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

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 4.59. 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 4.60. 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 4.61. 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 4.62. 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 le cas de toutes les parties 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 4.63. 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 4.64. 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 4.65. *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

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

PREUVE. 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 4.61);
- 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 $I(\alpha) = \operatorname{card}(P_2^{\alpha,-})$ par définition. Et de plus $\operatorname{card}(B_\sigma^\tau)) = I(\sigma)$. 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

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

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

Et de plus

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

□

LEMME 4.66. *Si σ est une* transposition*, alors $I(\sigma)$ est impair.*

PREUVE. 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 4.65 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 4.66 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 4.67. 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 4.68 (**La signature est multiplicative. Servez vous en !**). On a vu dans le corollaire 4.58 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 4.58 pour faire le calcul.

Exemple 4.69. 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 4.58 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 $\mathbb{C}$. Ceux-là 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, ou 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. 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.

CHAPITRE 2

Groupes et géométrie

1. Le groupe orthogonal

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie.

DÉFINITION 1.1. Un produit scalaire sur E est une application $E \times E \to \mathbb{R}$ qui satisfait les propriétés suivantes.

(1) C'est une application symétrique. C'est-à-dire que pour tout x et y dans E on a
$$(x|y) = (y|x)$$
(2) C'est une application bilinéaire, c'est-à-dire que pour tout x, y, z dans E et tout λ et μ dans $\mathbb{R}$, on a
$$(x|\lambda y + \mu z) = \lambda(x|y) + \mu(x|z)$$
(3) Elle est positive. C'est-à-dire que pour tout x dans E on a
$$(x|x) \geq 0$$
(4) Elle est définie. C'est-à-dire que l'équation
$$(x|x) = 0$$
n'est satisfaite que par $x = 0$.

DÉFINITION 1.2. Soit E un $\mathbb{R}$-un espace vectoriel muni d'un produit scalaire, on note $||x||$ la norme du vecteur x donnée par la formule
$$||x|| := \sqrt{(x|x)}$$

EXEMPLE 1.3. On dispose par exemple du produit scalaire canonique sur $\mathbb{R}^n$ donné par la formule suivante
$$(x|y) = \sum_i x_i y_i$$
avec $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$. On utilisera souvent l'observation suivante. Si on voit x et y comme des vecteurs colonnes (c'est-à-dire des matrices à n lignes et 1 colonnes), on a alors
$$(x|y) = {}^t xy$$

DÉFINITION 1.4. Une base $(u_1, \ldots, u_n)$ de $\mathbb{R}^n$ est dite orthogonale si $(u_i|u_j)$ est nul dès que $i \neq j$. Elle est dite orthonormée si en plus $(u_i|u_i) = 1$ pour tout i.

PROPOSITION 1.5. *Soit $(e_1, \ldots, e_n)$ une famille de n vecteurs de $\mathbb{R}^n$ telles que*
$$(e_i|e_j) = \delta_{ij}.$$
Alors cette famille est une base (et donc une base orthonormée).

PREUVE. Il suffit de montrer que cette famille est libre. Supposons donc
$$\sum_{i=1}^{n} \lambda_i e_i = 0$$

En prenant le produit scalaire de cette équation avec e_k, on trouve

$$\sum_{i=1}^{n} \lambda_i (e_i|e_k) = 0$$

En utilisant notre hypothèse, le membre de gauche est égal à λ_k. On a donc $\lambda_k = 0$. Comme cette égalité est vraie pour tout k, on a bien montré que la famille est libre. □

DÉFINITION 1.6. Une application linéaire $f : \mathbb{R}^n \to \mathbb{R}^n$ est dite une isométrie linéaire si, pour tout x et y dans $\mathbb{R}^n$, on a

$$(f(x)|f(y)) = (x|y)$$

Le mot isométrie signifie "qui préserve les distances". Cette terminologie est justifiée par la proposition suivante.

PROPOSITION 1.7. *Une application linéaire $f : \mathbb{R}^n \to \mathbb{R}^n$ est une isométrie si et seulement si elle préserve la norme. C'est-à-dire si et seulement si, pour tout x dans $\mathbb{R}^n$, on a l'égalité*

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

PREUVE. En effet, si f est une isométrie, on a

$$||f(x)||^2 = (f(x)|f(x)) = (x|x) = ||x||^2$$

Comme $||f(x)||$ et $||x||$ sont tous deux positifs, cela implique

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

. Réciproquement, supposons que f préserve la norme. On va commencer par observer l'identité suivante

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

qui se montre sans difficulté grâce à la bilinéarité du produit scalaire. On a donc

$$(f(x)|f(y)) = \frac{1}{2}\left(||f(x)+f(y)||^2 - ||f(x)||^2 - ||f(y)||^2\right)$$

Comme f est linéaire, on en déduit

$$(f(x)|f(y)) = \frac{1}{2}\left(||f(x+y)||^2 - ||f(x)||^2 - ||f(y)||^2\right)$$

Comme f préserve la norme, on en déduit

$$(f(x)|f(y)) = \frac{1}{2}\left(||x+y||^2 - ||x||^2 - ||y||^2\right) = (x|y)$$

□

On rappelle la notion de matrice orthogonale.

