Groupes et Géométrie
Notes de cours

Vincent Pecastaing

22 juillet 2023

Résumé

Ces notes sont issues d'un cours-TD de préparation à l'agrégation. Elles ont été écrites pour servir d'appui aux révisions et donner une vue d'ensemble des sujets abordés, sans la prétention d'être exhaustives. Certains points sont développés en détail, notamment suite aux échanges avec les étudiants, d'autres sont simplement évoqués et on renvoie vers des références externes. Bien que le tout soit rédigé en suivant une forme de progression partant des définitions de base, l'idée reste que le lecteur a déjà rencontré la plupart des concepts et on s'autorise par endroit l'emploi de notions qui ne sont (ré)introduites que plus loin dans le texte.

Introduction

On va survoler dans ce cours quelques aspects de la théorie des groupes et les liens étroits qu'elle entretient avec la géométrie, en particulier via les actions de groupes. L'essentiel des résultats que nous allons considérer concerne les groupes finis et certains groupes linéaires.

Lorsque la notion a émergé au début du 19ème siècle, on voyait un groupe comme une famille de symétries d'un objet mathématique, stable par composition et passage à l'inverse. C'est le cas des groupes de Galois vus comme un sous-ensemble bien particulier de permutations des racines d'un polynôme, ou bien des groupes cristallographiques composés d'isométries de polyèdres.

Plus abstraite, l'approche moderne donne une définition intrinsèque des groupes, au sens où ils ne sont plus définis relativement à un autre objet mathématique (polynôme, polyèdre..). On ne retient du groupe que ses éléments et la façon dont ils se composent. C'est cela qui fait le groupe. On peut en particulier définir un groupe en explicitant cette loi de composition, via un tableau à deux entrées dans le cas fini, ou bien via la présentation générateurs/relations pour certains groupes de type fini par exemple.

Si ce point de vue axiomatique est celui retenu, il est très important de savoir revenir au premier, et donc de réaliser un groupe abstrait comme un groupe de symétries d'un objet mathématique donné, et en particulier de le voir agir sur cet ensemble. Sans cela, il serait bien difficile de comprendre sa structure.

Bien-sûr, à une structure de groupe donnée correspondent souvent beaucoup d'actions de natures distinctes, qui sont donc autant d'atouts pour l'analyser. Ainsi, le groupe $\mathrm{SL}_2(\mathbf{Z})$ des matrices 2×2 à coefficients entiers et de déterminant 1 apparaît d'abord comme un groupe linéaire, mais nous verrons qu'à un petit détail près il se réalise comme un groupe d'homographies du demi-plan supérieur $\mathbb{H}^2 = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. Cette deuxième caractérisation permet par exemple de voir de façon assez éclairante qu'il est engendré par deux matrices particulières S et T.

Nous nous intéresserons en particulier aux représentation linéaires des groupes finis, il s'agira de voir comment un groupe G donné peut se réaliser comme un groupe linéaire, c'est à dire un sous-groupe du groupe linéaire $\mathrm{GL}(V)$ d'un espace vectoriel complexe V de dimension finie.

Table des matières

1 Généralités sur les groupes

1.1 Groupes, Sous-groupes, Premiers exemples

Définition 1.1

Un groupe est la donnée d'un couple $(G, *)$, où G est un ensemble et $*$ une loi de composition interne sur G, c'est à dire une application $(g, h) \in G \times G \mapsto g * h \in G$, qui est

1. associative : $\forall g_1, g_2, g_3 \in G$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$
2. possède un élément neutre e, c'est à dire tel que $\forall g \in G, g * e = e * g = g$
3. telle que tout élément admet un inverse : $\forall g \in G$, $\exists h \in G : g * h = h * g = e$.

Il y a unicité du neutre : si e et e' sont deux neutres, alors par définition $e*e' = e = e'$. De même, il y a unicité de l'inverse d'un élément : si h_1, h_2 sont deux inverses d'un élément g, alors d'une part $h_2 * (g * h_1) = h_2$, et d'autre part $h_2 * (g * h_1) = (h_2 * g) * h_1 = h_1$ par associativité, d'où $h_1 = h_2$. On parle donc *du* neutre d'un groupe, et de *l'*inverse d'un élément. L'inverse de g sera noté g^{-1}.

Remarque 1.1. Sauf dans le cas abélien où on préférera noter additivement la loi, on prendra toujours comme notation gh pour la loi de G, ce qu'on sous-entend en disant que la loi est notée « multiplicativement ». On parlera alors par abus du *produit* de deux éléments de G, de même que les itérés sont appelés *puissances* et notés g^n. Le neutre du groupe sera noté e, ou parfois id.

Encore une fois, ceci est pour le cas général. Malheureusement, ces notations sont peu adaptées et perturbantes dans le cas abélien (prendre $\mathbf{Z}$ par exemple). Aussi, on préférera souvent une notation additive pour les groupes abéliens : la composition de deux éléments sera noté $x + y$, le neutre sera noté 0, l'inverse d'un élément x sera noté $-x$, et les itérés $n.x$, pour $n \in \mathbf{Z}$.

Remarque 1.2. Pour un groupe quelconque G, on a toujours $(gh)^{-1} = h^{-1}g^{-1}$.

Dorénavant, les groupes sont notés multiplicativement, sauf mention explicite du contraire. On leur réserve le plus souvent possible les lettres G et H, et les lettres g, h, k (parfois assorties d'indices) pour leurs éléments.

Définition 1.2

On dit d'un groupe G qu'il est *abélien (ou commutatif)* si pour tous $g, h \in G$, on a $gh = hg$. On définit le *centre* de G, noté $\mathcal{Z}(G)$, comme étant

$$\mathcal{Z}(G) = \{g \in G \mid \forall h \in G,\ gh = hg\}.$$

Ainsi, un groupe G est abélien si et seulement si $\mathcal{Z}(G) = G$.

Exercice 1.1

Soit G un groupe tel que pour tout $g \in G$, $g^2 = e$. Montrer que G est abélien.

Définition 1.3

L'*ordre* d'un groupe fini G est son cardinal, noté $|G|$.

Définition 1.4

Un *sous-groupe* de G est une partie non-vide $H \subset G$ stable par produit et passage à l'inverse, c'est à dire telle que pour tous $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.

La loi de G se restreint alors en une loi de groupe sur H qui sera, sauf mention explicite du contraire, celle qu'on considérera.

On note qu'en particulier $e \in H$ pour tout sous-groupe H de G puisque $H \neq \emptyset$ (il possède donc au moins un élément h et par définition $e = hh^{-1} \in H$).

Exercice 1.2
Montrer que les sous-groupes de $(\mathbf{Z}, +)$ sont les $n\mathbf{Z}$, où $n \in \mathbf{N}$.

Exercice 1.3
Montrer que les sous-groupes de $(\mathbf{R}, +)$ sont soit denses dans $\mathbf{R}$ (comme par exemple $\mathbf{Q}$ ou $\mathbf{Q}[\sqrt{2}]$), soit de la forme $a\mathbf{Z}$ avec $a > 0$.

Exercice 1.4
Montrer que $\mathbf{Z} + a\mathbf{Z}$ est un sous-groupe de $\mathbf{R}$ et qui est dense si et seulement si $a \notin \mathbf{Q}$.

Remarque 1.3. Pour démontrer qu'un ensemble avec une loi de composition est un groupe, il est souvent préférable de montrer qu'il s'agit d'un sous-groupe d'un groupe déjà connu, et non pas redémontrer que sa loi vérifie tous les axiomes.

Proposition 1.1
Soient G un groupe et $(H_i)_{i\in I}$ une famille quelconque de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Preuve. En exercice. □

Définition 1.5
Soient G un groupe et $A \subset G$ une partie. On appelle **sous-groupe engendré par** A, et on note $\langle A \rangle$, le plus petit sous-groupe de G qui contient A.

Preuve. Cette définition sous-entend que ce sous groupe existe et est unique. On peut le voir avec le point de vue *externe*, c'est à dire en considérant

$$H_0 := \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H.$$

D'après la proposition précédente, c'est un sous-groupe de G. Il contient A. Et si H_1 est un sous-groupe de G contenant A, alors

$$H_0 = H_1 \cap \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H \\ H \neq H_1}} H \subset H_1.$$

Ainsi, H_0 est contenu dans tout sous-groupe de G contenant A, c'est donc le plus petit.

On peut également définir $\langle A \rangle$ du point de vue interne. Nécessairement, $\langle A \rangle$ contient tous les éléments de A, leurs inverses, et tous les produits qu'on peut faire entre eux. Il est donc naturel de considérer

$$\{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n},\ n \geqslant 0,\ a_1, \dots a_n \in A,\ \varepsilon_k \in \{\pm 1\}\} \subset G$$

l'ensemble de tous les mots sur l'alphabet formés des éléments de A et leurs inverses. On vérifie que c'est un sous-groupe de G. Il s'agit donc nécessairement de $\langle A \rangle$. □

Dans le cas où $A = \{g\}$ est réduit à un singleton, on note simplement $\langle A \rangle = \langle g \rangle$. On a alors $\langle g \rangle = \{g^n, n \in \mathbf{Z}\}$, une caractérisation plus « parlante » que l'intersection de tous les sous-groupes de G contenant g. De même, pour une partie finie $A = \{g_1, \dots, g_k\}$, on notera simplement $\langle A \rangle = \langle g_1, \dots, g_k \rangle$.

Remarque 1.4. Dans le cas abélien, ou plus généralement si $g_1, \dots, g_k$ commutent deux à deux, le sous-groupe qu'ils engendre s'écrit plus simplement. On peut simplement regrouper les puissances entre-elles :

$$\langle g_1, \dots, g_k \rangle = \{g_1^{n_1} \dots g_k^{n_k},\ n_1, \dots, n_k \in \mathbf{Z}\}.$$

Lorsque G est abélien, la notation additive est très pertinent puisqu'elles se réfère à celle des $\mathbf{Z}$-modules. Ici, le sous-groupe engendré par un élément g sera noté $\langle g \rangle = \mathbf{Z}.g = \{k.g,\ k \in \mathbf{Z}\}$ et le sous-groupe engendré par un nombre fini d'éléments $g_1, \dots, g_k$ sera lui noté $\mathbf{Z}.g_1 + \dots + \mathbf{Z}.g_k$, puisque tout élément du groupe engendré s'écrit $n_1.g_1 + n_2.g_2 + \dots + n_k.g_k$

Définition 1.6

On dit qu'un groupe est **finiment engendré**, ou de **type fini**, s'il existe une partie finie $A \subset G$ telle que $G = \langle A \rangle$.

Bien-sûr, tout groupe fini est finiment engendré, puisque $G = \langle G \rangle$! Parmi les groupes infinis, $\mathbf{Z} = \langle 1 \rangle$ est finiment engendré, tout comme $\mathbf{Z}^k$ qui est par exemple engendré (en tant que groupe additif) par les k vecteurs de la base canonique de $\mathbf{R}^k$. Il existe d'autres groupes qui sont finiment engendrés et pour lesquels c'est moins évident, par exemple $\mathrm{SL}_n(\mathbf{Z})$. *A contrario* :

Exercice 1.5

Montrer que le groupe additif $(\mathbf{Q}, +)$ n'est pas finiment engendré.

Exercice 1.6

Montrer que tout groupe finiment engendré est au plus dénombrable.

Remarque 1.5. En algèbre linéaire, un espace vectoriel est de dimension finie s'il est finiment engendré, en tant qu'espace vectoriel. Un résultat fondamental de la théorie de la dimension est qu'un sous-espace d'un espace de dimension finie est également de dimension finie.

L'analogue de ce résultat est *faux* avec les groupes : un sous-groupe d'un groupe finiment engendré n'est pas nécessairement finiment engendré. Voir la feuille de TD 1 pour un contre-exemple.

Exemple 1.1. L'algorithme du pivot de Gauss permet de voir que $\mathrm{GL}_n(\mathbf{R})$ est engendré par les matrices élémentaires d'opérations sur les lignes et les colonnes, à savoir

- les matrices de transvection $T_{ij}(x) = I_n + xE_{ij}$, $i \neq j$,
- les matrices de dilations $D_i(\lambda) = \mathrm{diag}(1, \dots, \lambda, \dots, 1)$, λ en position i
- les matrices de transposition $\mathcal{T}_{ij} = (\delta_{k\tau(\ell)})$, où $\tau = (i\ j)$ est la transposition échangeant i et j.

Exercice 1.7

Montrer que $\mathrm{SL}_n(\mathbf{R})$ est engendré par les transvections.

Ces propriétés des groupes linéaires permettent d'établir des faits généraux tels que leur connexité par arc ou bien de déterminer leur groupe dérivé.

Définition 1.7

On dit d'un groupe G qu'il est **monogène** s'il existe $g_0 \in G$ tel que $G = \langle g_0 \rangle$. Il est dit **cyclique** s'il est monogène et fini.

Exemple 1.2. $(\mathbf{Z}, +)$ est monogène, $\mathbf{Z}/n\mathbf{Z}$ est cyclique. Par contre, $\mathbf{Z}^2$ n'est pas monogène, tout comme $(\mathbf{Z}/2\mathbf{Z})^2$ (tout élément y est d'ordre 2).

Définition 1.8

Soient G et H deux groupes. Un **morphisme** de G vers H est une application $f : G \to H$ telle que pour tous $g_1, g_2 \in G$, on a $f(g_1 g_2^{-1}) = f(g_1) f(g_2)^{-1}$. En particulier $f(e_G) = e_H$.

Si $f : G \to H$ est un morphisme, son **noyau** $\ker f = \{g \in G \ : \ f(g) = e_H\}$ et son image $\mathrm{Im}(f) = f(G) = \{f(g), \ g \in G\}$ sont des sous-groupes de G et H respectivement.

Un **isomorphisme** $f : G \to H$ est un morphisme de groupes bijectif. Deux groupes sont dits isomorphes s'il existe un isomorphisme entre eux.

Un isomorphisme $f : G \to G$ est appelé un **automorphisme de** G. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Remarque 1.6. Comme en algèbre linéaire, un morphisme $f : G \to H$ est injectif si et seulement si $\ker f = \{e_G\}$.

La notion d'isomorphisme de groupe est centrale. Comme expliqué en introduction, un groupe doit être pensé comme la donnée de ses éléments et de leur loi de composition. Une même structure de groupe peut donc apparaître dans des contextes différents et l'enjeu est de la *reconnaître*. La notion d'isomorphisme formalise cette idée : on considère deux groupes isomorphes comme étant *les mêmes* puisqu'on peut identifier leurs éléments de sorte que la loi se transporte.

Exemple 1.3. Soit $T \subset \mathbf{R}^2$ un triangle équilatéral pour la structure euclidienne standard. Le groupe $G = \{f \in \mathrm{Isom}(\mathbf{R}^2) \ : \ f(T) = T\}$ est le groupe formé des six éléments $\mathrm{id}, s_1, s_2, s_3, r, r^2$ où s_1, s_2, s_3 sont les réflexions par rapport aux médiatrices des cotés, et r la rotation d'angle $2\pi/3$ et centrée au centre de gravité de T.

Quitte à renuméroter les s_i, l'application $f : \mathfrak{S}_3 \to G$ telle que $f(\mathrm{id}) = \mathrm{id}$, $f((1\ 2)) = s_1$, $f((1\ 3)) = s_2$, $f((2\ 3)) = s_3$, $f((1\ 2\ 3)) = r$ et $f((1\ 3\ 2)) = r^2$ est un isomorphisme entre G et $\mathfrak{S}_3$. C'est ce qu'on entend en disant que le groupe des isométries du triangle équilatéral *est* $\mathfrak{S}_3$. La structure de groupe est la même, ça n'est qu'un autre avatar du même groupe.

Proposition 1.2

Les automorphismes de G, munis de la composition, forment un groupe $(\mathrm{Aut}(G), \circ)$.

Preuve. Vérifier que c'est un sous-groupe de $(\mathrm{Bij}_G, \circ)$. □

Définition 1.9

Pour tout $g \in G$, l'application

$$\begin{array}{rccc} i_g : & G & \longrightarrow & G \\ & h & \mapsto & ghg^{-1} \end{array}$$

est un automorphisme de G, dit **intérieur**.

On notera que $i_{g^{-1}} = (i_g)^{-1}$ (c'est ce qui permet de voir que i_g est bien bijectif). En fait :

Proposition 1.3
Pour tout groupe G, l'application

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & \mathrm{Aut}(G) \\ & g & \mapsto & i_g \end{array}$$

est un morphisme de groupes tel que $\ker \varphi = \mathcal{Z}(G)$.

Définition 1.10
Si H_1, H_2 sont deux sous-groupes de G, on dit qu'ils sont *conjugués* s'il existe $g \in G$ tel que $H_2 = i_g(H_1)$.

En particulier, deux sous-groupes conjugués de G sont isomorphes, l'isomorphisme étant simplement la restriction $i_g|_{H_1}$. Mais ce n'est pas parce que deux sous-groupes de G sont isomorphes qu'ils sont conjugués. Par exemple, dans $G = \mathrm{GL}_2(\mathbf{R})$, les sous-groupes

$$H_1 = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix},\ x \in \mathbf{R}_+^* \right\} \text{ et } H_2 = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},\ t \in \mathbf{R} \right\}$$

sont tous les deux isomorphes à $(\mathbf{R}, +)$ (faire le calcul). Pourtant, tous les éléments de H_1 sont diagonalisables sur $\mathbf{R}$ alors que la seule matrice diagonalisable de H_2 est I_2. Il n'existe donc pas de conjugaison entre ces sous-groupes.

On notera également que généralement, si $g_1, g_2 \in G$ ont le même ordre fini k, alors $H_1 = \langle g_1 \rangle$ et $H_2 = \langle g_2 \rangle$ sont tous deux isomorphes à $\mathbf{Z}/k\mathbf{Z}$, néanmoins ils ne seront pas forcément conjugués. Par exemple, dans $G = \mathfrak{S}_4$, $g_1 = (1\ 2)(3\ 4)$ et $g_2 = (1\ 2)$ sont d'ordre 2 mais ne sont pas conjuguées (la première est de support total mais pas la deuxième.

1.2 Torsion, Ordre d'un élément

Définition 1.11
Soient G un groupe et $g \in G$. L'*ordre* de g est l'élément $\omega(g)$ de $\mathbf{N} \cup \{\infty\}$ défini par

$$\omega(g) = \min\{n \geqslant 1 \ :\ g^n = e\}.$$

(on rappelle la convention $\min \emptyset = \infty$)

Définition 1.12
Un élément $g \in G$ est dit de *torsion* si $\omega(g) < \infty$.

Exemple 1.4. Dans un groupe fini, tous les éléments sont de torsion, leur ordre divisant l'ordre de G (voir plus bas le théorème de Lagrange). Dans $(\mathbf{C}^*, \times)$, les complexes de module 1 de la forme $e^{i\pi\alpha}$, avec $\alpha \in \mathbf{Q}$, sont tous d'ordre fini. Similairement, dans $\mathrm{GL}_2(\mathbf{R})$, les matrices de rotation dont l'angle est commensurable à π sont d'ordre fini.

Proposition 1.4
Soit g un élément d'un groupe G. On considère l'application

$$\begin{array}{rccc} \varphi_g : & \mathbf{Z} & \longrightarrow & G \\ & n & \mapsto & g^n \end{array}$$

Alors φ_g est un morphisme de groupes, d'image $\langle g \rangle$. Si g est d'ordre infini, alors φ_g est injectif. Sinon, $\ker \varphi_g = n\mathbf{Z}$, où $n = \omega(g)$.

Si g est d'ordre infini alors $\langle g \rangle \simeq \mathbf{Z}$, et si g est d'ordre fini égal à n, alors $\langle g \rangle \simeq \mathbf{Z}/n\mathbf{Z}$.

Preuve. Le fait que φ_g est un morphisme suit des propriétés élémentaires des puissances. Son noyau est donc un sous-groupe de $\mathbf{Z}$, donc de la forme $k\mathbf{Z}$, $k \in \mathbf{N}$. Par définition, $k = 0$ si et seulement si g est d'ordre infini. Lorsqu'il est non nul, on sait que l'entier k est donné par $\min(\ker \varphi_g \cap \mathbf{N}^*)$, ce qui est précisément la définition de $\omega(g)$.

Lorsque g est d'ordre infini, φ_g est injectif et réalise donc un isomorphisme de $\mathbf{Z}$ sur son image $\langle g \rangle$. Lorsque g est d'ordre fini, on peut vérifier directement que l'application $\overline{\phi} : \overline{k} \in \mathbf{Z}/n\mathbf{Z} \mapsto g^k$ est bien définie, et réalise un isomorphisme de $\mathbf{Z}/n\mathbf{Z}$ sur $\langle g \rangle$, mais ceci est un cas particulier du théorème de factorisation énoncé ci-après. □

En particulier, si g est un élément d'ordre n et si $g^m = e$, alors $n|m$. Nous verrons plus en détail la structure des groupes cycliques un peu plus loin en section 2.2. Mais notons déjà deux observations élémentaires :

Proposition 1.5
Soit $g \in G$ un élément d'ordre $n \geqslant 1$.

1. Soit $m \in \mathbf{N}^*$. Alors g^m est d'ordre $n/(n \wedge m)$.
2. Si $f : G \to H$ est un morphisme injectif de groupes, alors $f(g)$ est également d'ordre n.

Notamment, l'ordre d'un élément est un invariant par isomorphisme. Si un groupe G a un élément d'ordre n, alors dans tout groupe isomorphe à G il existe un élément d'ordre n. Ceci permet de dire très rapidement que deux groupes ne sont pas isomorphes.

Preuve.

1. Notons $d = n \wedge m$, et $n = dn'$ et $m = dm'$. Soit $h := g^m$. Alors d'une part $h^{n'} = g^{m'dn'} = e$, donc l'ordre de h divise n'. D'autre part, si $h^k = e$, alors n divise mk, donc n' divise $m'k$, d'où n' divise k puisque m' et n' sont premiers entre-eux. Ainsi, h est bien d'ordre n'.
2. Immédiatement, $f(g)^n = e_H$, ce qui montre que l'ordre de $f(g)$ dans H divise n. De plus, si $f(g)^k = e_H$, alors $g^k \in \ker f = \{e_G\}$, d'où $g^k = e$ et $n|k$.

□

Exercice 1.8
Soient g, h deux éléments d'un groupe G. Supposons $gh = hg$, que g est d'ordre fini n, h d'ordre fini m et que $n \wedge m = 1$. Montrer alors que gh est d'ordre nm.

Donner un contre-exemple lorsque g et h ne commutent pas, et lorsqu'il commutent mais que $n \wedge m \neq 1$.

1.3 Quotient(s) d'un groupe par un sous-groupe, indice, sous-groupes distingués

1.3.1 Relations d'équivalence, ensembles quotients, factorisation

On revient brièvement sur les ensembles quotients des relations d'équivalence.

Soit X un ensemble. Formellement, une relation d'équivalence sur X est une partie $\mathcal{R} \subset X \times X$ vérifiant :

1. $\forall x \in X$, $(x, x) \in \mathcal{R}$ (réflexivité)
2. $\forall x, y \in X$, $(x, y) \in \mathcal{R} \iff (y, x) \in \mathcal{R}$ (symétrie)
3. $\forall x, y, z \in X$, $((x, y) \in \mathcal{R}$ et $(y, z) \in \mathcal{R}) \Rightarrow (x, z) \in \mathcal{R}$ (transitivité)

On note alors $x\mathcal{R}y$ pour signifier $(x, y) \in \mathcal{R}$, qu'on lit « x est en relation avec y ».

Définition 1.13

Si $\mathcal{R}$ est une relation d'équivalence sur X, et si $x \in X$, on définit la **classe d'équivalence** de x (sous-entendu modulo $\mathcal{R}$), notée $C(x)$, comme étant l'ensemble des éléments de X qui sont en relation avec x :

$$C(x) = \{y \in X \mid x\mathcal{R}y\} \subset X.$$

Remarque 1.7. Dans la pratique (groupes quotients, anneaux quotients ...) on n'utilise pas une notation aussi lourde que $C(x)$. Fréquemment, on note $[x]$ ou $\overline{x}$ pour désigner la classe d'équivalence de x modulo une certaine relation d'équivalence.

Par réflexivité, on a $x \in C(x)$ pour tout $x \in X$. Il est donc immédiat que les classes d'équivalence recouvrent tout l'ensemble : $X = \cup_{x \in X} C(x)$. Cependant, il a bien-sûr de la redondance et des classes sont répétées (a priori) plusieurs fois si on parcourt exhaustivement X comme écrit précédemment. Question naturelle : que se passe-t-il lorsque deux classes s'intersectent ? Réponse :

Proposition 1.6

Soient $x, y \in X$. Alors :

- Ou bien $C(x) = C(y)$, ce qui revient à dire $x\mathcal{R}y$,
- Ou bien $C(x) \cap C(y) = \emptyset$.

Ainsi, deux classes d'équivalence qui s'intersectent sont nécessairement égales.

Preuve. Montrons déjà que $C(x) = C(y) \iff x\mathcal{R}y$. Pour l'implication directe, si $C(x) = C(y)$, alors comme $y \in C(y) = C(x)$, on a $x\mathcal{R}y$ par définition. Pour l'autre implication, par symétrie de la relation, il suffit de voir $x\mathcal{R}y \Rightarrow C(y) \subset C(x)$. Supposons donc $x\mathcal{R}y$. Soit alors $z \in C(y)$. Par définition, cela signifie $y\mathcal{R}z$. Par transitivité, on en déduit $x\mathcal{R}z$, c'est à dire $z \in C(x)$, d'où l'inclusion annoncée.

La proposition se reformule en $\forall x, y \in X$, $C(x) \cap C(y) \neq \emptyset \Rightarrow C(x) = C(y)$. Supposons que deux éléments x et y vérifient $C(x) \cap C(y) \neq \emptyset$. Il existe donc $z \in C(x) \cap C(y)$. Ceci signifie $x\mathcal{R}z$ et $y\mathcal{R}z$. Par symétrie et transitivité de $\mathcal{R}$, on en déduit $x\mathcal{R}y$, soit $C(x) = C(y)$ comme on vient de le voir. □

Notons $\mathcal{P}(X)$ l'ensemble des parties de X.

Définition 1.14

On appelle **partition** de X toute famille de parties $(A_i)_{i \in I} \in \mathcal{P}(X)^I$ telle que

1. $\forall i, j \in I$, $i \neq j \Rightarrow A_i \cap A_j = \emptyset$.

2. $X = \bigcup_{i \in I} A_i$.

Revenons à notre relation d'équivalence $\mathcal{R}$ définie sur X.

Définition 1.15

On appelle **système de représentants** des classes de $\mathcal{R}$ toute famille $(x_i)_{i \in I}$ d'éléments de X telle que

$$\forall x \in X,\ \exists ! \, i \in I \ :\ x \in C(x_i).$$

On notera bien qu'en conséquence, $\forall i, j \in I,\ i \neq j \Rightarrow C(x_i) \neq C(x_j)$, ce qui revient à dire que les classes de deux représentants distincts sont disjointes.

Proposition 1.7

Une famille $(x_i)_{i \in I}$ est un système de représentants de la relation $\mathcal{R}$ si et seulement si la famille de leurs classes d'équivalence $(A_i)_{i \in I} = (C(x_i))_{i \in I}$ forme une partition de X.

Proposition 1.8

Toute relation d'équivalence admet (au moins) un système de représentants.

Remarque 1.8. Dans le cas où X est fini (situation qui tout particulièrement nous intéresser par la suite), ceci est très instinctif. On prend un premier élément $x_1 \in X$ quelconque et on regarde sa classe. Ou bien $X = C(x_1)$, et $\{x_1\}$ est bien un système de représentants, ou bien$X \supsetneq C(x_1)$ et il existe $x_2 \in X \setminus C(x_1)$. Si $X = C(x_1) \cup C(x_2)$, alors $\{x_1, x_2\}$ est un système de représentants.Sinon, il existe $x_3 \in X$ tel que $x_3 \notin C(x_1) \cup C(x_2)$ et on considère $C(x_1) \cup C(x_2) \cup C(x_3)$ etc .. Comme X est fini, on est sûr que cet algorithme va s'arrêter, et on aboutit sur un nombre fini d'éléments $x_1, \ldots, x_k \in X$ tels que $(C(x_i))_{i \in \{1,\ldots,k\}}$ forme une partition de X.

On voit vite arriver les limites de cette approche si X est infini. Rien d'étonnant, c'est essentiellement l'axiome du choix. Laissons cette subtilité de côté.

Définition 1.16

On appelle **ensemble quotient de X par la relation $\mathcal{R}$**, et on note $X/\mathcal{R}$, l'ensemble de toutes les classes d'équivalence définies par $\mathcal{R}$:

$$X/\mathcal{R} = \{C(x),\ x \in X\} = \{C(x_i),\ i \in I\},$$

où (x_i) est un système de représentants (quelconque).

Formellement, l'ensemble quotient est donc une partie de l'ensemble des parties de X :

$$X/\mathcal{R} \subset \mathcal{P}(X).$$

Néanmoins, si ce formalisme est nécessaire pour parvenir à une définition satisfaisante, il vaut mieux savoir s'en affranchir pour manipuler les quotients. L'idée reste invariablement la même : on veut *identifier* certains éléments de X et considérer que ce sont les mêmes, on veut *oublier* qu'ils sont distincts dans l'ensemble X de départ et travailler avec le représentant qui nous arrange. C'est un processus cognitif qui s'effectue depuis le plus jeune âge ! Un exemple typique est celui des fractions d'entiers.

Exemple 1.5. Si on suppose connu l'anneau des entiers relatifs $\mathbf{Z}$, on peut définir le corps des nombres rationnels en introduisant sur l'ensemble $X = \mathbf{Z} \times \mathbf{N}^*$ la relation $\mathcal{R}$ donnée par $(p,q)\mathcal{R}(p',q') \iff pq' = p'q$. On définit alors ensemblistement $\mathbf{Q} = (\mathbf{Z} \times \mathbf{N}^*)/\mathcal{R}$, et on va ici choisir de **noter** $\frac{p}{q}$ la classe d'équivalence du couple $(p,q) \in \mathbf{Z}\times\mathbf{N}^*$. On a alors $\frac{p}{q} = \frac{p'}{q'}$ si et seulement si $pq' = p'q$, on reconnaît la règle du produit en croix.

Un système de représentants de cette relation est $\{(p,q) \in \mathbf{Z}\times\mathbf{N}^*,\ p\wedge q = 1\}$: toute fraction a un représentant bien particulier qui est son écriture sous forme irréductible.

On notera que ceci n'est pas une façon de retrouver le corps des rationnels, mais bien de *définir* ce qu'est une fraction. C'est la formalisation du rapport entre deux entiers, une notion pas aussi évidente qu'il n'y paraît. Nous verrons plus loin comment introduire les lois naturelles sur les ensembles quotients.

Exercice 1.9

Soient $\sim$ et $\sim_+$ les relations binaires définies sur $\mathbf{R}^{n+1} \setminus \{0\}$ par $\forall v, w \in \mathbf{R}^{n+1} \setminus \{0\}$,

$$v \sim w \iff \exists \lambda \in \mathbf{R}^* \ :\ w = \lambda.v$$
$$v \sim_+ w \iff \exists \lambda \in \mathbf{R}_+^* \ :\ w = \lambda.v$$

1. Justifier que ce sont des relations d'équivalence.
2. Quelles sont les classes d'équivalence de $\sim$?
3. Donner une bijection entre l'ensemble quotient $(\mathbf{R}^{n+1} \setminus \{0\})/\sim_+$ et la sphère unité $\mathbf{S}^n$ définie par $\mathbf{S}^n = \{x \in \mathbf{R}^{n+1} \ :\ x_1^2 + \cdots + x_{n+1}^2 = 1\}$.

On note $P^n(\mathbf{R}) := (\mathbf{R}^{n+1} \setminus \{0\})/\sim$, l'*espace projectif réel* de dimension n.

4. Définir une relation d'équivalence $\mathcal{R}$ sur $\mathbf{S}^n$ telle que $\mathbf{S}^n/\mathcal{R}$ est en bijection avec $P^n(\mathbf{R})$.

Si K est un corps quelconque, on définit l'*espace projectif sur* K par $P^n(K) = (K^{n+1} \setminus \{0\})/\sim$, où similairement $v \sim w \iff \exists \lambda \in K^* \ :\ w = \lambda.v$.

5. Donner une bijection naturelle entre la *droite projective complexe* $P^1(\mathbf{C})$ et la sphère $\mathbf{S}^2$.

À présent notons $[x] \in X/\mathcal{R}$ la classe d'équivalence de $x \in X$ modulo $\mathcal{R}$.

Définition 1.17

Étant donné X muni d'une relation d'équivalence $\mathcal{R}$, on appelle **projection canonique** l'application

$$\begin{array}{rccc} \pi : & X & \longrightarrow & X/\mathcal{R} \\ & x & \mapsto & [x] \end{array}$$

Elle est surjective par définition, et $\pi(x) = \pi(y) \iff x\mathcal{R}y$.

Proposition 1.9

Soit X un ensemble muni d'une relation d'équivalence $\mathcal{R}$ dont on note π la projection canonique. Soit $f : X \to Y$ une application à valeurs dans un autre ensemble Y. Les propositions suivantes sont équivalentes :

1. f est constante sur les classes d'équivalence de $\mathcal{R}$.
2. Il existe une application $\overline{f} : X/\mathcal{R} \to Y$ telle que $f = \overline{f} \circ \pi$.

Lorsqu'elle existe, une telle application $\overline{f}$ est nécessairement unique, on l'appelle

application induite au quotient par f.

Preuve. (1) $\Rightarrow$ (2) : Si une telle application $\overline{f}$ existe, alors nécessairement pour tout $x \in X$, on a $\overline{f}(\overline{x}) = \overline{f}(\pi(x)) = f(x)$. Elle est donc complètement déterminée par f puisque la projection canonique est surjective. La question est de voir si ceci *définit* bien une fonction (un point a-t-il bien une et une seule image ?). Il faut donc voir que si y est un autre élément de X tel que $\overline{y} = \overline{x}$, alors $f(y) = f(x)$. Or si $\overline{x} = \overline{y}$, cela signifie que x et y appartiennent à la même classe d'équivalence. La fonction f étant constante sur les classes d'équivalence par hypothèse, on a bien $f(y) = f(x)$.

(2) $\Rightarrow$ (1) : Soient $x, y \in X$. Si $x\mathcal{R}y$, alors $\pi(x) = \pi(y)$, d'où $f(x) = \overline{f}(\overline{x}) = \overline{f}(\overline{y}) = f(y)$. Ceci montre bien que f prend une seule valeur sur une classe d'équivalence donnée. □

1.3.2 Quotient par un sous-groupe, théorème de Lagrange, structure de groupe au quotient, sous-groupes distingués

Soit G un groupe et H un sous-groupe de G. Le quotient à droite de G par H est l'ensemble quotient de G pour la relation d'équivalence $g_1 \sim_d g_2 \iff g_1^{-1}g_2 \in H$. On le note G/H. Similairement, le quotient à gauche de G par H est l'ensemble quotient de G par la relation d'équivalence $g_1 \sim_g g_2 \iff g_1 g_2^{-1} \in H$. On le note $H\backslash G$.

Un élément de G/H est de la forme $gH = \{gh,\ h \in H\}$, où $g \in G$, alors qu'un élément de $H\backslash G$ est de la forme $Hg = \{hg,\ h \in H\}$.

Remarque 1.9. Point glissant : beaucoup de références classiques appellent « classe à gauche » les éléments gH de G/H (Perrin, Lang, Bourbaki). Néanmoins, une telle appellation semble quand même assez questionnable. Les classes gH sont les orbites de H pour l'action par multiplication à droite, il est raisonnable de parler de classes à droite et d'appeler G/H le quotient à droite de G par H.

Le problème ayant peu d'intérêt, pour faire simple, on pourra le plus souvent possible éviter de les citer nommément, comme on va le faire par la suite.

Proposition 1.10
Les quotients G/H et $H\backslash G$ sont en bijection.

Preuve. La bijection est donnée par $gH \in G/H \mapsto Hg^{-1} \in H\backslash G$, cette application étant bien définie parce que pour tous $g_1, g_2 \in G$, $g_1 \sim_d g_2$ si et seulement si $g_1^{-1} \sim_g g_2^{-1}$. □

Définition 1.18
Soient G et $H < G$ un sous-groupe. On dit que H est d'*indice fini* dans G si G/H (et donc $H\backslash G$) sont finis. Sinon, on dit que H est d'ordre infini. Dans tous les cas, on note $[G : H] = \mathrm{card}(G/H) = \mathrm{card}(H\backslash G) \in \mathbf{N}^* \cup \{\infty\}$, appelé *indice de G dans H*.

Théorème 1.1 (Lagrange)
Soient G un groupe fini et $H < G$ un sous groupe. Alors $|H|$ divise $|G|$. Plus précisément, on a $|G|/|H| = \mathrm{card}(G/H) = \mathrm{card}(H\backslash G)$.

Attention, ni G/H ni $H\backslash G$ ne sont des groupes à ce stade !

Preuve. On le fait par exemple pour le quotient à droite. On choisit $g_1, \dots, g_k \in G$ des représentants des classes d'équivalences de $\sim_d$, de sorte qu'on ait la partition suivante

$$G = \bigsqcup_{1 \leqslant i \leqslant k} g_i H.$$

(Le symbole $\sqcup$ signifie réunion disjointe.)

Vérifions que pour tout $g \in G$, $\mathrm{card}(gH) = |H|$. Soit $L_g : H \to gH$ l'application $h \mapsto gh$. On voit directement qu'elle est injective, et comme elle est sujective par définition, H et gH sont en bijection et ils ont donc le même cardinal.

Dès lors, comme la réunion ci-dessus est disjointe, on a

$$|G| = \sum_{i=1}^{k} \mathrm{card}(g_i H) = \sum_{i=1}^{k} |H| = k|H|.$$

Comme $k = \mathrm{card}(G/H)$ par définition, on a bien le résultat annoncé. □

Corollaire 1.1

Soit G un groupe fini. Alors $g \in G$ est d'ordre fini, et $\omega(g)$ divise $|G|$. En particulier, $g^{|G|} = e$ pour tout g.