DÉFINITION 1.8. Une matrice A de $M_n(\mathbb{R})$ est dite orthogonale si ${}^tAA = I_n$.

DÉFINITION 1.9. On note $O_n(\mathbb{R})$ l'ensemble des matrices orthogonales de taille n.

PROPOSITION 1.10. *L'ensemble $O_n(\mathbb{R})$ muni de la multiplication matricielle est un groupe.*

PREUVE. On va montrer que c'est un sous-groupe de $GL_n(\mathbb{R})$. La matrice I_n est orthogonale. Si A est orthogonale, elle est inversible d'inverse ${}^tA$. On a par ailleurs

$${}^t({}^tA){}^tA = A{}^tA = {}^t({}^tAA) = {}^tI_n = I_n$$

de qui montre que $A^{-1} = {}^tA$ est bien orthogonale. Enfin si A et B sont orthogonale

$${}^t(AB)AB = {}^tB{}^tAAB = {}^tBI_nB = {}^tBB = I_n$$

ce qui montre que AB est orthogonale. □

PROPOSITION 1.11. *Soit A une matrice dans $M_n(\mathbb{R})$. Les propriétés suivantes sont équivalentes.*

(1) *A est orthogonale.*

(2) *Les colonnes de A forment une famille orthonormée de $\mathbb{R}^n$.*
(3) *Les lignes de A forment une famille orthonormée de $\mathbb{R}^n$.*
(4) *La matrice A est la matrice de changement de base de la base canonique à une base orthonormée de $\mathbb{R}^n$.*
(5) *La matrice A est la matrice de changement de base d'une base orthonormée de $\mathbb{R}^n$ vers une base orthonormée de $\mathbb{R}^n$.*

PREUVE. L'équivalence entre (2) et (4) découle immédiatement de la définition d'une matrice de changement de base.

Clairement (4) implique (5). Supposons que $A = P_B^{B'}$ ou B et B' sont deux bases orthonormée de $\mathbb{R}^n$. Notons $M = P_C^B$ où C est la base canonique de $\mathbb{R}^n$. Alors M est orthogonale d'après l'équivalence de (2) et (4) ainsi que le produit $MA = P_C^{B'}$. Comme $A = M^{-1}MA$, elle est orthogonale d'après la Proposition 1.10.

Calculons l'entrée (i, j) de la matrice ${}^tAA$. Par définition du produit matriciel, on a

$$({}^tAA)_{ij} = \sum_{k=1}^{n} ({}^tA)_{ik} A_{kj} = \sum_{k=1}^{n} A_{ki} A_{kj} = (L_i | L_j)$$

où on a noté L_i et L_j la ième et jème ligne de A. On déduit facilement de cette formule que les conditions (1) et (3) sont équivalentes. D'un autre côté, on vérifie facilement que A est orthogonale si et seulement si ${}^tA$ est orthogonale. On en déduit que (1) et (2) sont également équivalentes. □

PROPOSITION 1.12. *Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une application linéaire. Les propriétés suivantes sont équivalentes*

(1) *L'application est une isométrie.*
(2) *La matrice de f dans la base canonique est une matrice orthogonale.*
(3) *La matrice de f dans toute base orthonormée est une matrice orthogonale.*

PREUVE. On va montrer (3) $\implies$ (2) $\implies$ (1) $\implies$ (3). L'implication (3) $\implies$ (2) est évidente.

Supposons que A la matrice de f dans la base canonique, est orthogonale. On va montrer que f est une isométrie. Soient X et Y deux vecteurs de $\mathbb{R}^n$ qu'on voit comme des vecteurs colonnes. Alors, on a $f(X) = AX$ et $f(Y) = A(Y)$. On a donc (en utilisant l'exemple 1.3)

$$(f(X)|f(Y)) = (AX|AY) = {}^t(AX)(AY) = {}^tX{}^tAAY = {}^tXY = (X|Y).$$

Enfin, si f est une isométrie, f envoie toute base orthonormée sur une famille satisfaisant l'hypothèse de la Proposition 1.5 et donc sur une base orthonormée grâce à cette proposition. Cela montre que (1) implique (3). □

Nous notons $\mathrm{Isom}(\mathbb{R}^n)$ l'ensemble des isométries de $\mathbb{R}^n$.

PROPOSITION 1.13. *Cet ensemble est un sous-groupe de* $\mathrm{Bij}(\mathbb{R}^n)$.