Preuve. Ceci vient du fait que $\langle g \rangle$ est un sous-groupe fini de G, d'ordre $\omega(g)$. Si on écrit $|G| = k\omega(g)$, alors $g^{|G|} = (g^{\omega(g)})^k = e$. □

À présent on voudrait une structure de groupe naturelle sur G/H ou $H\backslash G$. La loi la plus plausible est $g_1 H \star g_2 H = g_1 g_2 H$, c'est à dire une structure de groupe telle que π_d soit un morphisme.

Problème : ceci n'est pas bien défini en général. Néanmoins :

Proposition 1.11

Soient G un groupe et $H < G$ un sous-groupe. Il y a équivalence entre les propriétés suivantes.

1. Il existe une loi de groupe sur G/H telle que la projection canonique π_d soit un morphisme.
2. Il existe une loi de groupe sur $H\backslash G$ telle que la projection canonique π_g soit un morphisme.
3. Pour tout $g \in G$, $gH = Hg$.
4. Pour tout $g \in G$, $gHg^{-1} = H$.
5. Il existe un morphisme de groupe $f : G \to G_1$ tel que $H = \ker f$.

Définition 1.19

Un sous-groupe H vérifiant ces conditions équivalentes est dit *distingué* (ou *normal*) dans G. On note alors $H \triangleleft G$.

On note que lorsque H est distingué, classes à gauche et à droite coïncident. Il n'y a donc plus à considérer séparément G/H et $H\backslash G$. On parlera donc de *la* projection canonique de G sur G/H.

Remarque 1.10. On notera que lorsqu'elle existe, une structure de groupe sur G/H ou $H\backslash G$ rendant la projection canonique multiplicative est nécessairement **unique**.

Exemple 1.6.

- Les sous-groupes triviaux de G, à savoir $\{e\}$ et G lui-même sont toujours distingués.
- Dans un groupe abélien, tous les sous-groupes sont distingués. Le centre $\mathcal{Z}(G)$ d'un groupe est toujours un sous-groupe distingué.
- Dans $\mathfrak{S}_3$, le sous-groupe $\langle(123)\rangle$ est distingué.

Définition 1.20

Soit G un groupe. Pour tous $g, h \in G$, on définit le *commutateur* de g et h par $[g,h] = ghg^{-1}h^{-1}$. On appelle *sous-groupe dérivé* de G, et on note $D(G)$, le sous groupe engendré par les commutateurs :

$$D(G) = \langle [g,h],\ g,h \in G \rangle.$$

Remarque 1.11. On rencontre également la notation $[G,G]$ pour le sous-groupe dérivé d'un groupe G.

Remarque 1.12. Attention, c'est le sous-groupe engendré par les commutateurs. L'ensemble des commutateurs ne forme pas un sous-groupe en général.

Proposition 1.12

Le sous-groupe dérivé $D(G)$ est un sous-groupe distingué de G. Mieux, c'est un sous-groupe **caractéristique** : pour tout $f \in \mathrm{Aut}(G)$, $f(D(G)) = D(G)$.

Le quotient $G/D(G)$ est abélien, et c'est le plus grand quotient abélien de G : pour tout sous-groupe $H \subset G$, on a équivalence entre

1. $D(G) \subset H$
2. $H \triangleleft G$ et G/H est abélien.

Définition 1.21

Le quotient $G/D(G)$ est appelé l'*abélianisé* de G.

Preuve. Vérifions que $D(G)$ est caractéristique. Soit $f \in \mathrm{Aut}(G)$. Soient $x, y \in G$. Alors $f([x,y]) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x), f(y)]$, montrant que l'image d'un commutateur est un commutateur, d'où $f(D(G)) \subset D(G)$ pour tout $f \in \mathrm{Aut}(G)$. Donc $f^{-1}(D(G)) \subset D(G)$ et donc $D(G) \subset f(D(G))$. En appliquant ceci à un automorphisme intérieur $f = i_g$, cela montre que $D(G) \triangleleft G$.

Soit maintenant $H \triangleleft G$ un sous-groupe distingué tel que G/H est abélien. Notons $\pi : G \to G/H$ la projection canonique. Comme G/H est abélien, pour tous $g_1, g_2 \in G$, nous avons $\pi([g_1,g_2]) = e_{G/H}$. Ainsi, $H = \ker \pi$ contient tous les commutateurs d'éléments de G. Par définition, ceci implique que $D(G) \subset H$.

Inversement, si $D(G) \subset H$, alors pour tous $g \in G$ et $h \in H$, comme $ghg^{-1}h^{-1} \in D(G)$, on a $ghg^{-1}h^{-1} \in H$, d'où $ghg^{-1} \in H$. Ceci montre que $gHg^{-1} \subset H$ pour tout $g \in G$, et H est donc distingué dans G. On vérifie alors comme précédemment que G/H est abélien. Si $\pi : G \to G/H$ désigne la projection canonique, alors pour tous $g, h \in G$, $[\pi(g), \pi(h)] = \pi([g,h]) = e_{G/H}$ puisque $[g,h] \in H$. Ainsi, $\pi(g)$ et $\pi(h)$ commutent, ce qui montre que G/H est abélien.

□

Exercice 1.10
Déterminer le groupe dérivé de $\mathbf{H}_8$ et identifier l'abélianisé.

Exercice 1.11
Montrer que le sous-groupe dérivé de $\mathrm{GL}_n(K)$ est $\mathrm{SL}_n(K)$, sauf si $n = 2$ et K est de caractéristique 2. De même, montrer que $D(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)$.

En déduire que pour tout groupe abélien G, tout morphisme $\mathrm{SL}_n(K) \to G$ est trivial.

Donnons un dernier exemple général important de sous-groupe distingué.

Proposition 1.13
Soit G un groupe. Dans le groupe $\mathrm{Aut}(G)$, le sous-groupe des automorphismes intérieurs est distingué. On appelle groupe des *automorphismes extérieurs* le quotient $\mathrm{Ext}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$.

Le résultat suivant est très important, il permet notamment de construire des isomorphismes entre groupes quotients.

Proposition 1.14
Soit $f : G \to G'$ un morphisme de groupes. Soit $H = \ker f$. Alors il existe un unique morphisme de groupes injectif $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ \pi$, où $\pi : G \to G/H$ est la projection canonique. En particulier, $\overline{f}$ induit un isomorphisme

$$\overline{f} : G/\ker f \to \mathrm{Im}(f).$$

On dit que f se *factorise* en $\overline{f}$, ou encore que f *descend au quotient* en $\overline{f}$.

Exemple 1.7.
1. Si g est un élément d'ordre n de G, alors l'application φ_g définie plus haut se factorise en un morphisme injectif $\mathbf{Z}/n\mathbf{Z} \to G$, d'image $\langle g \rangle$.
2. En considérant le noyau du morphisme surjectif $f : t \in (\mathbf{R}, +) \mapsto e^{it} \in \mathbb{U}$, on obtient un isomorphisme $\mathbb{U} \simeq \mathbf{R}/2\pi\mathbf{Z}$, entre le groupe multiplicatif des nombres complexes de module 1 et le groupe quotient $\mathbf{R}/2\pi\mathbf{Z}$.
3. L'action naturelle de $\mathrm{SL}_2(\mathbf{Z})$ sur $\mathbb{H}_2 = \{z \in \mathbf{C} \ : \ \mathrm{Im}(z) > 0\}$ factorise en une action de $\mathrm{PSL}_2(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z})/\{\pm \mathrm{id}\}$. Analogue pour les actions projectives.
4. Si G est un groupe fini et $f : G \to G'$ un morphisme de groupes, alors $|G| = |\mathrm{Im}(f)| \times |\ker(f)|$.

Remarque 1.13. Ce résultat, bien qu'élémentaire, est très récurrent. On le retrouve dans des cadres avec plus de structure algébrique, comme en algèbre linéaire, ou dans le cas des quotients d'anneaux par des idéaux.

Exemple 1.8. Soient E, F deux espaces vectoriels sur un même corps de base et soit $f : E \to F$ une application linéaire. Alors f induit un isomorphisme d'espaces vectoriels $\overline{f} : E/\ker(f) \to \mathrm{Im}(f)$. On en déduit le *théorème du rang* en dimension finie :

$$\mathrm{Rg}(f) = \dim(E/\ker(f)) = \dim E - \dim \ker(f).$$

Rappelons que pour tout sous-espace F de E, le groupe additif quotient E/F admet une structure d'espace vectoriel naturelle, et que si $\dim E < \infty$, alors E/F est de dimension finie et $\dim(E/F) = \dim E - \dim F$ (cf feuille de TD2).

Exemple 1.9. Soit $f : \mathbf{R}[X] \to \mathbf{C}$ l'application donnée par $f(P) = P(i)$ pour tout $P \in \mathbf{R}[X]$. C'est un morphisme d'anneaux, surjectif puisque $f(\mathbf{R}_1[X]) = \{a+ib,\ a, b \in \mathbf{R}\} = \mathbf{C}$, et son noyau est $\ker(f) = (X^2+1)\mathbf{R}[X]$, l'idéal engendré par X^2+1, noté (X^2+1). On obtient alors par factorisation de f un isomorphisme d'anneaux

$$\overline{f} : \mathbf{R}[X]/(X^2+1) \to \mathbf{C}.$$

Exercice 1.12
Déterminer les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$.

On déduit de ce résultat de factorisation une preuve d'un résultat important, dans le cas des groupes abéliens.

Théorème 1.2 (Cauchy : cas abélien)

Soit G un groupe abélien fini d'ordre n. Soit $p > 1$ un facteur premier de n. Alors il existe un élément d'ordre p dans G.

Remarque 1.14. On rappelle que d'après le théorème de Lagrange, l'ordre d'un élément divise toujours l'ordre du groupe. Ce résultat, en fait valable pour tout groupe fini (**ref**), donne la réciproque lorsque le diviseur de n est premier. Le premier théorème de Sylow améliore encore ceci.

Preuve. Comme G est fini, il finiment engendré. Soient $g_1, \dots, g_k$ des éléments engendrant G. Puisqu'il est abélien, il se met sous la forme $G = \{g_1^{m_1} \dots g_k^{m_k},\ m_1, \dots, m_k \in \mathbf{Z}\}$, et l'application

$$\begin{array}{rccc} f : & \langle g_1\rangle \times \cdots \times \langle g_k\rangle & \longrightarrow & G \\ & (g_1^{m_1}, \dots, g_k^{m_k}) & \mapsto & g_1^{m_1} \dots g_k^{m_k} \end{array}$$

est un morphisme surjectif (il est capital que G soit commutatif pour cela !). D'après le théorème de factorisation, on en déduit $|\langle g_1\rangle \times \cdots \times \langle g_k\rangle| = |G|.|\ker f|$. Comme p est un facteur premier de $n = |G|$, on en déduit que p divise $|\langle g_1\rangle| \cdots |\langle g_k\rangle|$, donc qu'il existe un $i \in \{1, \dots, k\}$ tel que p divise $|\langle g_i\rangle| = n_i$, où $n_i = \omega(g_i)$ est l'ordre de g_i. Ainsi, en écrivant $n_i = pm_i$, on en déduit que $g_i^{m_i}$ est d'ordre p. □

Remarque 1.15. Soient G_1, G_2, H des groupes. Si $f : G_1 \times G_2 \to H$ est un morphisme, alors les images $f(G_1)$ et $f(G_2)$ "commutent" : pour tout $h_i \in f(G_i)$, on a $h_1h_2 = h_2h_1$.

Exercice 1.13
Vérifier que la donnée d'un morphisme $f : \mathbf{Z}^n \to G$ est la même que celle d'un n-uplet $(g_1, \dots, g_n)$ d'éléments qui commutent deux à deux.

Remarque 1.16. La fin de la preuve était le cas où G est cyclique, on a pu s'y ramener en démontrant qu'il existe un sous-groupe cyclique de G dont l'ordre est divisible par p.

1.4 Groupe symétrique : une première couche de rappels

On rappelle que le groupe symétrique d'ordre n (appellation à éviter à mon avis, mais fréquente), noté $\mathfrak{S}_n$ est par définition l'ensemble des permutations $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ muni de la composition. Il est fini d'ordre $n!$.

Une permutation σ se représente concrètement comme une matrice de taille $2 \times n$ de la façon suivante :

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

Définition 1.22

Si σ est une permutation, son support est $\{i \ : \ \sigma(i) \neq i\}$. On appelle **dérangement** une permutation de support total.

On appelle **transposition** toute permutation τ dont le support contient exactement deux éléments, disons i et j, qu'elle échange nécessairement. On note une telle transposition $\tau = (i\ j)$ (notation généralisée plus loin avec les k-cycles).

En particulier τ est d'ordre 2 dans $\mathfrak{S}_n$.

Proposition 1.15

Pour toute transposition $(i\ j)$, et pour toute permutation $\sigma \in \mathfrak{S}_n$, on a

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

En particulier, toutes les transpositions sont conjuguées.

Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en un produit de transposition. Autrement dit, $\mathfrak{S}_n$ est engendré par les transpositions.

Preuve. Preuve du fait que les transpositions engendrent $\mathfrak{S}_n$. □

Exercice 1.14

Montrer que $\mathfrak{S}_n$ est engendré par les transpositions $(i\ i+1)$, pour $1 \leqslant i \leqslant n$.

Proposition 1.16

Pour tout $n \geqslant 3$, $\mathfrak{S}_n$ n'est pas engendré par $n-2$ transpositions ou moins.

Preuve. On commence par l'observation suivante : si $\sigma_1, \dots, \sigma_r \in \mathfrak{S}_n$ engendrent $\mathfrak{S}_n$, alors $[\![1, n]\!] = \cup_{1 \leqslant i \leqslant r} \mathrm{Supp}(\sigma_i)$. En effet, dans le cas contraire, il existerait $k_0 \in [\![1, n]\!]$ tel que $\sigma_i(k_0) = k_0$ pour tout i, montrant que $\sigma_i \in \mathrm{Stab}_{\mathfrak{S}_n}(k_0)$ pour tout i et donc que $\langle \sigma_1, \dots, \sigma_r \rangle \subset \mathrm{Stab}_{\mathfrak{S}_n}(k_0) \subsetneq \mathfrak{S}_n$.

On se donne à présent $\tau_1, \dots, \tau_r$ des transpositions engendrant $\mathfrak{S}_n$. On note $A_i = \mathrm{Supp}(\tau_i)$ pour tout i, de sorte que les A_i sont des parties à deux éléments, qui recouvrent $[\![1, n]\!]$ d'après ce qu'on vient d'observer.

On prouve alors le résultat combinatoire suivant :

Lemme 1.1

Soient $n \geqslant 4$ et $X_1, \dots, X_r \subset [\![1, n]\!]$ des parties de cardinal 2, telles que $[\![1, n]\!] = X_1 \cup \cdots \cup X_r$. Si $r \leqslant n-2$, alors il existe une partition $[\![1, r]\!] = I \cup J$, avec $I \neq \emptyset$ et $J \neq \emptyset$ et telle que

$$\left(\bigcup_{i \in I} X_i \right) \cap \left(\bigcup_{j \in J} X_j \right) = \emptyset.$$

Démonstration. On démontre la contraposée : supposons qu'il n'existe pas de telle partition, et montrons que $r > n-2$.

On définit une permutation $\sigma \in \mathfrak{S}_r$ par induction :

— $\sigma(1) = 1$

— Pour $1 \leqslant k \leqslant r-1$, prenons

$$\sigma(k+1) = \min\{i \in [\![1, r]\!] \setminus \{\sigma(1), \dots, \sigma(k)\} \mid X_i \cap (X_{\sigma(1)} \cup \cdots \cup X_{\sigma(k)}) \neq \emptyset\}$$

Notons bien que σ est bien définie puisque si on avait $\forall i \in [\![1,r]\!] \setminus \{\sigma(1),\dots,\sigma(k)\}$, $X_i \cap (X_{\sigma(1)} \cup \cdots \cup X_{\sigma(k)}) = \emptyset$, alors cela contredirait notre hypothèse avec $I = \{\sigma(1),\dots,\sigma(k)\}$ et $J = [\![1,r]\!] \setminus I$.

Par construction, $\sigma : [\![1,r]\!] \to [\![1,r]\!]$ est injective, donc bijective. On montre alors par récurrence finie sur $k \in [\![1,r]\!]$ que $\sharp(X_{\sigma(1)} \cup \cdots \cup X_{\sigma(k)}) \leqslant k+1$.

— Initialisation $k = 1$: $X_{\sigma(1)}$ est de cardinal 2 par hypothèse.

— Hérédité : Supposons $\sharp(X_{\sigma(1)} \cup \cdots \cup X_{\sigma(k)}) \leqslant k+1$ pour un certain $k \in [\![1, r-1]\!]$. Alors

$$\begin{aligned}\sharp(X_{\sigma(1)} \cup \cdots \cup X_{\sigma(k)} \cup X_{\sigma(k+1)}) &\leqslant k+1+\sharp X_{\sigma(k+1)} \\ &\quad - \underbrace{\sharp((X_{\sigma(1)} \cup \cdots \cup X_{\sigma(k)}) \cap X_{\sigma(k+1)})}_{\geqslant 1 \text{ par construction}} \\ &\leqslant k+2,\end{aligned}$$

ce qui établit l'hérédité, et termine la récurrence.

On a alors $\sharp(X_{\sigma(1)} \cup \cdots \cup X_{\sigma(r)}) = \sharp(X_1 \cup \cdots \cup X_r) = \sharp[\![1,n]\!] = n \leqslant r+1$, comme attendu. □

Supposons maintenant $r \leqslant n-2$ et appliquons le lemme à $A_1,\dots,A_r$. Appelons $G_1 = \langle\{\tau_i,\ i \in I\}\rangle$ et $G_2 = \langle\{\tau_j,\ j \in J\}\rangle$. Montrons que pour tous $\sigma_1 \in G_1$ et $\sigma_2 \in G_2$, $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Pour cela, considérons d'abord pour tout $j \in J$, le centralisateur (dans $\mathfrak{S}_n$) de τ_j défini par $\mathcal{Z}(\tau_j) = \{\sigma \in \mathfrak{S}_n \mid \sigma\tau_j = \tau_j\sigma\}$. On vérifie que c'est un sous-groupe de $\mathfrak{S}_n$ et il contient les τ_i, $i \in I$ par construction. Il contient donc le sous-groupe qu'elles engendrent, ainsi $G_1 \subset \mathcal{Z}(\tau_j)$ pour tout $j \in J$. Si on considère maintenant le centralisateur $\mathcal{Z}(G_1) = \{\sigma \in \mathfrak{S}_n \mid \forall\sigma_1 \in G_1,\ \sigma\sigma_1 = \sigma_1\sigma\} = \cap_{\sigma_1 \in G_1}\mathcal{Z}(\sigma_1)$, c'est un sous-groupe de $\mathfrak{S}_n$ qui contient tous les τ_j, $j \in J$. Il contient donc G_2, ce qui signifie bien que toute permutation de G_1 commute avec toute permutation de G_2.