PREUVE. D'abord, observons que toute isométrie est bijective. On peut par exemple utiliser le fait que sa matrice est orthogonale et qu'une matrice orthogonale est inversible (son inverse est sa transposée par définition). On en déduit que $\mathrm{Isom}(\mathbb{R}^n)$ est bien un sous-ensemble de $\mathrm{Bij}(\mathbb{R}^n)$. Ensuite, on vérifie que $\mathrm{id}_{\mathbb{R}^n} \in \mathrm{Isom}(\mathbb{R}^n)$. En effet

$$(\mathrm{id}_{\mathbb{R}^n}(x)|\mathrm{id}_{\mathbb{R}^n}(y)) = (x|y)$$

Si f est une isométrie, alors f^{-1} également. En effet, comme f est une isométrie, on a

$$(f(a)|f(b)) = (a|b)$$

pour tous vecteurs a et b dans $\mathbb{R}^n$. En particulier, on peut appliquer cette égalité à $a = f^{-1}(x)$ et $b = f^{-1}(y)$ pour deux vecteurs quelconques de $\mathbb{R}^n$ x et y. On trouve

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

qui donne

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

Enfin, si f et g sont des isométries, on a, pour tous x et y

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

ce qui montre que $f \circ g$ est également une isométrie. □

PROPOSITION 1.14. *L'application*

$$\mathrm{Isom}(\mathbb{R}^n) \to O_n(\mathbb{R})$$

qui envoie une isométrie de $\mathbb{R}^n$ sur sa matrice dans la base canonique est un isomorphisme de groupes.

2. Le groupe spécial orthogonal

2.1. Définition.

PROPOSITION 2.1. *Le déterminant définit un morphisme de groupe*

$$det : O_n(\mathbb{R}) \to \{\pm 1\}$$

PREUVE. Observons déjà que la formule ${}^tAA = I_n$ implique

$$det(A)^2 = 1$$

On en déduit que le déterminant d'une matrice orthogonale est 1 ou -1. Le fait que $det(AB) = det(A)det(B)$ est une formule classique apprise dans le cours d'algèbre. linéaire. □

DÉFINITION 2.2. On note $SO_n(\mathbb{R})$ le noyau de det. C'est-à-dire

$$SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}), det(A) = 1\}.$$

C'est un sous-groupe de $O_n(\mathbb{R})$ par le Lemme 2.32.

DÉFINITION 2.3. Une isométrie est dite directe si sa matrice est dans $SO_n(\mathbb{R})$.

2.2. Orientation.

DÉFINITION 2.4. Soient $e_1, \ldots, e_n$ une base de $\mathbb{R}^n$ vus comme des vecteurs colonnes. On dit que cette base est orientée positivement si le déterminant de la matrice dont les colonnes sont les vecteurs $e_1, \ldots, e_n$ est strictement positif. Dans le cas contraire, on dit que cette base est orientée négativement.

On a une caractérisation géométrique de l'orientation positive dans $\mathbb{R}^2$ et $\mathbb{R}^3$.

PROPOSITION 2.5. *Une base e_1, e_2 de $\mathbb{R}^2$ est orientée positivement si l'angle orienté entre e_1 et e_2 est dans l'intervalle $]0, \pi[$. Elle est orientée négativement si l'angle est dans l'intervalle $]\pi, 2\pi[$.*

PREUVE. Soit u le vecteur $(1, 0)$. Notons α_1 l'angle orienté entre u et e_1 et α_2 l'angle orienté entre u et e_2. L'angle orienté entre e_1 et e_2 est donc $\alpha_2 - \alpha_1$. Multiplier e_1 et e_2 par un réel strictement positif ne modifie ni leur angle orienté ni le signe du déterminant. On peut donc supposer sans perte de généralité que e_1 et e_2 sont de norme 1. On a donc

$$e_1 = \begin{pmatrix} \cos(\alpha_1) \\ \sin(\alpha_1) \end{pmatrix} e_2 = \begin{pmatrix} \cos(\alpha_2) \\ \sin(\alpha_2) \end{pmatrix}$$

Le déterminant considéré est donc donné par

$$\det \begin{pmatrix} \cos(\alpha_1) & \cos(\alpha_2) \\ \sin(\alpha_1) & \sin(\alpha_2) \end{pmatrix} = \cos(\alpha_1)\sin(\alpha_2) - \cos(\alpha_2)\sin(\alpha_1) = \sin(\alpha_2 - \alpha_1)$$

La dernière égalité venant de la formule d'addition des sinus. Pour conclure, on peut utiliser qu'un angle orienté est dans l'intervalle $]0, \pi[$, si et seulement si son sinus est strictement positif. □

Pour des vecteurs de $\mathbb{R}^3$, on rappelle la notion de produit vectoriel.

DÉFINITION 2.6. Soient deux vecteurs de $\mathbb{R}^3$

$$u = \begin{pmatrix} a \\ b \\ c \end{pmatrix} v = \begin{pmatrix} d \\ e \\ f \end{pmatrix}$$

Leur produit vectoriel est le vecteur $u \wedge v$ de coordonnées

$$u \wedge v = \begin{pmatrix} bf - ec \\ -af + dc \\ ae - db \end{pmatrix}$$

REMARQUE 2.7. Il y a une interprétation très intuitive souvent utilisée en physique du produit vectoriel. En premier lieu, on observe que $u \wedge v$ est orthogonal à u et à v. Si u et v forment une famille libre, le vecteur $u \wedge v$ est de plus non-nul. Pour trouver la direction dans laquelle il pointe, on peut utiliser la règle de main droite. Si on aligne son pouce de la main droite avec u et son index (de la même main !) avec v, alors le majeur pointera dans la direction de $u \wedge v$.