Vérifions à présent que $\mathfrak{S}_n = \{\sigma_1\sigma_2,\ \sigma_1 \in G_1,\ \sigma_2 \in G_2\}$. Appelons H le membre de droite. C'est un sous-groupe de $\mathfrak{S}_n$ puisqu'il contient id, que pour toutes σ_1, σ_2, on a $(\sigma_1\sigma_2)^{-1} = \sigma_1^{-1}\sigma_2^{-1} \in H$ puisqu'elles commutent et $\sigma_1\sigma_2\sigma_1'\sigma_2' = (\sigma_1\sigma_1')(\sigma_2\sigma_2') \in H$ toujours grâce aux relations de commutation. Ainsi, H est un sous-groupe de $\mathfrak{S}_n$ contenant G_1 et G_2, donc en particulier H contient $\tau_1,\dots,\tau_r$ et donc $H = \mathfrak{S}_n$.

Montrons maintenant que $G_1 \triangleleft \mathfrak{S}_n$. Soit $\tilde{\sigma}_1 \in G_1$ et soit $\sigma \in \mathfrak{S}_n$. D'après ce qu'on vient de voir, il existe $\sigma_1 \in G_1$ et $\sigma_2 \in G_2$ telles que $\sigma = \sigma_1\sigma_2$. Nous avons donc $\sigma\tilde{\sigma}_1\sigma^{-1} = \sigma_1 \underbrace{\sigma_2\tilde{\sigma}_1\sigma_2^{-1}}_{=\tilde{\sigma_1}} \sigma_1^{-1} = \sigma_1\tilde{\sigma}_1\sigma_1^{-1} \in G_1$, parce que σ_2 et $\tilde{\sigma}_1$ commutent.

Puisque G_1 est distingué et qu'il contient (au moins) une transposition, il les contient toutes. En effet, si $(i\ j) \in G_1$ et si $(k\ \ell)$ est une transposition quelconque, si on se donne une permutation arbitraire $\sigma \in \mathfrak{S}_n$ telle que $\sigma(i) = k$ et $\sigma(j) = \ell$, alors $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j)) = (k\ \ell) \in \sigma G_1\sigma^{-1} = G_1$. Comme les transpositions engendrent $\mathfrak{S}_n$, on en déduit $G_1 = \mathfrak{S}_n$, une contradiction puisque les éléments de G_1 sont tous à support contenu dans $\cup_{i\in I}A_i \subsetneq [\![1,n]\!]$ (même argument qu'au début). □

On notera que la preuve a mis en avant deux propriétés intéressantes et valides plus généralement :

Proposition 1.17

Soit G un groupe et soient $A_1, A_2 \subset G$ deux parties telles que $\forall(g_1,g_2) \in A_1 \times A_2$, $g_1g_2 = g_2g_1$. Soient $G_1 = \langle A_1\rangle$ et $G_2 = \langle A_2\rangle$. Alors $\forall(g_1,g_2) \in G_1 \times G_2$, $g_1g_2 = g_2g_1$. Si $H = \langle A_1 \cup A_2\rangle$, alors $H = G_1G_2$ et $G_1 \triangleleft H$ et $G_2 \triangleleft H$.

Preuve. Exactement pareil. □

De même, on pourra retenir la définition du centralisateur d'une partie d'un groupe.

Proposition 1.18
Soit G un groupe et soit $A \subset G$ une partie. Alors $\{g \in G \mid \forall h \in A,\ gh = hg\}$ est un sous-groupe de G, appelé **centralisateur de** A (dans G), et noté $\mathcal{Z}_G(A)$ ou simplement $\mathcal{Z}(A)$ s'il n'y a pas d'ambiguïté.

Exercice 1.15
Montrer que pour toute partie $A \subset G$, on a $\mathcal{Z}(A) = \mathcal{Z}(\langle A \rangle)$.

Définition 1.23
Soit σ une permutation de $\{1, \dots, n\}$. On appelle **matrice de permutation** associée à σ la matrice P_σ qui est la matrice dans la base canonique de $\mathbf{R}^n$ de l'endomorphisme u_σ défini par $u_\sigma(e_i) = e_{\sigma(i)}$ pour tout i, où $(e_1, \dots, e_n)$ désigne la base canonique de $\mathbf{R}^n$.

De façon équivalente, on peut définir P_σ comme la matrice dont le coefficient (i, j) est $\delta_{i,\sigma(j)}$, où $\delta_{i,j}$ désigne le symbole de Kronecker.

Proposition 1.19
L'application $\{\sigma \mapsto P_\sigma\}$ est un morphisme injectif de $\mathfrak{S}_n$ dans $\mathrm{GL}_n(\mathbf{R})$.

C'est un exemple de *représentation linéaire fidèle* du groupe symétrique.

Exercice 1.16
Prouver la proposition précédente.

Théorème 1.3
Il existe un unique morphisme non trivial ε de $\mathfrak{S}_n$ vers $\{\pm 1\}$, appelé *signature*.

Exercice 1.17
Soit G un groupe fini. Montrer que tout morphisme $G \to (\mathbf{R}^*, \times)$ est à image dans $\{\pm 1\}$. Généraliser à $\mathbf{C}^*$.

Preuve. (Unicité) Notons que nécessairement $\varepsilon(\tau) = -1$ pour toute transposition τ. En effet, premièrement, si $\varepsilon(\tau) = 1$ pour toute transposition, alors $\varepsilon \equiv 1$ puisque $\mathfrak{S}_n$ est engendré par les transpositions. Il existe donc une transposition τ_0 telle que $\varepsilon(\tau_0) = -1$. Ensuite, si τ est quelconque, alors il existe une permutation σ telle que $\tau = \sigma\tau_0\sigma^{-1}$, d'où $\varepsilon(\tau) = \varepsilon(\tau_0) = -1$.

Comme les transpositions engendrent $\mathfrak{S}_n$, toute permutation s'écrit $\sigma = \tau_1 \dots \tau_k$, alors $\varepsilon(\sigma) = (-1)^k$. D'où l'unicité (s'il existe) d'un tel morphisme. Mais attention, ceci ne suffit pas à la définir : il faudrait s'assurer que ceci ne dépend pas de la décomposition en produit de transposition, qui n'est pas unique. □

Un corollaire de ce théorème est donc : La *parité* du nombre de transpositions dans la décomposition en produit de transpositions d'une permutation est indépendant de la décomposition. Si cela en découle, ce n'est pas facile de le démontrer directement, la définition classique passe par le **nombre d'inversion**.

Définition 1.24

Soit σ une permutation. On appelle **nombre d'inversion** de σ, et on note $I(\sigma)$, l'entier

$$I(\sigma) = \mathrm{card}\{(i,j) \in \{1,\dots,n\}^2 \ : \ i < j \text{ et } \sigma(i) > \sigma(j)\}.$$

On peut alors démontrer :

Théorème 1.4

Pour toutes $\sigma_1, \sigma_2 \in \mathfrak{S}_n$, on a $(-1)^{I(\sigma_1\sigma_2)} = (-1)^{I(\sigma_1)}(-1)^{I(\sigma_2)}$.

Une fois ceci établi, on en déduit l'existence de la signature, il suffit en effet de prendre $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ pour toute $\sigma \in \mathfrak{S}_n$. Cette construction nous permet pratiquement de déterminer la signature d'une permutation explicite en comptant le nombre de croisements des flèches [Dessin].

Remarque 1.17. De façon plus condensée, on peut également définir la signature via

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Définition 1.25

On appelle **sous-groupe alterné**, et on note $\mathcal{A}_n$ le sous-groupe $\mathcal{A}_n = \ker \varepsilon$.

C'est donc le sous-groupe de $\mathfrak{S}_n$ formé des permutations *paires*, *i.e.* admettant un nombre pair d'inversions, ou bien qui s'écrivent comme produit d'un nombre pair de transpositions.

Proposition 1.20

$\mathcal{A}_n \triangleleft \mathfrak{S}_n$ et $\mathfrak{S}_n/\mathcal{A}_n \simeq \{\pm 1\}$. En particulier, $|\mathcal{A}_n| = n!/2$.

On définit à présent les cycles, qui nous donnent une décomposition naturelle et unique d'une permutation. L'idée est intuitive mais on a besoin d'un peu de formalisme pour le faire proprement.

Soit $\sigma \in \mathfrak{S}_n$. Il lui correspond alors une action de $\mathbf{Z}$ sur $\{1,\dots,n\}$, dont on utilise la partition en orbites pour obtenir la décomposition de σ en produit de cycles à support disjoints. On le fait ici sans utiliser le vocabulaire des actions de groupes pour des raisons chronologiques du déroulement du cours.

Sur $X = \{1,\dots,n\}$, on introduit la relation d'équivalence suivante : $i \sim_\sigma j$ si et seulement si $\exists k \in \mathbf{Z} \ : \ j = \sigma^k(i)$. Comme pour toute relation d'équivalence, X se partitionne en classes d'équivalence pour $\sim_\sigma$. Les classes de cardinal 1 sont les points fixes de σ, leur complémentaire le support de σ.

Définition 1.26

On dit que σ est un k-cycle, pour $2 \leqslant k \leqslant n$, si le support de σ est de cardinal k et ne contient qu'une seule classe d'équivalence de $\sim_\sigma$. On ordonne alors ses éléments $a_1,\dots,a_k$ de sorte que $a_{i+1} = \sigma(a_i)$ et on écrit $\sigma = (a_1\ a_2\ \cdots\ a_k)$.

Proposition 1.21
Si $c = (a_1, \dots, a_k) \in \mathfrak{S}_n$ est un k-cycle, et $\sigma \in \mathfrak{S}_n$, alors

$$\sigma c \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Proposition 1.22
Toute permutation σ s'écrit comme un produit (commutatif) de cycles à **supports disjoints** $\sigma = c_1 \dots . c_k$. À permutation près de $c_1, \dots, c_k$, cette décomposition est unique.

Preuve. On reprend la relation d'équivalence définie par σ sur $\{1, \dots, n\}$. □

Exemple 1.10. Un exemple explicite pris au hasard.

Remarque 1.18. On retiendra bien que deux permutations à supports disjoints commutent.

Exercice 1.18
Combien y a-t-il de cycles de longueur k dans $\mathcal{S}_n$?

Exercice 1.19
Quelle est la signature d'un k-cycle ?

Théorème 1.5
Soient σ, τ deux permutations dont les décompositions en produit de cycles à supports disjoints sont $\sigma = c_1 \dots c_k$ et $\tau = c'_1 \dots c'_\ell$.

Alors, σ et τ sont conjuguées si et seulement si $\ell = k$ et si, quitte à réordonner, c_i et c'_i sont de même longueur pour tout $1 \leqslant i \leqslant k$.

Preuve. Ceci repose essentiellement sur le

Lemme 1.2
Pour tous $k \leqslant n$ et tout k-uplets d'éléments deux à deux distincts $(a_1 \dots a_k)$ et $(b_1 \dots b_k)$, il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que pour tout $1 \leqslant i \leqslant k$, $\sigma(a_i) = b_i$.

□

Corollaire 1.2
Dans le groupe symétrique, il y a exactement p_n classes de conjugaison, où p_n est le *nombre de partitions* de n en somme d'entiers strictement positifs $n = k_1 + \dots + k_r$.

Par exemple, la classe de conjugaison $\{\mathrm{id}\}$ de l'identité est associée à la partition $n = 1 + 1 + \dots + 1$, et à la partition $n = n$ correspond la classe de conjugaison du n-cycle $c = (1\ 2\ \cdots\ n)$. Pour $n = 3$, il y a ainsi 3 classes de conjugaison : $\{\mathrm{id}\}$, $\{(1\ 2\ 3),\ (1\ 3\ 2)\}$ et $\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$. Pour $n = 4$, on dénombre cinq partitions $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$, qui correspondent dans le même ordre à la classe des 4-cycles, la classe des 3-cycles, la classe des doubles transpositions, la classe des transpositions, et enfin $\{\mathrm{id}\}$.

Proposition 1.23
Le sous-groupe dérivé $D(\mathfrak{S}_n) = \mathcal{A}_n$.

Preuve. Comme $\varepsilon([\sigma, \tau]) = 1$ pour tout commutateur, et ε étant un morphisme, l'inclusion $\subset$ est directe. Pour l'autre inclusion, on montre que tout 3-cycle est un commutateur et que $\mathcal{A}_n$ est engendré par les 3-cycles.

Soit $(a\ b\ c)$ un 3-cycle. Alors, de $(a\ b)(b\ c)(a\ b) = (a\ c)$, on tire $(a\ b)(b\ c)(a\ b)(b\ c) = (a\ c)(b\ c) = (a\ c\ b)$. Cette formule montre que tout 3-cycle est un commutateur de transpositions.

Pour voir que $\mathcal{A}_n$ est engendré par les 3-cycles, on revient à la décomposition en produit de transpositions. Par définition, toute $\sigma \in \mathcal{A}_n$ est un produit pair de transpositions : $\sigma = \tau_1 \cdots \tau_{2p}$. On écrit $\tau_k = (a_k\ b_k)$ et pour tout $1 \leqslant i \leqslant p$, considérons le produit $\tau_{2i-1}\tau_{2i}$ qu'on suppose $\neq \mathrm{id}$. On a alors deux cas :

1. Les supports de τ_{2i-1} et τ_{2i} ont exactement un point en commun. Alors, la formule précédente nous montre que leur produit est un 3-cycle.
2. Les supports de τ_{2i-1} et τ_{2i} sont disjoints. Alors on force la jonction de leurs supports en introduisant une transposition sur le schéma suivant :

$$(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d)$$

montrant que le produit $\tau_{2i-1}\tau_{2i}$ est égal au produit de deux 3-cycles.

Ainsi, en regroupant les transpositions par paires, on observe que σ s'écrit comme un produit de 3-cycles. □

Mettons bien en avant ce que la preuve a montré :

Proposition 1.24
Le groupe $\mathcal{A}_n$ est engendré par les 3-cycles.

On retiendra également la règle de calcul : $(a\ b)(b\ c) = (a\ b\ c)$, quand a, b, c sont deux à deux distincts. Dans quelle mesure se généralise-t-elle ?

Exercice 1.20
Utiliser cette règle pour retrouver le fait que $\mathfrak{S}_n$ est engendré par les transpositions.

Exercice 1.21
Montrer que $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1\ 2\ k)$, où $3 \leqslant k \leqslant n$.

Citons pour finir deux résultats qui font l'objet de développements classiques.

Théorème 1.6
Si $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.

Comme on a vu en exercice que le centre $\mathfrak{S}_n$ est trivial dès que $n > 2$, on obtient que $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$ pour $n \geqslant 3$, $n \neq 6$.

Théorème 1.7
Pour $n \geqslant 5$, le groupe alterné $\mathcal{A}_n$ est simple : ses seuls sous-groupes distingués sont $\{\mathrm{id}\}$ et lui-même.

On vérifie facilement que la seule valeur pour laquelle ce groupe n'est pas simple est $n = 4$, le sous-groupe distingué incriminé étant le groupe des doubles transpositions. On notera qu'elles forment bien un sous-groupe dans le cas $n = 4$ seulement.

1.5 Actions de groupes

On passe à présent à la notion omniprésente dans ce cours, les opérations de groupes sur des ensembles. C'est ce qui fait la jonction entre algèbre et géométrie. Dans ce qui suit, sauf mention explicite du contraire, on note X un ensemble et G un groupe.

Définition 1.27

Une action de G sur X est la donnée d'une application $G \times X \to X$, $(g, x) \mapsto g.x$, telle que

1. pour tout $x \in X$, $e.x = x$;
2. pour tout $x \in X$ et tous $g, h \in G$, $g.(h.x) = (gh).x$.

De façon équivalente, cela revient à se donner un morphisme de groupes $\varphi : G \mapsto \mathfrak{S}_X$. En effet, si on s'est donné un tel morphisme, alors on lui fait correspondre l'action $(g, x) \mapsto \varphi(g)[x]$ (vérifier que c'est bien une action), et inversement, si $(g, x) \mapsto g.x$ est une action, alors en notant pour tout $g \in G$ $\varphi(g)$ on définit $\varphi(g) : X \to X$, $\varphi(g)[x] := g.x$, et ces applications vérifient $\varphi(gh) = \varphi(g)\varphi(h)$ pour tous g et h et $\varphi(e) = \mathrm{id}_X$, montrant directement que $\varphi(g)$ est bijective d'inverse $\varphi(g^{-1})$.

Définition 1.28

Une action de G sur X est dite **fidèle** si le morphisme φ défini ci-dessus est injectif, c'est à dire si pour tout $g \in G$, on a

$$(\forall x \in X,\ g.x = x) \Rightarrow g = e.$$

Encore plus spécifiquement, une action est dite **libre** si

$$\forall x \in X,\ \forall g \in G,\ g.x = x \Rightarrow g = e.$$

Enfin, on dit que l'action est **transitive** si

$$\forall x, y \in X,\ \exists g \in G \mid y = g.x.$$

Exemple 1.11. Les premiers exemples sont les actions de G sur lui-même, *i.e.* le cas $X = G$.

1. L'action par translation à gauche : $g.x = gx$ pour tous $g \in G$ et $x \in X = G$. Elle est libre et transitive.
2. L'action par translation à droite : $g.x = xg^{-1}$ pour tous $g \in G$ et $x \in X = G$. De même, cette action est libre et transitive. **Attention**, si on omet de prendre l'inverse, on obtient une action dite "à droite", c'est à dire vérifiant $g.(h.x) = (hg).x$.
3. L'action par conjugaison : $g.x = gxg^{-1}$ pour tous $g \in G$ et $x \in X = G$. Elle n'est jamais libre : $x = e$ est fixé par tous les éléments de G.

Exercice 1.22

Toujours dans l'exemple précédent, exhiber une bijection $\psi : X \to X$ qui *conjugue* la première action à la deuxième, c'est-à-dire telle que pour tout $g \in G$, on a $\psi^{-1} \circ \varphi_2(g) \circ \psi = \varphi_1(g)$

Exemple 1.12. Dans les premiers exemples, on retrouve également l'action du groupe symétrique $G = \mathfrak{S}_n$ sur $X = \{1 \dots n\}$, donnée par $\sigma.k = \sigma(k)$ pour toute permutation σ et tout $k \in X$. Cette action est transitive (pourquoi ?), fidèle, mais non libre.

Plus généralement, si X est un ensemble, le groupe des bijections Bij_X agit naturellement sur X.

Remarque 1.19. Étant donnée une action de G sur un ensemble X, et $H < G$ un sous-groupe, on peut toujours considérer l'**action restreinte** à H. En interprétant l'action de G comme un morphisme $\phi : G \to \mathrm{Bij}_X$, l'action restreinte à H est simplement la restriction $\phi|_H$.

Théorème 1.8 (Cayley)

Tout groupe G est isomorphe à un sous-groupe du groupe des bijections Bij_X d'un certain ensemble X.

Dit autrement, pour tout groupe G, il existe (au moins) un ensemble X et un morphisme injectif $f : G \to \mathrm{Bij}_X$, et G s'identifie alors au groupe image $f(G)$. Le théorème de Cayley signifie donc que tout groupe agit fidèlement sur un certain ensemble X. La preuve est donc très rapide.

Preuve. L'action de G sur $X = G$ par translation à gauche est une action libre, puisque $gx = x$ implique $g = e$ pour tous $g, x \in G$. Elle est donc fidèle. □

Même si sa preuve est d'un intérêt assez modéré, le théorème en soi confirme l'idée que tout groupe peut être pensé comme un groupe de transformations d'un certain ensemble. Au moins un ensemble.

À ce stade, tous les groupes que nous avons considérés ont été introduits comme des sous groupes d'un groupe de permutations d'un ensemble fini ou infini (le groupe linéaire $\mathrm{GL}(V)$ d'un espace vectoriel est bien un sous-groupe du groupe des bijections ensemblistes de V !).

Saisissons l'occasion pour définir un groupe célèbre abstraitement.

Définition 1.29

Le groupe $\mathbf{H}_8$ est le groupe formé des éléments $\{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$, où on déclare que 1 et -1 sont centraux (i.e. $\mathcal{Z}(\mathbf{H}_8) = \{\pm 1\}$), et tel que $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -ij$, $kj = -jk$ et $ik = -ki$, et enfin la multiplication par -1 fait ce qu'on attend.

Puisqu'il y a un petit nombre d'éléments, on peut dresser la "table de multiplication" dans ce groupe :

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Il y a un sous-entendu dans cette définition : cette loi est bien une loi de groupe. L'existence d'un neutre, et d'un inverse est claire. On peut vérifier un peu fastidieusement l'associativité en distinguant les cas. Le plus efficace est d'observer qu'il existe des

matrices de $\mathrm{GL}_2(\mathbf{C})$ qui vérifient exactement les relations de $\mathbf{H}_8$. L'associativité de cette loi découle alors de celle du produit matriciel.

Il suffit de prendre les matrices suivantes :

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ M_i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ M_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ M_k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

ainsi que les matrices opposées pour les éléments "opposés" $-1, -i, -j, -k$. On vérifie rapidement qu'elles vérifient les relations ci-dessus. On fait alors d'une pierre plusieurs coups : ceci assure que la loi de $\mathbf{H}_8$ est associative, montre un exemple de représentation linéaire fidèle de ce groupe fini (Exemple 5.1), et donc le réalise comme un sous-groupe de permutations d'un ensemble (ici l'espace vectoriel $\mathbf{C}^2$). Cette réalisation comme un groupe de permutations n'est pas celle fournie par le théorème de Cayley, mais elle est très naturelle comme on le verra plus loin en étudiant les quaternions plus en détails (Section 4.5.4).

Définition 1.30

Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, on appelle **stabilisateur de** x le sous-groupe $\mathrm{Stab}_G(x) = G_x = \{g \in G \ :\ g.x = x\}$. On appelle **orbite de** x, et on note $G.x$ ou encore $\mathcal{O}(x)$, l'ensemble $G.x = \{g.x,\ g \in G\}$.

Étant donné une action de G sur X, on introduit une relation d'équivalence sur X définie par

$$\forall x, y \in X,\ x \sim y \iff \exists g \in G \mid y = g.x.$$

On vérifie facilement que c'est une relation d'équivalence, et que la classe d'équivalence d'un élément $x \in X$ coïncide avec son orbite. Comme les classes d'équivalences définissent une partition de X, on en déduit l'existence d'une famille de représentants $(x_\alpha)_{\alpha \in \mathcal{A}}$ tels que X s'écrit comme la réunion disjointe des orbites des x_α

$$X = \bigsqcup_{\alpha \in \mathcal{A}} \mathcal{O}(x_\alpha).$$

Exemple 1.13. Reprenons l'action naturelle de $\mathfrak{S}_n$ sur $X = \{1 \dots n\}$. Soit $\sigma \in \mathfrak{S}_n$ et $H = \langle \sigma \rangle$ le sous-groupe qu'elle engendre. On peut considérer la restriction à H de l'action de $\mathfrak{S}_n$ sur X. Alors les orbites de H de cardinal 1 sont les points fixes de σ et celles de cardinal $\geqslant 2$ sont les supports des cycles qui apparaissent dans la décomposition de σ en produit de cycles à supports disjoints.

Pour tout $x \in X$, on introduit l'**application orbitale en** x

$$\begin{array}{rccc} \varphi_x : & G & \longrightarrow & \mathcal{O}(x) \\ & g & \mapsto & g.x \end{array}$$

Par définition, φ_x est surjective.

Proposition 1.25

Pour tout $x \in X$, l'application orbitale induit une bijection

$$\overline{\varphi_x} : G/G_x \to \mathcal{O}(x)$$

telle que $\varphi_x = \overline{\varphi_x} \circ \pi_x$, où $\pi_x : G \to G/G_x$ désigne la projection canonique.

Remarque 1.20. **Attention** : Le stabilisateur G_x n'est en général pas un sous-groupe distingué de G, et l'orbite de x n'est pas un groupe non plus. Il s'agit d'une identification purement ensembliste à ce degré de généralité. Elle sera néanmoins fort utile dans le cas des groupes finis pour faire du dénombrement.

Exercice 1.23
Retrouver le théorème de Lagrange en utilisant la partition de X en orbites pour une action de groupe bien choisi.

Exercice 1.24
On considère l'action linéaire naturelle de $\mathrm{GL}_n(\mathbf{R})$ sur $\mathbf{R}^n$. Quelles sont les orbites ? De même pour les actions de $\mathrm{SL}_n(\mathbf{R})$ et $O_n(\mathbf{R})$.

Proposition 1.26
Si G agit sur X et si deux points x et y sont dans la même orbite, alors leurs stabilisateurs sont conjugués. Précisément :

$$\text{Si } y = g.x,\ g \in G, \text{ alors } G_y = gG_xg^{-1}.$$

Définition 1.31
Soit G un groupe et soit X un ensemble sur lequel G agit. On appelle **invariant** pour cette l'action de G toute application $f : X \to Y$, Y étant un autre ensemble, qui est constante sur les orbites de G.

On appelle **invariant total** un invariant $f : X \to Y$ tel qu'en plus, pour tous $x, y \in X$, si $G.x \neq G.y$, alors $f(x) \neq f(y)$.

On notera que $f : X \to Y$ est un

- invariant si $\forall (g, x) \in G \times X,\ f(g.x) = f(x)$.
- invariant total si $\forall x, y \in X, \mathcal{O}(x) = \mathcal{O}(y) \iff f(x) = f(y)$.

Exercice 1.25
En appliquant la proposition 1.9, montrer qu'un invariant induit une application sur *l'espace des orbites* de G sur X, c'est à dire l'ensemble des orbites de tous les éléments de X. Vérifier ensuite que cette application est injective si et seulement si l'invariant est total.

Remarque 1.21. Même s'il n'est pas total, un invariant donne toujours des obstructions pour que deux éléments soient dans la même orbite : si $f(x) \neq f(y)$, alors x et y ont deux orbites différentes.

Exemple 1.14. Soit $G = \mathfrak{S}_n$ et $X = G$ et considérons l'action de G sur X par conjugaison. Alors la fonction $f : X \to [\![1, n]\!]$ définie par $f(\sigma) = \sharp\,\mathrm{Supp}(\sigma)$ est un invariant de l'action, mais pas total. Par exemple, une double transposition a pour image 4, mais un 4-cycle aussi.

Exercice 1.26
Soit $X = \mathcal{S}_n^+(\mathbf{R}) \subset \mathcal{M}_n(\mathbf{R})$ l'ensemble des matrices symétriques définies positives. Soit $G = \mathrm{GL}_n(\mathbf{R})$. On considère l'action par congruence de G sur X : $(g, M) \in G \times X \mapsto gX\,{}^tg \in X$.

1. Justifier que cette action est bien définie.
2. Montrer qu'elle est transitive.
3. Donner le stabilisateur d'un point quelconque.

Définition 1.32

Étant donnée une action de G sur X, on peut toujours considérer l'**action diagonale** de G sur $X^k = X \times X \times \cdots \times X$ (k fois) donnée par

$$g.(x_1, \ldots, x_k) = (g.x_1, \ldots, g.x_k).$$

Notons $\Delta_k \subset X^k$ le sous-ensemble $\Delta_k = \{(x_1, \ldots, x_k) \in X^k \ : \ i \neq j \Rightarrow x_i \neq x_j\}$.

Définition 1.33

Une action de G sur X est dite k-transitive si Δ_k est une G-orbite dans X^k.

Exemple 1.15. On a vu que pour tout k compris entre 1 et n, l'action de $\mathfrak{S}_n$ sur $X = \{1, \ldots, n\}$ est k-transitive.

Exercice 1.27 (Action 3-transitive sur $P^1(K)$)

On reprend les notations et définitions de l'Exercice 1.9. Si $v \in K^{n+1} \setminus \{0\}$, on note $[v] \in P^n(K)$ son image par la projection canonique.

1. Définir une action naturelle de $\mathrm{GL}_{n+1}(K)$ sur $P^n(K)$.
2. Est-elle fidèle ? Quel est son noyau ?
3. Montrer qu'elle est transitive.
4. Montrer que l'action de $\mathrm{GL}_2(K)$ sur sur la droite projective $P^1(K)$ est *simplement 3-transitive*, c'est-à-dire qu'étant donnés deux triplets $([v_1], [v_2], [v_3])$, $([w_1], [w_2], [w_3]) \in (P^1(K))^3$ formés d'éléments deux à deux distincts, alors il existe $g \in \mathrm{GL}_2(K)$ tel que $g.[v_1] = [w_1]$, $g.[v_2] = [w_2]$ et $g[v_3] = [w_3]$, et que de plus, un autre élément g' vérifiant ces conditions est de la forme $g' = \lambda g$, avec $\lambda \in K^*$.

Soit G un groupe fini agissant sur un ensemble fini X. On note $X^G = \{x \in X \mid \forall g \in G, \ g.x = x\}$ l'ensemble des points fixes de G. Pour $x \in X$, on note G_x le stabilisateur de x dans G.

Proposition 1.27 (Équation aux classes)

Il existe une partie $\mathcal{R}' \subset X \setminus X^G$ telle que

$$\sharp X = \sharp X^G + \sum_{x \in \mathcal{R}'} |G|/|G_x|.$$

Noter que pour tout $x \in X \setminus X^G$, $G_x \neq G$.

Preuve. Il s'agit simplement de la traduction du fait que X est partitionné en G-orbites. On met d'un coté les orbites de cardinal 1 *i.e.* les éléments de X^G, puis on choisit un représentant pour chaque orbite dans $X \setminus X^G$ et on utilise le fait général que toute orbite $G.x$ est en bijection avec le quotient G/G_x. [Dessin] □

Exercice 1.28 (Centre d'un p-groupe)
Soit G un groupe fini d'ordre p^n, où p est un nombre premier et $n \geqslant 1$. Montrer que $\mathcal{Z}(G) \neq \{e\}$.

Proposition 1.28 (Formule de Burnside)
Soit Ω l'ensemble des G-orbites de l'action de G sur X. Alors

$$\sharp\Omega = \frac{1}{|G|} \sum_{x \in G} \sharp \mathrm{Fix}(g)$$

où pour tout $g \in G$, $\mathrm{Fix}(g) = \{x \in X \mid g.x = x\}$.

Preuve. Cf. TD 3. □

1.6 Groupe des isométries de l'espace euclidien, groupe affine

On munit l'espace $\mathbf{R}^n$ du produit scalaire euclidien standard, dont on note $\|.\|$ la norme associée.On note $d(x, y) = \|x - y\|$ la distance associée.

Définition 1.34
On appellle **isométrie** de $\mathbf{R}^n$ une application $f : \mathbf{R}^n \to \mathbf{R}^n$ telle que

$$\forall x, y \in \mathbf{R}^n,\ d(f(x), f(y)) = d(x, y).$$

Pour tout $v \in \mathbf{R}^n$, on note τ_v la translation de vecteur v, c'est à dire l'application $\tau_v : \mathbf{R}^n \to \mathbf{R}^n$ définie par $\tau_v(x) = x + v$ pour tout $x \in \mathbf{R}^n$. On observe alors :

1. Toute translation est une isométrie.
2. Tout matrice orthogonale $A \in O_n(\mathbf{R})$ est une isométrie fixant l'origine.
3. La composée de deux isométries est une isométrie.

Ce faisant, on vient de décrire toutes les isométries par la proposition suivante.

Proposition 1.29
Les isométries de $\mathbf{R}^n$ forment un groupe, noté $\mathrm{Isom}(\mathbf{R}^n)$, et toute isométrie $f \in \mathrm{Isom}(\mathbf{R}^n)$ s'écrit de façon unique comme la composée d'une translation et d'une matrice orthogonale : $f = \tau_v \circ A$, pour $v \in \mathbf{R}^n$ et $A \in O_n(\mathbf{R})$.

On notera bien qu'il n'y a aucune hypothèse sur f autre que de préserver la distance euclidienne, il n'est pas clair *a priori* que f est bijective par exemple. La conclusion de cette proposition est donc que f se définit de manière unique sous la forme $f(x) = Ax+v$, avec A orthogonale et $v = f(0)$.

Preuve. Soit $v = f(0) \in \mathbf{R}^n$. Alors $\tau_v^{-1} \circ f(0) = f(0) - v = 0$. Appelons $g = \tau_v^{-1} \circ f$. D'après les observations faites précédemment, g est une isométrie, et $g(0) = 0$. En particulier, nous avons pour tout $x \in \mathbf{R}^n$, $\|g(x)\| = \|x\|$. On va montrer que g préserve le produit scalaire $\langle ., . \rangle$ dont dérive la norme.

Rappelons la formule de polarisation $\langle u, v \rangle = \frac{1}{2}(\|u + v\|^2 - \|u\|^2 - \|v\|^2)$. Nous avons alors pour tous $u, v \in \mathbf{R}^n$

$$\begin{aligned}\langle g(u), g(v) \rangle &= -\frac{1}{2}(\|g(u) - g(v)\|^2 - \|g(u)\|^2 - \|g(v)\|^2) \\ &= -\frac{1}{2}(\|u - v\|^2 - \|u\|^2 - \|v\|^2) = \langle u, v \rangle,\end{aligned}$$

puisque $d(g(u), g(v)) = d(u, v)$. Ainsi, g préserve le produit scalaire. On montre qu'elle est linéaire par le calcul suivant :

$$\begin{aligned}\|g(x+y) - g(x) - g(y)\|^2 &= \|g(x+y)\|^2 + \|g(x)\|^2 + \|g(y)\|^2 - 2\langle g(x+y), g(x)\rangle \\ &\quad - 2\langle g(x+y), g(y)\rangle - 2\langle g(x), g(y)\rangle \\ &= \|x+y\|^2 + \|x\|^2 + \|y\|^2 - 2\langle x+y, x\rangle \\ &\quad - 2\langle x+y, y\rangle - 2\langle x, y\rangle \\ &= \|(x+y) - x - y\|^2 = 0.\end{aligned}$$

Ainsi, $g(x+y) = g(x) + g(y)$ pour tous $x, y \in \mathbf{R}^n$. On vérifie par la même méthode que $g(\lambda x) = \lambda g(x)$ pour tout $\lambda \in \mathbf{R}$ et $x \in \mathbf{R}^n$.

Ainsi, $g \in \mathcal{L}(\mathbf{R}^n)$ et elle préserve le produit scalaire euclidien standard : $g \in O_n(\mathbf{R})$. Puisque $g = \tau_v^{-1} \circ f$, on en déduit $f = \tau_v \circ g$ et on obtient l'existence de la décomposition annoncée. En particulier, ceci montre que tout isométrie est bijective, puisque les translations et les matrices orthogonales le sont.

Pour l'unicité, si $f = \tau_v \circ g$ est une telle décomposition, on l'évalue en 0 pour obtenir $v = f(0)$ qui est donc uniquement déterminé. On a alors nécessairement $g = \tau_v^{-1} \circ f$ qui est aussi uniquement déterminé.

Vérifions enfin que $\mathrm{Isom}(\mathbf{R}^n)$ est un sous-groupe de $\mathrm{Bij}(\mathbf{R}^n)$. Il est non-vide puisqu'il contient l'identité. On a déjà vu qu'il est stable par composition. Enfin pour toute $f \in \mathrm{Isom}(\mathbf{R}^n)$, on a

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

montrant que l'inverse (qui existe) de f est également une isométrie. □

Insistons lourdement : $\mathrm{Isom}(\mathbf{R}^n)$ n'est **pas** un sous-groupe du groupe linéaire de $\mathbf{R}^n$: les translations ne sont pas des applications linéaires. C'est en revanche un sous-groupe du *groupe affine* de $\mathbf{R}^n$. Rappelons sa définition (qui n'est pas la plus intrinsèque, mais convient pour ce qui nous intéresse) :

Définition 1.35

On appelle **application affine** de $\mathbf{R}^n$ toute fonction $f : \mathbf{R}^n \to \mathbf{R}^n$ de la forme $f(x) = Ax + v$, où $A \in \mathrm{GL}_n(\mathbf{R})$ et $v \in \mathbf{R}^n$, c'est-à-dire de la forme $f = \tau_v \circ A$.

Proposition 1.30

Si f est une application affine de $\mathbf{R}^n$, alors l'écriture $f = \tau_v \circ A$ est unique. L'ensemble des applications affines de $\mathbf{R}^n$ forme un groupe pour la composition. Si on identifie une application au couple $(A, v) \in \mathrm{GL}_n(\mathbf{R}) \times \mathbf{R}^n$ qui la définit, alors la loi de composition se traduit par la règle :

$$(A_1, v_1) \star (A_2, v_2) = (A_1 A_2, v_1 + A_1 v_2).$$

On va utiliser l'observation suivante.

Lemme 1.3

Pour tout $v \in \mathbf{R}^n$, et tout $A \in \mathrm{GL}_n(\mathbf{R})$, on a

$$A \circ \tau_v \circ A^{-1} = \tau_{Av}.$$

Preuve. Pour tout $x \in \mathbf{R}^n$, nous avons

$$A \circ \tau_v \circ A^{-1}(v) = A(A^{-1}x + v) = x + Av = \tau_{Av}(x),$$

ce qui conclut. □

Comme dans le cas des isométries, si une transformation se met sous la forme $f = \tau_v \circ A$, alors nécessairement $v = f(0)$ et $A = \tau_{-v} \circ f$, qui sont donc bien uniquement déterminés. On peut donc parler de *la* composante translation τ_v et de *la* composante linéaire A de f [1]. Vérifions que l'ensemble des applications affines forme un sous-groupe de $\mathrm{Bij}_{\mathbf{R}^n}$. Il est non vide car il contient l'identité. Si on se donne deux applications affines f_1, f_2, s'écrivant $f_i = \tau_{v_i} A_i$, $i \in \{1, 2\}$, alors on a

$$\begin{aligned} f_1 \circ f_2 = \tau_{v_1} A_1 \tau_{v_2} A_2 &= \tau_{v_1}(A_1 \tau_{v_2} A_1^{-1}) A_1 A_2 \\ &= \tau_{v_1} \tau_{A_1 v_2} A_1 A_2 \\ &= \tau_{v_1 + A_1 v_2}(A_1 A_2) \end{aligned}$$

d'après le lemme. Ceci montre bien que la composée des deux est une application affine d'éléments caractéristiques $A_1 A_2$ et $v_1 + A_1 v_2$. On peut également vérifier cela directement en écrivant :

$$\forall x \in \mathbf{R}^n,\ f_1 \circ f_2(x) = A_1(A_2 x + v_2) + v_1 = A_1 A_2 x + (v_1 + A_1 v_2).$$

Pour la stabilité par passage à l'inverse, on utilise la même ruse :

$$(\tau_v \circ A)^{-1} = A^{-1} \circ \tau_{-v} = (A^{-1} \tau_{-v} A) A^{-1} = \tau_{-A^{-1}v} A^{-1},$$

d'après le lemme. L'inverse s'écrit bien comme la composée d'une translation et d'une application linéaire inversible (dans le bon ordre). Au passage, on observe que le passage à l'inverse se traduit par la transformation de (A, v) en $(A^{-1}, -A^{-1}v)$.