PROPOSITION 2.8. *Soient*

$$u = \begin{pmatrix} a \\ b \\ c \end{pmatrix} v = \begin{pmatrix} d \\ e \\ f \end{pmatrix} w = \begin{pmatrix} g \\ h \\ i \end{pmatrix}$$

trois vecteurs de $\mathbb{R}^3$ formant une base. Alors ils sont orientés positivement si et seulement si on a

$$(w|u \wedge v) > 0$$

PREUVE. En effet, on a

$$(w|u \wedge v) = gbf - gec - haf + hdc + iae - idb$$

qui est exactement le déterminant de la matrice

$$\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$$

comme on peut le voir en développant par rapport à la dernière colonne. □

REMARQUE 2.9. Géométriquement, si w et x sont non-nuls, la condition $(w|x) = 0$ traduit le fait que w est dans le plan orthogonal à x. La condition $(w|x) > 0$ s'interprète en disant que w est dans le demi-espace délimité par ce plan contenant le vecteur x. Au contraire $(w|x) < 0$ signifie que w est dans l'autre demi-espace. On peut donc interpréter la proposition précédente de la manière suivante. Pour savoir si une base (u, v, w) est orientée positivement on doit vérifier que w est dans le même demi-espace que $u \wedge v$ par rapport au plan déterminé par u et v,

2.3. Produit semi-direct.

DÉFINITION 2.10. Une action à gauche d'un groupe G sur un groupe H est la donnée d'une action à gauche du groupe G sur l'ensemble H écrite

$$(g, h) \mapsto g.h$$

telle que, pour tout g dans G et tous h, h' dans H, on ait

$$g.(hh') = (g.h)(g.h')$$

DÉFINITION 2.11. Une action à droite d'un groupe G sur un groupe H est la donnée d'une action à droite du groupe G sur l'ensemble H écrite

$$(h, g) \mapsto h.g$$

telle que, pour tout g dans G et tous h, h' dans H, on ait

$$(hh').g = (h.g)(h'.g)$$

PROPOSITION 2.12. *Soit une action à gauche d'un groupe G sur un groupe H. Aors, pour tout g dans G, on a*

$$g.e_H = e_H$$

et pour tous g dans G et H dans H, on a

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

PREUVE. Pour la première équation, on a, pour tout h dans H

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

ce qui montre que $g.e_H = e_H$.

Pour la seconde, on a

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

donc $g.(h^{-1})$ est bien l'inverse de $g.h$. □

DÉFINITION 2.13. Supposons donnée une action à gauche d'un groupe G sur un groupe H notée $(g,h) \mapsto g.h$. On construit sur le produit $H \times G$ une loi de composition interne notée $\star$ donnée par la formule

$$(h,g) \star (h',g') = (h(g.h'), gg')$$

PROPOSITION 2.14. *Cette loi de composition interne fait de $G \times H$ un groupe.*

PREUVE. Clairement (e_G, e_H) est l'élément neutre pour cette loi.

On a

$$(g,h) \star (g^{-1}, g^{-1}.(h^{-1})) = (e_G, h(g.(g^{-1}.h^{-1}))) = (e_G, hh^{-1}) = (e_G, e_H)$$

De même

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

ce qui montre que l'élément (g,h) admet $(g^{-1}, g^{-1}.(h^{-1}))$ comme inverse.

L'associativité est laissée en exercice. □

NOTATION 2.15. On note $G \ltimes H$ le produit $G \times H$ muni de cette loi de groupe. On l'appelle le produit semi-direct de G et H.

REMARQUE 2.16. Il faut noter que cette notation est amibigüe puisque la structure de groupe sur $G \ltimes H$ ne dépend pas que de la structure de groupe sur G et celle de H. Elle dépend également de l'action de G sur H.

De même, on a la proposition suivante pour une action à droite.

PROPOSITION 2.17. *Soit G un groupe agissant à droite sur H un groupe. Alors, on peut construire un groupe $H \rtimes G$ dont l'ensemble sous-jacent est $H \times G$ et dont la loi de groupe est*

$$(h,g) \star (h',g') = (,gg')$$

2.4. Le groupe orthogonal comme produit semi-direct. Soit A une matrice de $O_n(\mathbb{R})$ de déterminant -1 et satisfaisant $A^2 = I_n$. Un exemple d'une telle matrice est la matrice diagonale dont tous les coefficients diagonaux sont des 1 à part l'un d'entre eux qui est -1.

On définit une application

$$\mathbb{Z}/2\mathbb{Z} \times SO_n(\mathbb{R}) \to SO_n(\mathbb{R})$$

par la formule

$$\overline{k}.M := A^k M A^k$$

PROPOSITION 2.18. *Cette application définit une action à gauche de $\mathbb{Z}/2\mathbb{Z}$ sur $SO_n(\mathbb{R})$.*

PREUVE. Déjà on remarque que la condition $A^2 = I_n$ implique que A^k ne dépend que du reste de k modulo 2 et donc que l'application est bien définie. □

THÉORÈME 2.19. *L'application* $\rho : SO_n(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z} \to O_n(\mathbb{R})$ *donnée par*

$$\rho(M, \overline{k}) = MA^k$$

est une bijection.