Proposition 1.31

L'ensemble des translations $N = \{\tau_v,\ v \in \mathbf{R}^n\}$ est un sous-groupe distingué de $\mathrm{Aff}(\mathbf{R}^n)$, et isomorphe à $\mathbf{R}^n$. *A contrario*, le sous-groupe $\mathrm{GL}_n(\mathbf{R}) < \mathrm{Aff}(\mathbf{R}^n)$ n'est pas distingué, et se caractérise par

$$\mathrm{GL}_n(\mathbf{R}) = \{f \in \mathrm{Aff}(\mathbf{R}^n) \mid f(0) = 0\},$$

en d'autres termes, c'est le stabilisateur de 0 pour l'action naturelle sur $\mathbf{R}^n$. Enfin, on a

$$\mathrm{Aff}(\mathbf{R}^n) = N.\,\mathrm{GL}_n(\mathbf{R}) \text{ et } N \cap \mathrm{GL}_n(\mathbf{R}) = \{\mathrm{id}\}$$

la première identité signifiant que toute transformation affine est produit d'un élément de N et d'un élément de $\mathrm{GL}_n(\mathbf{R})$, la deuxième impliquant que cette écriture est unique. Enfin, si $g_1 = \tau_{v_1} A_1$ et $g_2 = \tau_{v_2} A_2$, alors leur composée s'écrit

$$g_1 g_2 = \tau_{v_1} A_1 \tau_{v_2} A_2 = \tau_{v_1}(A_1 \tau_{v_2} A_1^{-1}) A_1 A_2 = \tau_{v_1 + A_1 v_2} A_1 A_2.$$

1. Encore une fois, ce point de vue n'est pas le bon pour considérer les applications affines, on pourra se référer notamment au chapitre 1 de [Aud06] pour une construction plus profonde de la géométrie affine et des transformations affines

Exercice 1.29

Vérifier que $\bigcap_{g \in \mathrm{Aff}(\mathbf{R}^n)} g\,\mathrm{GL}_n(\mathbf{R})g^{-1} = \{\mathrm{id}\}$.

1.7 Groupe diédral

On identifie $\mathbf{R}^2 \simeq \mathbf{C}$ de la façon usuelle. Rappelons la définition des similitudes.

Définition 1.36

On appelle **similitude directe** du plan complexe toute application $f : \mathbf{C} \to \mathbf{C}$ de la forme $f(z) = az + b$, où $a, b \in \mathbf{C}$, $a \neq 0$. On appelle **similitude indirecte** toute application $g : \mathbf{C} \to \mathbf{C}$ de la forme $g(z) = a\overline{z} + b$, où $a, b \in \mathbf{C}$, $a \neq 0$.

Les similitudes (directes et indirectes) forment un groupe pour la composition, qu'on note $\mathrm{Sim}(\mathbf{R}^2)$.

Via l'identification standard avec $\mathbf{R}^2$, en écrivant $a = \rho e^{i\theta}$ sous forme polaire, et $b = b_1 + ib_2$, une similitude directe $f(z) = az + b$ correspond à l'application affine

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \rho \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

et une similitude indirecte $g(z) = a\overline{z} + b$ à l'application affine

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \rho \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

Ainsi, $\mathrm{Sim}(\mathbf{R}^2)$ est un sous-groupe du groupe affine $\mathrm{Aff}(\mathbf{R}^2)$, et les isométries sont les similitudes pour lesquelles le nombre complexe a est de module $\rho = 1$.

Proposition 1.32

Le groupe des isométries de $\mathbf{R}^2$ est distingué dans le groupe des similitudes :

$$\mathrm{Isom}(\mathbf{R}^2) \triangleleft \mathrm{Sim}(\mathbf{R}^2).$$

Preuve. Notons $h_\rho \in \mathrm{Sim}(\mathbf{R}^2)$ l'homothétie de rapport $\rho > 0$: $h_\rho(v) = \rho v$ pour tout $v \in \mathbf{R}^2$. Alors, toute similitude f se met sous la forme $f = h_\rho \circ g$, où $g \in \mathrm{Isom}(\mathbf{R}^2)$. Maintenant si φ est une isométrie de $\mathbf{R}^2$, alors $f \circ \varphi \circ f^{-1} = h_\rho(g\varphi g^{-1})h_\rho^{-1}$ et $g\varphi g^{-1} \in \mathrm{Isom}(\mathbf{R}^2)$. Il s'agit donc de voir pourquoi une isométrie conjuguée par une homothétie reste une isométrie. Le calcul est immédiat :

$$h_\rho \varphi h_\rho^{-1}(z) = \rho(a\rho^{-1}z + b) = az + \rho b.$$

Le coefficient a étant inchangé, le résultat est bien une isométrie. □

Lemme 1.4

Si P et P' sont deux polygones réguliers à n cotés dans $\mathbf{R}^2$, alors il existe une similitude $\varphi \in \mathrm{Sim}(\mathbf{R}^2)$ telle que $P' = \varphi(P)$.

Soient P_1 et P_2 deux polygones réguliers à n cotés. On considère $G_i = \{\varphi \in \mathrm{Isom}(\mathbf{R}^2) : \varphi(P_i) = P_i\}$ pour $i = 1, 2$. Soit $\psi \in \mathrm{Sim}(\mathbf{R}^2)$ telle que $P_2 = \psi(P_1)$. Alors

$$G_2 = \psi G_1 \psi^{-1} \text{ dans } \mathrm{Sim}(\mathbf{R}^2).$$

(le vérifier en exercice). Notamment, G_1 et G_2 sont isomorphes. On peut alors définir *le* groupe diédral d'ordre $2n$.

Exercice 1.30
Où utilise-t-on que ψ est une similitude ?

Définition 1.37
Soit $n \geqslant 1$. Le groupe diédral d'ordre $2n$ est le groupe abstrait D_n tel que pour tout polygone régulier à n cotés P, on a

$$D_n \simeq \{\phi \in \mathrm{Isom}(\mathbf{R}^2) \ : \ \phi(P) = P\}.$$

Remarque 1.22. Si P et P' sont deux polygones réguliers distincts, en général les groupes d'isométries les préservant sont distincts. Néanmoins, ils sont toujours isomorphes car conjugués dans $\mathrm{Sim}(\mathbf{R}^2)$. La structure de groupe est donc la même, et c'est elle qui nous intéresse.

Concrètement, on peut comprendre D_n en se donnant un polygone qui nous arrange le plus et en classant ses isométries. Prenons celui dont les sommets sont les racines n-ème de l'unité dans $\mathbf{C}$, listées dans l'ordre $(S_0, \dots, S_{n-1})$, où $S_k = e^{\frac{2ik\pi}{n}}$, pour $k = 0, \dots, n-1$. Appelons-le P_0. Notons $\theta_k = \frac{2k\pi}{n}$ pour $0 \leqslant k \leqslant n-1$.

Une isométrie de P_0 est donc une isométrie φ du plan $\mathbf{C}$ qui préserve l'ensemble de ses sommets. Comme $\sum_{0 \leqslant k \leqslant n-1} e^{\frac{2ik\pi}{n}} = 0$, l'isobarycentre des sommets de P_0 est l'origine $0 \in \mathbf{C}$. Les applications affines préservant les barycentres, on en déduit que $\varphi(0) = 0$, et φ est donc **linéaire** : $\varphi \in O_2(\mathbf{R})$. Ainsi, il existe $a \in \mathbb{U} = \{z \in \mathbf{C} \ : \ |z| = 1\}$ tel que $\varphi(z) = az$ (rotation) ou $\varphi(z) = a\overline{z}$ (réflexion).

Notons que la réflexion $s_0 : z \mapsto \overline{z}$ préserve P_0 : précisément, elle fixe S_0 et envoie S_k sur S_{n-k} pour $1 \leqslant k \leqslant n-1$.

On peut alors décrire explicitement φ :

— Ou bien φ est directe, c'est une rotation $\varphi(z) = az$, et $a = \varphi(1) = \varphi(S_0) = S_k$ pour un certain $k \in \{0, \dots, n-1\}$, c'est à dire $a = e^{i\theta_k}$ et φ est la rotation d'angle θ_k. Inversement, toute telle rotation préserve P_0.

— Ou bien φ est indirecte, et alors $\varphi \circ s_0$ est directe, donc de la forme $z \mapsto e^{i\theta_k} z$. On en déduit $\varphi(z) = e^{i\theta_k}\overline{z}$. C'est la réflexion orthogonale par rapport à la droite dirigée par $e^{i\theta_k/2}$. Inversement, toute telle réflexion préserve P_0.

En définitive, le groupe diédral D_n est isomorphe au sous-groupe d'ordre $2n$ de $O_2(\mathbf{R})$ suivant :

$$\underbrace{\left\{\begin{pmatrix}\cos(\theta_k) & -\sin(\theta_k)\\ \sin(\theta_k) & \cos(\theta_k)\end{pmatrix}, \ 0 \leqslant k \leqslant n-1\right\}}_{\subset \mathrm{SO}_2(\mathbf{R})} \sqcup \underbrace{\left\{\begin{pmatrix}\cos(\theta_k) & \sin(\theta_k)\\ \sin(\theta_k) & -\cos(\theta_k)\end{pmatrix}, \ 0 \leqslant k \leqslant n-1\right\}}_{\subset O_2(\mathbf{R}) \setminus \mathrm{SO}_2(\mathbf{R})}.$$

Notons

$$R_n = \left\{\begin{pmatrix}\cos(\theta_k) & -\sin(\theta_k)\\ \sin(\theta_k) & \cos(\theta_k)\end{pmatrix}, \ 0 \leqslant k \leqslant n-1\right\} \simeq \mathbf{Z}/n\mathbf{Z}.$$

C'est le sous-groupe (cyclique) des rotations préservant P_0. Si on note $s = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ la matrice de la réflexion associé à $z \mapsto \overline{z}$, alors le sous-groupe des isométries préservant P_0 s'écrit $R_n \sqcup R_n s$. En fait $R_n s = s R_n$ et R_n est distingué dans le sous-groupe des isométries préservant P_0. Ceci pouvait se déduire directement du fait qu'il est d'indice 2 (cf exercices). Notons r la matrice de rotation d'angle θ_1, de sorte que r est d'ordre n et $R_n = \langle r \rangle$. On vérifie qu'on a alors $srs = r^{-1}$, la rotation d'angle $-\theta_1$.

Proposition 1.33

Identifions D_n au sous-groupe de $\mathrm{Isom}(\mathbf{R}^2)$ préservant P_0. Alors en notant r et s la rotation et la symétrie définies ci-dessus, tout élément $g \in D_n$ s'écrit de façon unique

$$g = r^k s^i, \text{ où } i \in \{0,1\} \text{ et } k \in \{0,\dots,n-1\}.$$

Dit autrement, si $R_n = \langle r \rangle \simeq \mathbf{Z}/n\mathbf{Z}$ et $S = \langle s \rangle \simeq \mathbf{Z}/2\mathbf{Z}$, alors tout élément de D_n s'écrit de façon unique comme produit d'un élément de R et d'un élément de S. De plus, $R \triangleleft D_n$. Enfin, si $g_1 = r^{k_1}s^{i_1}$ et $g_2 = r^{k_2}s^{i_2}$, alors

$$g_1 g_2 = r^{k_1}s^{i_1}r^{k_2}s^{i_2} = r^{k1}(s^{i_1}r^{k_2}s^{i_1})s^{i_1}s^{i_2} = r^{k_1+\varepsilon(i_1)k_2}s^{i_1+i_2}$$

où $\varepsilon(i_1) = 1 - 2i_1$ vaut 1 si $i_1 = 0$ et -1 si $i_1 = 1$.

Remarque 1.23. Toute ressemblance avec des structures de groupes existantes rencontrées précédemment serait purement fortuite.

Si l'ironie de cette remarque n'était pas déjà apparue clairement, ce qui suit devrait parachever le travail.

1.8 Produit semi-direct, Suites exactes courtes, Groupes simples

Dans les exemples que nous venons de voir, on a un groupe G qui admet un sous-groupe distingué $N \triangleleft G$, et un sous-groupe $H < G$ *a priori* non distingué tels que tout élément $g \in G$ s'écrit de façon unique $g = nh$ où $n \in N$ et $g \in G$. On peut donc identifier **ensemblistement** G et le produit cartésien $N \times H$, et on veut comprendre comment la loi de G se transporte sur $N \times H$.

Si g_1 est associé au couple (n_1, h_1) et g_2 au couple (n_2, h_2), quel couple de $N \times H$ correspond au produit $g_1 g_2$? La petite ruse consiste simplement à écrire :

$$g_1 g_2 = n_1 h_2 n_2 h_2 = n_1 (\underbrace{h_1 n_2 h_1^{-1}}_{\in N}) h_1 h_2,$$

puisque N est distingué dans G. Ainsi, $g_1 g_2$ s'écrit comme le produit d'un élément de N et d'un élément de H :

$$g_1 g_2 = (\underbrace{n_1 (h_1 n_2 h_1^{-1})}_{\in N})(\underbrace{h_1 h_2}_{\in H}).$$

Ceci montre donc qu'en suivant la loi de G, le produit $N \times H$ est muni de la loi :

$$(n_1, h_1) \star (n_2, h_2) = (n_1 (h_1 n_2 h_1^{-1}), h_1 h_2).$$

Nous avons vu qu'on peut comprendre intrinsèquement ce qu'est la conjugaison hnh^{-1} sur les exemples rencontrés. Dans $G = \mathrm{Aff}(\mathbf{R}^n)$, l'action par conjugaison de $H = \mathrm{GL}_n(\mathbf{R})$ sur le groupe distingué des translations $N = \{\tau_v,\ v \in \mathbf{R}^n\} \simeq \mathbf{R}^n$ se traduit par l'action linéaire de $\mathrm{GL}_n(\mathbf{R})$ sur $\mathbf{R}^n$. Dans le cas de $G = D_n$, l'action par conjugaison de $H = \langle s \rangle$ sur $N = R_n$ se fait via $sr^k s^{-1} = r^{-k}$ pour $r \in R_n$ la rotation d'angle $2\pi/n$. Plus généralement, ceci nous conduit à la définition d'un produit semi-direct.

Définition 1.38

Soient N et H deux groupes, et $\varphi : H \to \mathrm{Aut}(N)$ un morphisme. On appelle **produit-semi direct** de N par H **relativement à** φ, et on note $N \rtimes_\varphi H$, le groupe dont l'ensemble sous-jacent est le produit cartésien $N \times H$, et dont la loi est

donnée, pour tous $(n_1, h_1), (n_2, h_2) \in N \times H$, par

$$(n_1, h_1).(n_2, h_2) = (n_1\varphi(h_1)[n_2], h_1h_2).$$

Preuve. Il faut vérifier que ceci définit bien une loi de groupe. Commençons par l'associativité. Soient $(n_i, h_i) \in N \times H$ pour $i \in \{1, 2, 3\}$. On calcule d'une part

$$\begin{aligned}(n_1, h_1).[(n_2, h_2).(n_3, h_3)] &= (n_1, h_1).(n_2\varphi(h_2)[n_3], h_2h_3)\\ &= (n_1\varphi(h_1)[n_2\varphi(h_2)[n_3]], h_1h_2h_3)\\ &= (n_1\varphi(h_1)[n_2](\varphi(h_1) \circ \varphi(h_2))[n_3], h_1h_2h_3)\\ &= (n_1\varphi(h_1)[n_2]\varphi(h_1h_2)[n_3], h_1h_2h_3),\end{aligned}$$

la troisième égalité venant du fait que $\varphi(h_1)$ est un morphisme de N, la quatrième du fait que φ est un morphisme de H vers $(\mathrm{Aut}(N), \circ)$. Et d'autre part

$$\begin{aligned}[(n_1, h_1).(n_2, h_2)].(n_3, h_3) &= (n_1\varphi(h_1)[n_2], h_1h_2).(n_3, h_3)\\ &= (n_1\varphi(h_1)[n_2]\varphi(h_1h_2)[n_3], h_1h_2h_3).\end{aligned}$$

Ainsi $(n_1, h_1).[(n_2, h_2).(n_3, h_3)] = [(n_1, h_1).(n_2, h_2)].(n_3, h_3)$, montrant l'associativité. Vérifions que (e, e) est un élément neutre (on ne s'embête pas à prendre différentes notations pour le neutre de N ou H). Soit $(n, h) \in N \times H$. On calcule :

$$(e, e).(n, h) = (e\varphi(e)[n], h) = (n, h) \text{ car } \varphi(e) = \mathrm{id}_N$$

et

$$(n, h).(e, e) = (n\varphi(h)[e], h) = (n, h) \text{ car } \forall f \in \mathrm{Aut}(N),\ f(e) = e.$$

Enfin, comme

$$(n, h).(\varphi(h)^{-1}[n^{-1}], h^{-1}) = (e, e) = (\varphi(h)^{-1}[n^{-1}], h^{-1})(n, h)$$

tout élément (n, h) est inversible d'inverse $(\varphi(h)^{-1}[n^{-1}], h^{-1})$. □

Remarque 1.24. Il faut toujours préciser le morphisme φ lorsqu'on parle d'un produit semi-direct.

Remarque 1.25. Notons qu'on peut toujours prendre le morphisme trivial $\varphi(h) = \mathrm{id}_N$ pour tout $h \in H$. On voit alors que la loi de produit semi-direct associée est celle du **produit direct** $N \times H$ de N et H : $(n_1, h_1).(n_2, h_2) = (n_1n_2, h_1h_2)$.

Remarque 1.26. On peut voir φ comme une *action* de H sur N par automorphismes.

Voyons à présent en quoi cette définition englobe ce que nous avons vu précédemment. La différence majeure (et l'intérêt) de ce point de vue est qu'on part de N et H et du morphisme φ pour construire un nouveau groupe G. Alors que dans les exemples, on avait identifié deux sous-groupes d'un groupe G donné au départ.

Définition 1.39

Soient G un groupe, et $N \triangleleft G$ un sous-groupe distingué. Soit H un sous-groupe de G. On appelle action par conjugaison de H sur N l'action $\varphi : H \to \mathrm{Aut}(N)$ donnée par

$$\forall h \in H,\ \forall n \in N,\ \varphi(h)[n] = hnh^{-1} \in N.$$

Notons bien que ceci ne peut être défini que pour un sous-groupe distingué N. Ainsi, pour tout unifier, il nous suffit de voir qu'étant donnée une action générale $\varphi : H \to$

$\mathrm{Aut}(N)$, les groupes N et H s'identifient à des sous-groupes de $G := N \rtimes_\varphi H$, avec N distingué dans G, tels que tout élément de G s'écrit de façon unique comme le produit d'un élément de N et d'un élément de H, et tels que l'action par conjugaison de H sur N corresponde à φ.

Proposition 1.34

Soient N et H deux groupes, et $\varphi : H \to \mathrm{Aut}(N)$ un morphisme. Notons $G = N \rtimes_\varphi H$ le produit semi-direct correspondant. Notons $i_N : N \to G$ l'application $i_N(n) = (n, e)$ et $i_H : H \to G$ l'application $i_H(h) = (e, h)$.

Alors i_N et i_H sont des morphismes injectifs, dont les images sont notées $\tilde{N}$ et $\tilde{H}$ respectivement. On a alors :

— $\tilde{N} \triangleleft G$

— $\tilde{N}.\tilde{H} = G$

— $\tilde{N} \cap \tilde{H} = (e, e)$

montrant que tout élément de G s'écrit de façon unique comme le produit d'un élément de $\tilde{N}$ et d'un élément de $\tilde{H}$. De plus, l'action par conjugaison de $\tilde{H}$ sur $\tilde{N}$ est donnée par

$$i_H(h) i_N(n) i_H(h)^{-1} = i_N(\varphi(h)[n]).$$

Preuve. Exercice. □

Exemple 1.16. Reprenons l'exemple du groupe affine de $\mathbf{R}^n$. Soient $H = \mathrm{GL}_n(\mathbf{R})$ et $N = (\mathbf{R}^n, +)$. Pour toute $A \in \mathrm{GL}_n(\mathbf{R})$, si on prend $\varphi_A : \mathbf{R}^n \to \mathbf{R}^n$ donnée par $\varphi_A(v) = Av$, on a bien $\varphi_A \in \mathrm{Aut}(\mathbf{R}^n)$ (pour la structure additive de $\mathbf{R}^n$), l'inverse étant bien-sûr $\varphi_{A^{-1}}$. Définissons alors

$$\begin{array}{rccc} \varphi : & \mathrm{GL}_n(\mathbf{R}) & \longrightarrow & \mathrm{Aut}(\mathbf{R}^n) \\ & A & \mapsto & \varphi_A. \end{array}$$

Alors, le produit semi-direct de $\mathbf{R}^n \rtimes_\varphi \mathrm{GL}_n(\mathbf{R})$ est donné par la loi :

$$(v_1, A_1).(v_2, A_2) = (v_1 + \varphi(A_1)(v_2), A_1 A_2) = (v_1 + A_1 v_2, A_1 A_2).$$

Ainsi, l'application

$$\begin{array}{ccc} \mathrm{Aff}(\mathbf{R}^n) & \longrightarrow & \mathbf{R}^n \rtimes_\varphi \mathrm{GL}_n(\mathbf{R}) \\ f = \tau_v A & \mapsto & (v, A) \end{array}$$

est un isomorphisme de groupes. Ce qu'on condense en disant que $\mathrm{Aff}(\mathbf{R}^n)$ est isomorphe au produit semi-direct de $\mathbf{R}^n$ par $\mathrm{GL}_n(\mathbf{R})$, *pour l'action linéaire de* $\mathrm{GL}_n(\mathbf{R})$ *sur* $\mathbf{R}^n$.

Exemple 1.17. De même, $\mathrm{Isom}(\mathbf{R}^n) \simeq \mathbf{R}^n \rtimes_\varphi O(n)$, pour l'action linéaire de φ de $O(n)$ sur $\mathbf{R}^n$. On peut en fait restreindre la partie linéaire à tout sous-groupe H de $\mathrm{GL}_n(\mathbf{R}^n)$.

Exemple 1.18. Le groupe diédral D_n d'ordre $2n$ est isomorphe au produit semi-direct $\mathbf{Z}/n\mathbf{Z} \rtimes_\varphi \mathbf{Z}/2\mathbf{Z}$, où $\varphi : \mathbf{Z}/2\mathbf{Z} = \{\pm 1\} \to \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$ est défini par $\varphi(\varepsilon) = \overline{\varepsilon k}$ pour tout $\varepsilon \in \{\pm 1\}$ et $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ (en identifiant $\mathbf{Z}/n\mathbf{Z}$ à R_n et $\mathbf{Z}/2\mathbf{Z}$ à $S = \langle s \rangle$).

Exercice 1.31

Montrer que $\mathfrak{S}_3 \simeq D_3$ (illustrer géométriquement). Expliciter l'isomorphisme $\mathfrak{S}_3 \simeq \mathbf{Z}/3\mathbf{Z} \rtimes_\varphi \mathbf{Z}/2\mathbf{Z}$ correspondant. (On verra une généralisation de ceci plus loin)

Plus généralement, une méthode très efficace pour comprendre/décrire un groupe G est d'identifier des sous-groupes *strictement plus petits* (et mieux compris) $N, H < G$ avec $N \triangleleft G$ tels que $G \simeq N \rtimes H$ pour l'action par conjugaison de H sur N, qu'il s'agit d'expliciter. Ceci passe nécessairement par une bonne compréhension du groupe $\mathrm{Aut}(N)$.

Dans le cadre des groupes finis (et dans celui du programme de l'agrégation), on se retrouvera principalement à identifier des produits semi-directs entre groupes cycliques, d'où notamment l'intérêt qu'on va leur porter dans la section suivante.

Pour clôturer cette (longue !) section généraliste, terminons par une définition qu'il est naturel de prendre à ce stade.

Définition 1.40

Un groupe G est dit **simple** si ses sous-groupes distingués sont $\{e\}$ et G.

Les groupes simples sont donc les groupes qu'on ne peut plus "dévisser", c'est-à-dire qu'on ne peut plus ramener leur étude à celle d'un sous-groupe distingué H strict et du quotient G/H. Leur rôle dans la théorie des groupes peut (assez grossièrement) être comparé à celui des nombres premiers en arithmétique. D'où notamment le traitement spécial qui leur est accordé. Dans le cas des groupes finis, leur classification a été achevée au début des années 1980, c'est dire l'ampleur de la tâche. Ceci déborde bien-sûr de notre programme. Néanmoins, on peut démontrer la simplicité de certains groupes que nous avons déjà rencontré. Ceci peut faire l'objet de très beaux développements.

Théorème 1.9

Pour tout $n \geqslant 5$, le groupe $\mathcal{A}_n$ des permutations paires est simple.

Corollaire 1.3

Pour $n \geqslant 5$, on a $D(\mathfrak{S}_n) = \mathcal{A}_n$ et $D(\mathcal{A}_n) = \mathcal{A}_n$.

Preuve. Les groupes $\mathfrak{S}_n$ et $\mathcal{A}_n$ sont non-abéliens (ici pour $n \geqslant 5$), puisqu'il suffit de considérer par exemple (1 2 3) et (3 4 5). Leurs groupes dérivés sont donc $\neq \{\mathrm{id}\}$. Par simplicité de $\mathcal{A}_n$, on en déduit $D(\mathcal{A}_n) = \mathcal{A}_n$ puisque $D(G) \triangleleft G$ pour tout groupe G. Ensuite, comme $\varepsilon([\sigma_1, \sigma_2]) = 1$ pour toutes permutations σ_1, σ_2, on a $A_n = D(\mathcal{A}_n) \subset D(\mathfrak{S}_n) \subset \mathcal{A}_n$, toutes ces inclusions sont donc des égalités. □

Remarque 1.27. Pour $n = 4$, le groupe $\mathcal{A}_4$ contient un sous-groupe distingué d'ordre 4 : celui formé par les doubles transpositions. Pour $n = 3$, $\mathcal{A}_3$ est simple car isomorphe à $\mathbf{Z}/3\mathbf{Z}$. D'ailleurs :

Proposition 1.35

Le groupe additif $\mathbf{Z}/n\mathbf{Z}$ est simple si et seulement si n est premier.

Preuve. Comme il est abélien, cela revient à dire qu'il n'admet pas de sous-groupe strict non-trivial, ce qui est une conséquence du théorème de Lagrange si n est premier, et si n n'est pas premier, il suffit de regarder le sous-groupe engendré par $\overline{d}$ pour un diviseur non-trivial de n. □

(Ceci ne peut pas faire l'objet d'un développement bien entendu !)

Théorème 1.10

Le groupe $\mathrm{SO}_3(\mathbf{R})$ est simple. Plus généralement, le groupe $\mathrm{PSO}_n(\mathbf{R})$ est simple pour $n \geqslant 5$.

Rappelons que $\mathrm{PSO}_n(\mathbf{R})$ désigne le quotient de $\mathrm{SO}_n(\mathbf{R})$ par son centre.

Exercice 1.32

Déterminer le centre de $\mathrm{SO}_n(\mathbf{R})$.

Le cas de $\mathrm{SO}_4(\mathbf{R})$ est très intéressant, et relié aux quaternions (cf **ref**). On termine sur deux petites propositions qu'il est bon d'avoir en tête.

Proposition 1.36

Soient G un groupe simple et H un groupe quelconque. Tout morphisme $f : G \to H$ est soit injectif, soit trivial, *i.e.* $f(g) = e$ pour tout $g \in G$.

Preuve. $\ker f \triangleleft G$. □

Proposition 1.37

Soit G un groupe simple et non abélien. Soit H un groupe abélien. Alors tout morphisme $f : G \to H$ est trivial, *i.e.* $\ker f = G$.

Preuve. Comme G est simple et non abélien, $D(G) = G$ puisque $D(G) \triangleleft G$. Comme H est abélien, on a

$$\forall g_1, g_2 \in G,\ f([g_1, g_2]) = f(g_1 g_2 g_1^{-1} g_2^{-1}) = [f(g_1), f(g_2)] = e_H.$$

Par définition de $D(G)$, on en déduit $f(g) = e_h$ pour tout $g \in D(G) = G$. □

Exemple 1.19. Tout morphisme $\mathrm{SO}_3(\mathbf{R}) \to (\mathbf{R}, +)$ est trivial.

Exercice 1.33

Quels sont les groupes simples et abéliens ?

Exercice 1.34

Sans utiliser la simplicité, comment voir que tout morphisme $f : \mathcal{A}_n \to (\mathbf{R}^*, \times)$ est trivial ?

2 Groupes abéliens finis

Rappelons que dans un groupe abélien, tout sous-groupe est distingué. Nous pouvons donc quotienter librement en toute impunité.

2.1 Structure des groupes cycliques : Retour sur $\mathbf{Z}/n\mathbf{Z}$

Comme son nom l'indique, $\mathbf{Z}/n\mathbf{Z}$ est le groupe quotient du groupe additif $\mathbf{Z}$ par son sous-groupe $n\mathbf{Z}$, où $n \geqslant 1$. On a vu que c'est le prototype du groupe cyclique d'ordre n : si $G = \langle g \rangle$ est un groupe cyclique d'ordre n, alors $G \simeq \mathbf{Z}/n\mathbf{Z}$ un isomorphisme étant donné par $\overline{k} \in \mathbf{Z}/n\mathbf{Z} \mapsto g^k \in G$. Ainsi, comprendre $\mathbf{Z}/n\mathbf{Z}$, c'est comprendre tous les groupes cycliques, notamment les sous-groupes engendrés par un élément de torsion dans un groupe quelconque.

En utilisant l'unicité dans la division euclidienne, on voit que $\{0, 1, \ldots, n-1\}$ forme un système de représentant dans $\mathbf{Z}$ pour la relation d'équivalence définissant $\mathbf{Z}/n\mathbf{Z}$:

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{k},\ k \in \mathbf{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Rappelons qu'il y a *plus* que la structure additive dans $\mathbf{Z}/n\mathbf{Z}$.

Proposition 2.1

Le groupe $\mathbf{Z}/n\mathbf{Z}$ admet une unique structure d'anneau (commutatif, unitaire) telle que la projection canonique $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ soit un morphisme d'anneaux.

Preuve. Ceci découle du fait que $n\mathbf{Z}$ est un idéal de $\mathbf{Z}$. □

Concrètement, si $\overline{k}_1, \overline{k}_2 \in \mathbf{Z}/n\mathbf{Z}$, leur somme et leur produit sont donnés par $\overline{k}_1 + \overline{k}_2 = \overline{k_1 + k_2}$ et $\overline{k}_1.\overline{k}_2 = \overline{k_1 k_2}$ (ces expressions sont bien définies et on a bien la propriété de distributivité). Un élément $\overline{k}$ est **inversible** (sous-entendu pour le produit) s'il existe $\overline{\ell}$ tel que $\overline{k}.\overline{\ell} = \overline{1}$. Lorsqu'il existe l'inverse est unique. L'ensemble des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ forme un groupe pour la multiplication.

Définition 2.1

On appelle **groupe des inversibles**, et on note $(\mathbf{Z}/n\mathbf{Z})^*$, le groupe des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$.

Rappelons que l'**indicatrice d'Euler** se définit par

$$\varphi(n) = \{k \in [\![1, \ldots, n-1]\!] \ :\ k \wedge n = 1\}.$$

Proposition 2.2

Un élément de $\mathbf{Z}/n\mathbf{Z}$ est inversible si et seulement s'il s'écrit $\overline{k}$, avec $k \wedge n = 1$. Par conséquent, $|(\mathbf{Z}/n\mathbf{Z})^*| = \varphi(n)$, où $\varphi(n)$ désigne l'indicatrice d'Euler.

Remarque 2.1. Notons que la condition $k \wedge n = 1$ est indépendante du choix du représentant : si $k - k' \in n\mathbf{Z}$, alors k est premier avec n si et seulement si k' est premier avec n.

Rappelons que l'**indicatrice d'Euler** se définit par

$$\varphi(n) = \{k \in [\![1, \ldots, n-1]\!] \ :\ k \wedge n = 1\}.$$

Preuve. Soit $k \in \mathbf{Z}$ un représentant d'un élément inversible. Par définition, il existe $\ell \in \mathbf{Z}$ tel que $\overline{k\ell} = \overline{1}$. Ainsi, il existe par définition encore $u \in \mathbf{Z}$ tel que $k\ell - 1 = un$. Ainsi, $k\ell - un = 1$, montrant que k et$n$ sont premiers entre-eux par le théorème de Bézout. Inversement, si $k \wedge n = 1$, alors toute relation de Bézout $ku + nv = 1$ montre que $\overline{k}\overline{u} = \overline{1}$ montrant que $\overline{k}$ est inversible. □

En particulier,

Théorème 2.1

Pour tout nombre premier p, l'anneau $\mathbf{Z}/p\mathbf{Z}$ est un corps.

Proposition 2.3

Un élément $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ est un générateur du groupe additif $(\mathbf{Z}/n\mathbf{Z}, +)$ si et seulement si $\overline{k} \in (\mathbf{Z}/n\mathbf{Z})^*$.

Noter que $\overline{k}$ est un générateur si et seulement s'il est d'ordre n.

Preuve. $\overline{k}$ est un générateur si et seulement si $\overline{1} \in \langle \overline{k} \rangle$ si et seulement si il existe ℓ tel que $\ell.\overline{k} = \overline{\ell k} = \overline{1}$ si et seulement si $\overline{k}$ est inversible. □

Proposition 2.4

Pour tout p premier et $\alpha > 0$ entier, on a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Preuve. Un entier $k \in [\![1, p^\alpha - 1]\!]$ est premier à p^α si et seulement s'il n'est pas divisible par p. Les entiers divisibles par p compris entre 1 et $p^\alpha - 1$ sont les pk, avec $1 \leqslant k \leqslant p^{\alpha-1} - 1$. D'où $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

On peut alors déterminer l'indicatrice d'Euler grâce au théorème suivant, appelé *théorème chinois*.

Théorème 2.2

Soient $n, m \geqslant 1$ deux entiers premiers entre-eux. On a un isomorphisme d'anneaux

$$\mathbf{Z}/nm\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

Preuve. Considérons l'application

$$\begin{array}{rccc} f : & \mathbf{Z} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \\ & k & \mapsto & (\overline{k}[n], \overline{k}[m]) \end{array}$$

où $\overline{k}[n]$ désigne la classe de k dans $\mathbf{Z}/n\mathbf{Z}$. Il est immédiat que f est un morphisme d'anneaux. Son noyau est formé des éléments k qui sont à la fois divisibles par m et n. Puisqu'ils sont premiers entre-eux, par le lemme de Gauss, un élément $k \in \mathbf{Z}$ est dans le noyau de f si et seulement s'il est divisible par nm. Autrement dit, $\ker f = nm\mathbf{Z}$. Par le théorème de factorisation, on en déduit que f induit un morphisme d'anneaux injectif $\overline{f} : \mathbf{Z}/nm\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. Par égalité des cardinaux, $\overline{f}$ est surjectif et réalise donc un isomorphisme. □

On déduit du théorème chinois que $\varphi(nm) = \varphi(n)\varphi(m)$ pour m, n des entiers premiers entre-eux. Notamment, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers, où les p_i sont deux à deux distincts, alors

$$\varphi(n) = \prod_{i=1}^{k} (p^{\alpha_i} - p^{\alpha_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Remarque 2.2. Cette formule théorique est difficile à implémenter dans la pratique puisqu'elle implique de connaître les facteurs premiers de n. Ceci joue un rôle en cryptographie (notamment pour le codage RSA [2]).

Théorème 2.3

Le groupe des automorphismes $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +)$ s'identifie au groupe des inversibles $(\mathbf{Z}/n\mathbf{Z})^*$. L'automorphisme associé à $\overline{k_0} \in (\mathbf{Z}/n\mathbf{Z})^*$ est $\{\overline{k} \mapsto \overline{k_0}.\overline{k}\}$.

Preuve. On a clairement une injection $(\mathbf{Z}/n\mathbf{Z})^* \hookrightarrow \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$. Il nous faut voir qu'elle est surjective. Si f est un automorphisme quelconque, notons $\overline{k_0} = f(\overline{1})$. Alors, pour tout $k \in [\![0, n-1]\!]$, on a $f(\overline{k}) = f(\overline{1} + \cdots + \overline{1}) = k.\overline{k_0} = \overline{k_0}.\overline{k}$. Comme f est surjectif, $\overline{1}$ admet un antécédent, ce qui signifie que $\overline{k_0} \in (\mathbf{Z}/n\mathbf{Z})^*$. □

Ainsi, la compréhension des automorphismes de $\mathbf{Z}/n\mathbf{Z}$ est ramenée à celle du groupe des inversibles, qui, d'après le résultat précédent, est isomorphe au groupe produit des $(\mathbf{Z}/p^{\alpha_i}\mathbf{Z})^*$. On est donc ramenés au cas où $n = p^\alpha$. On sait que le groupe est d'ordre $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Il est en faitæ lui-même cyclique, sauf dans le cas $p = 2$ et $\alpha > 2$.