PREUVE. Soit M un élément de $SO_n(\mathbb{R})$, alors $M = \rho(M, \overline{0})$. Si M est de déterminant -1, alors MA est de déterminant A et $M = \rho(MA, \overline{1})$. Cela montre la surjectivité de ρ. Pour l'injectivité, supposons que

$$\rho(M, \overline{k}) = \rho(N, \overline{\ell})$$

c'est-à-dire

$$MA^k = NA^\ell$$

en passant au déterminant, on trouve $(-1)^k = (-1)^\ell$ qui implique $\overline{k} = \overline{\ell}$. On a donc

$$MA^k = NA^\ell = NA^k$$

et donc par simplification $M = N$. □

On constate que cette bijection n'est pas un isomorphisme de groupe si on équipe $\mathbb{Z}/2 \times SO_n(\mathbb{R})$ de la structure de groupe produit. En fait, on a

PROPOSITION 2.20. *Soit* $\star$ *la loi de composition sur* $SO_n(\mathbb{R}) \times \mathbb{Z}/2$ *donnée par*

$$(M, \overline{k}) \star (N, \overline{\ell}) = (MA^k NA^k, \overline{k} + \overline{\ell})$$

Alors, la loi $\star$ *fait de* $SO_n(\mathbb{R}) \times \mathbb{Z}/2$*, de plus*

$$\rho : (SO_n(\mathbb{R}) \times \mathbb{Z}/2, \star) \to O_n(\mathbb{R})$$

est un isomorphisme de groupe.

3. Le groupe $O_2(\mathbb{R})$

3.1.

PROPOSITION 3.1. *Une matrice dans* $SO_2(\mathbb{R})$ *est de la forme*

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

pour un nombre réel α*.*

une matrice dans $O_2(\mathbb{R})$ *de déterminant* -1 *est de la forme*

$$\begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}$$

PREUVE. Soit

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

une matrice dans $O_2(\mathbb{R})$, alors on a $a^2 + c^2 = 1$ et $b^2 + d^2 = 1$. il existe donc des nombres réels α et β tels que la matrice soit égale à

$$\begin{pmatrix} \cos(\alpha) & \sin(\beta) \\ \sin(\alpha) & \cos(\beta) \end{pmatrix}$$

Maintenant la condition que les deux colonnes sont orthogonales nous donne

$$\cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\alpha) = 0$$

et la condition que le déterminant est ± 1 nous donne

$$\cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) = \pm 1.$$

Ces deux équations se traduisent, en utilisant les formules d'addition pour cosinus et sinus, par

$$\sin(\alpha + \beta) = 0$$

et

$$\cos(\alpha+\beta)=\pm 1.$$

Dans le cas où le déterminant est 1, on trouve donc $\alpha+\beta=0$ et dans le cas où le déterminant est 1, on trouve $\alpha+\beta=\pi$ (à chaque fois modulo 2π). Dans le premier cas, on a donc $\sin(\beta)=-\sin(\alpha)$ et $\cos(\beta)=\cos(\alpha)$ et dans le second cas, on a $\sin(\beta)=\sin(\alpha)$ et $\cos(\beta)=-\cos(\alpha)$. □

On peut donner une interprétation géométrique à chacune de ces matrices.

PROPOSITION 3.2. *La matrice*

$$\begin{pmatrix}\cos(\alpha) & -\sin(\alpha)\\ \sin(\alpha) & \cos(\alpha)\end{pmatrix}$$

est la matrice d'une rotation du plan de centre 0 *et d'angle* α*. La matrice*

$$\begin{pmatrix}\cos(\alpha) & \sin(\alpha)\\ \sin(\alpha) & -\cos(\alpha)\end{pmatrix}$$

est la matrice de la réflexion orthogonale par rapport à la droite engendrée par le vecteur $\begin{pmatrix}\cos(\alpha/2)\\ \sin(\alpha/2)\end{pmatrix}$.

PREUVE. S'en convaincre par un raisonnement géométrique. □

En particulier, on a

PROPOSITION 3.3. *Soit* $f:\mathbb{R}^2\to\mathbb{R}^2$ *une isométrie indirecte, alors il existe une base orthonormée directe de* $\mathbb{R}^2$ *telle que la matrice de* f *dans cette base est la matrice*

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

PREUVE. D'après la proposition précédente, il existe un nombre réel α tel que f soit la réflexion orthogonale par rapport à la droite engendrée par $\begin{pmatrix}\cos(\alpha/2)\\ \sin(\alpha/2)\end{pmatrix}$. Considérons la base x_1, x_2 donnée par

$$x_1=\begin{pmatrix}\cos(\alpha/2)\\ \sin(\alpha/2)\end{pmatrix}, x_2=\begin{pmatrix}\cos(\alpha/2+\pi/2)\\ \sin(\alpha/2+\pi/2)\end{pmatrix}=\begin{pmatrix}-\sin(\alpha/2)\\ \cos(\alpha/2)\end{pmatrix}.$$

Alors $f(x_1)=x_1$ et $f(x_2)=-x_2$. La matrice de f dans cette base est donc de la forme voulue. □

3.2. Utilistion des nombres complexes. On identifie le plan $\mathbb{R}^2$ avec $\mathbb{C}$.

PROPOSITION 3.4. *Une application* $\mathbb{C}\to\mathbb{C}$ *est une isométrie linéaire si et seulement si elle est de la forme*

$$f_a: z\mapsto az$$

ou

$$g_a: z\mapsto a\overline{z}$$

pour un nombre complexe a *de module* 1*. Par ailleurs dans le premier cas, l'application est une isométrie linéaire directe et dans le second une isométrie linéaire indirecte.*

PREUVE. Si λ et μ sont des réels

$$g_a(\lambda z+\mu z')=a\overline{(\lambda z+\mu z')}=a\lambda\overline{z}+a\mu\overline{z'}=\lambda g_a(z)+\mu g_a(z')$$

donc g_a est $\mathbb{R}$-linéaire (prendre garde au fait que g_a n'est pas $\mathbb{C}$-linéaire). De même f_a est $\mathbb{R}$-linéaire (et également $\mathbb{C}$-linéaire).

Vérifions maintenant que, sous l'hypothèse $|a|=1$, l'application g_a est une isométrie. L'identification $\mathbb{R}^2=\mathbb{C}$ identifie la norme de $\mathbb{R}^2$ avec le module des complexes. On doit donc montrer que g_a préserve le module. On le vérifie ainsi :

$$|g_a(z)|=|a\overline{z}|=\sqrt{(\overline{a\overline{z}})a\overline{z}}=\sqrt{\overline{a}a\overline{z}z}=|a||z|=|z|.$$

On montrerait de même que f_a préserve le module.

Réciproquement, si f est une isométrie linéaire $\mathbb{R}^2 \to \mathbb{R}^2$, on sait que sa matrice dans la base canonique est de l'une des deux formes de la Proposition 3.1. Supposons que la matrice de f dans la base canonique est

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

alors $f = f_{e^{i\alpha}}$. En effet, il suffit de vérifier que la matrice de $f_{e^{i\alpha}}$ dans la base canonique est la même ce qui est facile. De même si la matrice de f est

$$\begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}$$

alors $f = g_{e^{i\alpha}}$. □

4. Le groupe $O_3(\mathbb{R})$

PROPOSITION 4.1. *Toute matrice de $O_3(\mathbb{R})$ possède un vecteur propre pour la valeur propre 1 ou pour la valeur propre -1.*

PREUVE. On commence par observer que toute matrice réelle de taille impaire admet une valeur propre réelle. En effet son polynôme caractéristique est de degré impair et un tel polynôme a toujours au moins une racine réelle par le théorème des valeurs intermédiaires. Prenons maintenant $M \in O_3(\mathbb{R})$, alors M a une valeur propre réelle par ce qu'on vient de dire. Notons λ cette valeur propre. Il existe donc un vecteur colonne X dans $\mathbb{R}^3$ tel que $MX = \lambda X$. On a alors

$${}^tX {}^tMMX = ||MX||^2 = ||\lambda X||^2 = \lambda^2 ||X||^2$$

mais aussi, puisque ${}^tMM = I_3$, on a

$${}^tX {}^tMMX = ||X||^2.$$

De ces deux égalités, on déduit que $\lambda = \pm 1$. □

PROPOSITION 4.2. *Soit A une matrice de $O_3(\mathbb{R})$ alors, il existe une matrice orthogonale M et un reel α tels que $M^{-1}AM$ soit de l'une des 2 formes suivantes.*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Plutôt que de montrer directement cette proposition, on va montrer la proposition équivalente suivante.

PROPOSITION 4.3. *Soit f une isométrie linéaire de $\mathbb{R}^3$. Alors, il existe une base orthonormée de $\mathbb{R}^3$ telle que la matrice de f dans cette base soit de l'une des 2 formes suivantes.*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

PREUVE. L'équivalence entre les deux propositions résulte du cours d'algèbre linéaire auquel on adjoint la remarque qu'une matrice de changement de base entre bases orthonormées est orthogonale (Proposition 1.11).

D'après la Proposition précédente, on sait que f posséde un vecteur propre pour la valeur propre 1 ou -1. Notons x_1, un tel vecteur propre. Quitte à normaliser, on peut supposer que x_1 est de norme 1. Notons P le plan orthogonal à la droite engendrée par x_1. Le plan P est stable par f. En effet, si $p \in P$, on a

$$(f(p)|x_1) = \pm(f(p)|f(x_1)) = 0$$

donc $f(p) \in P$. Par ailleurs, si on équipe P de la restriction du produit scalaire de $\mathbb{R}^3$, on constate que $f_{|P}$ est une isométrie de P. Il existe donc une base orthonormée de P telle que la matrice de $f_{|P}$ dans cette base soit de l'une des deux formes de l'énoncé de la Proposition 3.1. En mettant ensemble le vecteur

x_1 et une telle base de P, on trouve une base orthonormée de $\mathbb{R}^3$ dans laquelle la matrice de f est de l'une des 4 formes suivantes.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Maintenant, on constate que, quitte à réordonner les vecteurs de la base, la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ peut se mettre sous la forme $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(0) & -\sin(0) \\ 0 & \sin(0) & \cos(0) \end{pmatrix}$. De même la matrice $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ peut se mettre sous la forme $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\pi) & -\sin(\pi) \\ 0 & \sin(\pi) & \cos(\pi) \end{pmatrix}$. On se ramène donc aux deux formes proposées. □

Une façon complètement équivalente mais plus géométrique d'exprimer cette proposition est la suivante.

PROPOSITION 4.4. *Soit f une isométrie linéaire de $\mathbb{R}^3$. Alors il existe une décomposition de $\mathbb{R}^3$ sous la forme $\mathbb{R}^3 = P \oplus D$ avec P un plan et D une droite orthogonale à ce plan telle que*

1. *Les espaces P et D sont stables par f.*
2. *L'application $f_{|P}$ est une rotation.*
3. *L'application $f_{|D}$ est $\pm\mathrm{id}$.*

5. Sous-groupes du groupe orthogonal

On rappelle que pour un ensemble E, on écrit $P(E)$ pour l'ensemble des parties de E, c'est-à-dire l'ensemble des sous-ensembles de E.

PROPOSITION 5.1. *On dispose d'une action à gauche de $O_n(\mathbb{R})$ sur $P(\mathbb{R}^n)$ donnée par*

$$O_n(\mathbb{R}) \times P(\mathbb{R}^n) \to P(\mathbb{R}^n)$$
$$(M, S) \mapsto M.S$$

où $M.S$ est donnée par la formule

$$M.S = \{MX, X \in S\}$$

PREUVE. □

PROPOSITION 5.2. *Soit S un ensemble d'éléments de $\mathbb{R}^n$, alors l'ensemble*

$$\{M \in O_n(\mathbb{R}), M.S = S\}$$

est un sous-groupe de $O_n(\mathbb{R})$.

PREUVE. En effet, il s'agit simplement du stabilisateur de S pour l'action décrite ci-dessus. Cette proposition est donc un cas particulier du Lemme 3.14 □

On notera maintenant ce groupe $\mathrm{Stab}(S)$.

PROPOSITION 5.3. *Si S est une famille génératrice finie de $\mathbb{R}^n$, alors $\mathrm{Stab}(S)$ est un groupe fini.*

PREUVE. Considérons l'application

$$f : \mathrm{Stab}(S) \to \mathrm{Bij}(S)$$

qui envoie $M \in \mathrm{Stab}(S)$ sur la bijection $s \mapsto Ms$ (c'est bien une bijection car son inverse est $s \mapsto M^{-1}s$). Il est facile de vérifier que cette application est un morphisme de groupe. Si S est fini $\mathrm{Bij}(S)$ est un groupe fini donc il suffit de montrer que f est injective. Pour cela, il suffit de montrer que son noyau est

réduit à l'élément neutre. Soit donc $M \in \mathrm{Stab}(S)$ tel que $f(M) = \mathrm{id}_S$. On a donc, pour tout $s \in S$, $Ms = s$. On est donc en train de dire que $Ms = I_n s$ pour tout s dans S. Comme S est une famille génératrice de $\mathbb{R}^n$, on a $Mx = I_n x$ pour tout x dans $\mathbb{R}^n$. Donc $M = I_n$. □

5.1. Le groupe dihédral. Considérons $R_n \subset \mathbb{C}$ l'ensemble des racines n-ième de l'unité. On note D_n et on appelle groupe dihédral le groupe $\mathrm{Stab}(R_n)$. D'après la Proposition 5.3, D_n est un sous-groupe fini de $O_2(\mathbb{R})$. Le but de cette sous-section est de décrire les éléments de ce groupe. Pour ce faire, il sera pratique d'utiliser le point de vue complexe de la sous-section 3.2. Notons $\zeta = e^{2i\pi/n}$. L'ensemble R_n est donc donné par

$$R_n = \{\zeta^k, 0 \leq k \leq n-1\}.$$

On note r l'application $r(z) = \zeta z$ et $s(z) = \overline{z}$. On vérifie facilement que r et s sont des éléments de D_n. Comme D_n est un groupe, toute composée de ces applications sont aussi des éléments de D_n.

En termes de matrices, ces deux éléments de $O_2(\mathbb{R})$ sont donnés par

$$Mat(s) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, Mat(r) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$

Proposition 5.4. *Le groupe D_n est donné, en tant qu'ensemble, par les éléments suivants distincts deux à deux*

$$D_n = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, r \circ s, \ldots, r^{n-1} \circ s\}$$

Par ailleurs, la structure de groupe est déterminée par les équations suivantes

$$s^2 = \mathrm{id},\ r^n = \mathrm{id},\ s \circ r = r^{n-1} \circ s.$$

Avant de prouver cette proposition explicitons ce que signifie la seconde phrase. Ce qu'on affirme c'est que ces trois équations paermettent de calculer tous les produits possibles dans D_n et de les identifier avec un des éléments de l'ensemble. Par exemple dans D_7, la composée $(r^5 \circ s) \circ r^2$ se calcule de la manière suivante

$$r^5 \circ s \circ r^2 = r^5 \circ s \circ r \circ r = r^5 \circ r^6 \circ s \circ r = r^5 \circ r^6 \circ r^6 \circ s = r^{17} \circ s = r^3 \circ s$$

de même le produit $(r^2 \circ s) \circ (r^3 \circ s)$ se calcule ainsi

$$r^2 \circ s \circ r \circ r \circ r \circ s = r^2 \circ r^6 \circ r^6 \circ r^6 \circ s \circ s = r^{16} \circ s^2 = r^2 \circ \mathrm{id} = r^2$$

Preuve. Notons temporairement U l'ensemble

$$U = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, r \circ s, \ldots, r^{n-1} \circ s\}$$

Clairement $U \subset D_n$ puisque r et s sont dans D_n et D_n est un groupe. Il est aussi facile de vérifier que les trois équations sont satisfaites. Montrons que $D_n \subset U$. Soit $f \in D_n$, alors par la sous-section 3.2, f est de la forme $f_a : z \mapsto az$ ou $g_a : z \mapsto a\overline{z}$ avec a un complexe de module 1. L'application f doit envoyer ζ sur une racine n-ième de l'unité, c'est-à-dire une puissance de ζ. La condition

$$f_a(\zeta) = \zeta^k$$

donne $a\zeta = \zeta^k$ donc $a = \zeta^{k-1}$. Mais l'application $f_{\zeta^{k-1}}$ coïncide avec r^{k-1} qui est elle-même égale à r^l où l est le reste de la division euclidienne de $k-1$ par n. La condition

$$g_a(\zeta) = \zeta^k$$

donne $a\zeta^{n-1} = \zeta^k$ donc $a = \zeta^{k-n+1}$ (en effet $\overline{\zeta} = \zeta^{n-1}$). Notons l le reste de la division euclidienne de $k-n+1$ par n. Alors $g_a = g_{\zeta^l}$ et on a

$$g_{\zeta^l}(z) = \zeta^l \overline{z} = r^l \circ s(z)$$

donc dans ce cas également on tombe sur un élément de U.

Finalement montrons que les $2n$ éléments de U sont distincts deux à deux. En évaluant sur 1, l'équation

$$r^i = r^j,$$

on trouve $\zeta^i = \zeta^j$ donc $n|(j-i)$ ce qui impose $i = j$ car i et j sont dans $\{0, \dots, n-1\}$. De même, en évaluant sur 1 l'équation

$$r^i \circ s = r^j \circ s,$$

on trouve $\zeta^i = \zeta^j$ et donc $i = j$.

Finalement, on ne peut jamais avoir d'égalité $r^i = r^j \circ s$ car le membre de gauche est une isométrie directe et le membre de droite une isométrie indirecte. □

On dispose du morphisme déterminant

$$\det : O_2(\mathbb{R}) \to \{\pm 1\}$$

qu'on peut précomposer avec l'inclusion $D_n \subset O_n(\mathbb{R})$ pour obtenir un morphisme de groupe

$$D_n \to \{\pm 1\}$$

Le noyau de ce morphisme est $SO_2(\mathbb{R}) \cap D_n$. On le note D_n^+, il s'agit du groupe des isométries directes préservant R_n. Grâce à la proposition précédente, on voit immédiatement que

$$D_n^+ = \{\mathrm{id}, r, \dots, r^{n-1}\} \subset D_n$$

PROPOSITION 5.5. *L'application $\mathbb{Z}/n\mathbb{Z} \to D_n^+$ qui envoie $\overline{k}$ sur r^k est un isomorphisme de groupe.*

PREUVE. Remarquons déjà que cette application est bien définie. Si $\overline{k} = \overline{l}$, alors $l - k$ est un multiple de n et donc $r^k = r^l$.

On vérifie aisément que cette application est un morphisme de groupe. Elle est surjective puisque □

5.2. Automorphismes du losange. On considère un autre exemple. On considère L l'ensemble des quatres nombres complexes suivants

$$L = \{2, -2, i, -i\}$$

On veut calculer le groupe $\mathrm{Stab}(L)$. C'est un sous-groupe fini de $O_2(\mathbb{R})$ d'après la Proposition 5.3.

Un élément f de $\mathrm{Stab}(L)$ est de la forme f_a ou g_a avec a un nombre complexe de module 1 (notation de la sous-section 3.2). Comme une isométrie préserve la norme (qui s'interprète comme le module dans les complexes), un élément de $\mathrm{Stab}(L)$ doit envoyer 2 sur ± 2 et i sur $\pm i$. On voit donc que les seules isométries satisfaisant cette condition sont

$$f_1, f_{-1}, g_1, g_{-1}$$

Le groupe $\mathrm{Stab}(L)$ a donc 4 éléments. Il reste à comprendre la structure de groupe sur cet ensemble. Pour cela, on a la proposition suivante

PROPOSITION 5.6. *L'application $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Stab}(L)$ donnée par*

$$(\overline{0}, \overline{0}) \mapsto f_1$$
$$(\overline{1}, \overline{0}) \mapsto f_{-1}$$
$$(\overline{0}, \overline{1}) \mapsto g_1$$
$$(\overline{1}, \overline{1}) \mapsto g_{-1}$$

est un isomorphisme de groupe.

PREUVE. Il suffit de vérifier toutes les compositions possibles ce qui est facile (mais un peu fastidieux). □