Théorème 2.4

Soit $p > 2$ un nombre premier. Alors $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique.

Preuve. Voir [Per96] pour les détails. On montre que $x = \overline{1+p}$, qui est un inversible, est d'ordre $p^{\alpha-1}$ dans $\mathbf{Z}/p^\alpha\mathbf{Z}$. Si on trouve un élément d'ordre $p-1$, alors on a fini en vertu du lemme (à vérifier en exercice) :

Lemme 2.1

Si G est un groupe commutatif, et si $x, y \in G$ sont d'ordre n, m avec $n \wedge m = 1$, alors xy est d'ordre nm.

Tout repose alors sur le cas $\alpha = 1$, qui est un cas spécial d'un résultat sur les corps finis.

Théorème 2.5

Pour tout nombre premier p, le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique, donc isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$.

2. Voir par exemple ces notes de D. Perrin

Preuve. Le point clé est la propriété suivante : Pour tout $d \geqslant 1$, dans le corps $\mathbf{Z}/p\mathbf{Z}$, l'équation $x^d = 1$ a au plus d solutions. Bien-sûr, ceci provient du fait que le polynôme $X^d - 1$ a au plus d racines.

Dès lors, considérons x un élément d'ordre d dans $(\mathbf{Z}/p\mathbf{Z})^*$. Par définition, le sous-groupe cyclique $\langle x \rangle$ est d'ordre d, et tout élément $y \in \langle x \rangle$ vérifie $y^d = 1$. Par conséquent, $\langle x \rangle$ est l'ensemble des solutions de l'équation $y^d = 1$ par cardinalité. En particulier, tout autre élément d'ordre d est dans $\langle x \rangle$. Il y a donc précisément $\varphi(d)$ éléments d'ordre d dans $(\mathbf{Z}/p\mathbf{Z})^*$.

Ainsi, étant donné un diviseur d de $p-1$, ou bien il n'y a aucun élément d'ordre d, ou bien il y a $\varphi(d)$ éléments d'ordre d. En regroupant les éléments selon leur ordre, on a :

$$\begin{aligned} p - 1 = |(\mathbf{Z}/p\mathbf{Z})^*| &= \sum_{d|p-1} \mathrm{Card}\{x \in (\mathbf{Z}/p\mathbf{Z})^* \ : \ x \text{ d'ordre } d\} \\ &\leqslant \sum_{d|p-1} \varphi(d) \\ &= p - 1. \end{aligned}$$

Ainsi, toutes les inégalités sont des égalités, et pour tout diviseur d, il existe des éléments d'ordre d. En particulier, il existe un élément d'ordre $p-1$, montrant la cyclicité. □

Remarque 2.3. La preuve du Théorème 2.5 se transpose *verbatim* à la situation où $\mathbf{Z}/p\mathbf{Z}$ est remplacé par un corps fini.

On peut terminer la preuve. On considère l'application naturelle $f : \mathbf{Z}/p^\alpha\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ (exercice : comment la définir ?). On vérifie qu'elle induit un morphisme surjectif $g : (\mathbf{Z}/p^\alpha\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$. Soit alors $x \in (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ un antécédent d'un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$. Nécessairement, l'ordre de x est divisible par $p-1$. Ceci montre donc qu'une certaine puissance de x est d'ordre $p-1$.

Comme on a vu qu'il existe un élément d'ordre $p^{\alpha-1}$, qui est premier avec $p-1$, on en déduit par le Lemme **??** qu'il existe un élément d'ordre $(p-1)p^{\alpha-1} = |(\mathbf{Z}/p\mathbf{Z})^*|$, d'où la cyclicité dans le cas général. □

Théorème 2.6

Pour tout $\alpha \geqslant 3$ entier, on a $(\mathbf{Z}/2^\alpha\mathbf{Z})^* \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. Il n'est donc pas cyclique.

Preuve. [Per96] □

Exercice 2.1

Le vérifier directement dans le cas de $\mathbf{Z}/8\mathbf{Z}$.

Proposition 2.5

Soit $n \geqslant 1$. Alors pour tout d diviseur de n, il existe un unique sous-groupe d'ordre d de $\mathbf{Z}/n\mathbf{Z}$. En notant $\ell = n/d$, il s'agit du sous-groupe engendré par $\overline{\ell}$, *i.e.* la projection de $\ell\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$.

Preuve. Soit $\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ la projection canonique. Soit $H \subset \mathbf{Z}/n\mathbf{Z}$ un sous-groupe. Considérons $H' = \pi^{-1}(H)$: c'est un sous-groupe de $\mathbf{Z}$, et il contient $\pi^{-1}(\{0\}) = n\mathbf{Z}$. D'après l'exercice **ref**, il existe $k \in \mathbf{N}$ tel que $H' = k\mathbf{Z}$, et on a de plus $n\mathbf{Z} \subset k\mathbf{Z}$, c'est-à-dire k divise n.

Comme k engendre additivement $H' = k\mathbf{Z}$, on en déduit que $\pi(k)$ engendre $H = \pi(H')$. Ceci montre que H est cyclique, il est d'ordre $d := n/k$. □

2.2 Théorème de structure des groupes abéliens finis

Commençons par prendre la définition générale suivante.

Définition 2.2

Un groupe G est dit d'*exposant fini* s'il existe un entier $k \geqslant 1$ tel que $g^k = e$ pour tout $g \in G$.

Dans ce cas, $\{k \in \mathbf{Z} \mid \forall g \in G,\ g^k = e\}$ est un sous-groupe non-trivial de $\mathbf{Z}$, donc de la forme $m\mathbf{Z}$, où $m \geqslant 1$. L'entier m est alors appelé l'*exposant* de G.

Exemple 2.1.

1. Tout groupe fini est d'exposant fini, et son exposant divise l'ordre du groupe.
2. Le groupe additif $G = (\mathbf{Z}/2\mathbf{Z})^{\mathbf{N}}$ des suites à valeurs dans $\mathbf{Z}/2\mathbf{Z}$ est infini et d'exposant fini (égal à 2).
3. Le groupe $(\mathbf{Z}, +)$ n'est pas d'exposant fini.
4. L'exposant de $\mathfrak{S}_3$ vaut 6, mais il n'existe aucun élément d'ordre 6.

Rappelons qu'on note $\omega(g)$ l'ordre d'un élément.

Proposition 2.6

Un groupe G est d'exposant fini si et seulement si tout élément est d'ordre fini et $\{\omega(g),\ g \in G\}$ est fini. Dans ce cas, son exposant est le ppcm des ordres de ses éléments.

Preuve. Pour le sens direct, l'ordre de tout élément doit diviser l'exposant m de G, donc $\{\omega(g),\ g \in G\}$ est contenu dans l'ensemble des diviseurs de m qui est bien-sûr fini. Pour la réciproque, si $X = \{\omega(g),\ g \in G\}$ est fini, alors en prenant pour k le ppcm des éléments de X, on a $g^k = e$ pour tout $g \in G$, montrant que G est d'exposant fini.

Si on suppose G d'exposant fini, alors avec les notations précédentes, on vient de voir que $m|k$. D'autre part, pour tout $g \in G$, comme $g^m = e$, on a $\omega(g)|m$. Ainsi, m est un multiple commun à tous les $\omega(g)$, $g \in G$, d'où $k|m$. □

Proposition 2.7

Soit G un groupe abélien fini. Alors, il existe un élément $g \in G$ dont l'ordre est l'exposant de G.

Preuve. Puisque G est fini, il existe un élément $g_0 \in G$ tel que

$$\omega(g_0) = \max\{\omega(g),\ g \in G\}.$$

Montrons par l'absurde que $\omega(g_0)$ est l'exposant de G, ce qui conclura. Supposons donc qu'il existe $g \in G$ tel que $\omega(g)$ ne divise pas $\omega(g_0)$. En considérant leurs décompositions en facteurs premiers, cela signifie qu'il existe un nombre premier p, deux entiers $\alpha, \beta \in \mathbf{N}^*$ tels que $\alpha < \beta$, et deux entiers $k_0, k \in \mathbf{N}^*$ tels que $k_0 \wedge p = k \wedge p = 1$

et

$$\omega(g_0) = p^\alpha k_0 \text{ et } \omega(g) = p^\beta k.$$

Comme $(g_0)^{p^\alpha}$ est d'ordre k_0 et g^k est d'ordre p^β puisque k_0 et p^β sont premiers entre-eux et que G est abélien, nous obtenons en vertu du Lemme **??** que l'élément $g_1 = (g_0)^{p^\alpha} g^k$ est d'ordre $p^\beta k > p^\alpha k = \omega(g_0)$: contradiction. □

Énonçons à présent le résultat principal de cette section.

Théorème 2.7

Soit G un groupe abélien fini. Alors il existe une suite d'entiers $d_1, \ldots, d_n \geqslant 1$ tels que pour tout $i \in [\![1, n-1]\!]$, $d_i | d_{i+1}$ et

$$G \simeq (\mathbf{Z}/d_1\mathbf{Z}) \times (\mathbf{Z}/d_2\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z}).$$

De plus, une telle suite est unique au sens où si $d'_1, \ldots, d'_m$ est une autre suite vérifiant $d'_i | d'_{i+1}$ pour tout $i \in [\![1, m-1]\!]$ et $G \simeq (\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d'_m\mathbf{Z})$, alors $n = m$ et $d_i = d'_i$ pour tout $i \in [\![1, n]\!]$.

On notera que d_n est l'exposant de G. Pour montrer ce résultat, on va utiliser un résultat qui assure le *prolongement des caractères* sur un groupe abélien fini.

Proposition 2.8

Soit G un groupe abélien fini et soit $H < G$ un sous-groupe. Soit $\chi_0 : H \to \mathbf{C}^*$ un morphisme. Alors il existe un morphisme $\chi : G \to \mathbf{C}^*$ tel que $\chi_0 = \chi|_H$.

Preuve. On procède par récurrence forte sur $[G : H]$.

Si H est un sous-groupe d'indice 1, alors le résultat est évident puisque $H = G$.

Supposons que pour $1 \leqslant k < |G|$, tout caractère défini sur un sous-groupe H d'indice au plus k s'étend en un caractère de G. Montrons que la proposition est vraie pour les sous-groupes d'indice $k+1$.

Soit donc H un sous-groupe d'indice $k+1$ dans G et soit χ_0 un caractère de H. Comme $k+1 > 1$, $H \neq G$ et on peut choisir $g \notin H$. Soit n l'ordre de gH dans le groupe quotient G/H (bien défini car G est abélien). Ainsi, n est le plus petit entier strictement positif tel que $g^n \in H$. Noter que $n \geqslant 2$.

Soit $H' = \{hg^k,\ h \in H,\ k \in \mathbf{Z}\}$ le sous-groupe engendré par $H \cup \{g\}$. Comme $|H'| > |H|$, on peut lui appliquer l'hypothèse de récurrence, et il nous suffit donc d'étendre χ_0 à H', qui s'étendra alors à tout G par hypothèse de récurrence.

Choisissons $z \in \mathbf{C}^*$ tel que $z^n = \chi_0(g^n)$ et montrons qu'on peut étendre χ_0 en un caractère $\chi'_0 : H' \to \mathbf{C}^*$ tel que $\chi'_0|_H = \chi_0$ et $\chi'_0(g) = z$. Tout élément de H' se met sous la forme hg^k, mais de façon non nécessairement unique. Néanmoins, si $h_1 g^{k_1} = h_2 g^{k_2}$ pour $h_1, h_2 \in H$ et $k_1, k_2 \in \mathbf{Z}$, alors $h_1 h_2^{-1} = g^{k_2 - k_1}$, d'où l'existence de $a \in \mathbf{Z}$ tel que $k_2 - k_1 = an$. Ainsi

$$\begin{aligned} \chi_0(h_2) z^{k_2} = \chi_0(h_2) z^{an} z^{k_1} &= \chi_0(h_2)\chi_0(g^n)^a z^{k_1} \\ &= \chi_0(h_2 g^{an}) z^{k_1} \\ &= \chi_0(h_1) z^{k_1}. \end{aligned}$$

Ainsi, *quelle que soit* l'écriture $h' = hg^k$, $h \in H$, $k \in \mathbf{Z}$ d'un élément de H', la valeur

de $\chi_0(h)z^k \in \mathbf{C}^*$ est la même, et nous pouvons bien définir une application

$$\begin{array}{rccc} \chi_0' : & H' & \longrightarrow & \mathbf{C}^* \\ & hg^k & \mapsto & \chi_0(h)z^k \end{array}$$

dont il est immédiat de vérifier que c'est un morphisme de groupes, donc un caractère de H' qui étend χ_0. D'après l'hypothèse de récurrence, il existe un caractère $\chi : G \to \mathbf{C}^*$ tel que $\chi|_{H'} = \chi_0'$, donc *a fortiori* $\chi|_H = \chi_0$, ce qui termine la récurrence. □

Preuve de l'existence de la décomposition. Soient $m \geqslant 1$ l'exposant de G et $h \in G$ un élément d'ordre m. Soit $H_1 = \langle h \rangle$. Soit $\chi_0 : G \to \mathbf{C}^*$ le morphisme tel que pour tout $k \in \mathbf{Z}$, $\chi_0(h^k) = \exp(\frac{2ik\pi}{m}) \in \mathbb{U}_m$ (qui est bien défini puisque h est d'ordre m). Soit $\chi : G \to \mathbf{C}^*$ étendant χ_0. Comme m est l'exposant de G, on a $g^m = e$ pour tout $g \in G$, et donc $\chi(G) \subset \mathbb{U}_m$. Soit $G_1 = \ker \chi$. Alors, d'une part $G_1 \cap H_1 = \{e\}$, et d'autre part, si $g \in G$, comme $\chi_0(H_1) = \mathbb{U}_m$, il existe $h \in H_1$ tel que $\chi(g) = \chi(h)$, d'où $gh^{-1} \in G_1$, ce qui montre que $G = G_1H_1$. Donc, G est isomorphe au groupe produit $G_1 \times H_1$. On pose $d_0 = m$. Si G_1 n'est pas cyclique, alors on appelle d_1 l'exposant de G_1, qui nécessairement divise celui de G et on applique ce qu'on vient de faire à G_1, pour obtenir un sous-groupe $G_2 \subset G_1$ et un sous-groupe cyclique $H_2 \subset G_1$ d'ordre d_1 tels que $G_1 \simeq G_2 \times H_2$. En itérant le processus, on définit ainsi une suite finie $G_k \subsetneq G_{k-1} \subsetneq \cdots \subsetneq G_1 \subsetneq G_0 = G$ telle que $G_k \neq \{e\}$ est cyclique, et si d_i est l'exposant de G_i ; alors pour tout $i \in \{0, \ldots, k-1\}$, il existe $H_{i+1} \subset G_i$ cyclique d'ordre d_i tel que $G_{i+1} \cap H_{i+1} = \{e\}$ et $G_i = G_{i+1}H_{i+1}$. On prend enfin $d_k = |G_k|$ et on a $d_k | d_{k-1} | \ldots | d_1 | d_0$ et G est isomorphe au produit $(\mathbf{Z}/d_k\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_0\mathbf{Z})$. En réordonnant la liste, on obtient bien la décomposition annoncée.

Preuve de l'unicité de la décomposition Considérons deux telles décompositions. Alors, nécessairement l'exposant de G est d_n, mais aussi d_m'. D'où $d_n = d_m'$. On voudrait alors « simplifier » les deux membres de $(\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z}) \simeq (\mathbf{Z}/d_1'\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_m'\mathbf{Z})$ par $\mathbf{Z}/d_n\mathbf{Z}$ et pouvoir appliquer le même argument en cascade. On utilise pour cela le résultat suivant, laissé en exercice.

Exercice 2.2
Soit G un groupe et soient $H_1 \triangleleft G$ et $H_2 \triangleleft G$ deux sous-groupes distingués. Montrer que s'il existe $f \in \mathrm{Aut}(G)$ tel que $f(H_1) = H_2$, alors $G/H_1 \simeq G/H_2$.
Donner un contre-exemple si on suppose seulement $H_1 \simeq H_2$.

Dans le cas présent, nous aurons donc quasiment conclu après avoir prouvé :

Lemme 2.2
Soit G un groupe abélien fini. Soient $g_1, g_2 \in G$ deux éléments dont l'ordre est égal à l'exposant de G. Alors, il existe un automorphisme $f \in \mathrm{Aut}(G)$ tel que $g_2 = f(g_1)$.

Autrement dit, le groupe $\mathrm{Aut}(G)$ opère transitivement sur l'ensemble des éléments d'ordre maximal de G.

Démonstration. D'après ce qui précède, on a existence d'entiers $d_1 | \cdots | d_n$ tels que $G \simeq (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z})$. Soit $k \leqslant n$ le plus petit entier tel que $d_k = d_n$. Notons $d = d_n$ l'exposant de G. Alors, un n-uplet $(x_1, \ldots, x_n) \in (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z})$ est d'ordre d si et seulement s'il existe $i \in \{k, \ldots, n\}$ tel que x_i est un générateur de $(\mathbf{Z}/d\mathbf{Z}, +)$. Appelons x_0 l'élément $(0, \ldots, 0, 1)$, qui est donc d'ordre d. Si $x = (x_1, \ldots, x_n)$ est un élément d'ordre d quelconque, il s'agit de trouver un automorphisme de G qui envoie x_0 sur x.

Étant donnée une permutation $\sigma : \{k, \dots, n\} \to \{k, \dots, n\}$, l'application $\varphi_\sigma : G \to G$ définie par $\varphi_\sigma(y_1, \dots, y_n) = (y_1, \dots, y_{k-1}, y_{\sigma(k)}, \dots, y_{\sigma(n)})$ est un automorphisme de G.[3] Ainsi, comme on sait qu'il existe $i \in \{k, \dots, n\}$ tel que x_i est inversible dans $\mathbf{Z}/d\mathbf{Z}$, on peut se ramener au cas $i = n$ à l'aide d'un automorphisme de la forme φ_σ, *i.e.* on peut supposer que x_n est inversible dans $\mathbf{Z}/d\mathbf{Z}$, ce que nous faisons dès à présent.

Définissons $H = \{(y_1, \dots, y_{n-1}, 0),\ y_i \in \mathbf{Z}/d_i\mathbf{Z}\}$, $K = \langle x \rangle$ et $K_0 = \langle x_0 \rangle$. Puisque la dernière composante de x est inversible dans $\mathbf{Z}/d\mathbf{Z}$, tout comme celle de x_0, nous avons $H \cap K = H \cap K_0 = \{0\}$. Par conséquent, les applications

$$\varphi : \begin{array}{ccc} H \times K & \to & G \\ (y, z) & \mapsto & y + z \end{array} \quad \text{et} \quad \varphi_0 : \begin{array}{ccc} H \times K_0 & \to & G \\ (y, z) & \mapsto & y + z \end{array}$$

sont injectives, donc bijectives par cardinalité, donc des isomorphismes de groupes. Notons $\alpha : K_0 \to K$ l'isomorphisme tel que $\alpha(x_0) = x$ et $\tilde{\alpha} = (\mathrm{id}, \alpha) : H \times K_0 \to H \times K$. Alors, $\psi = \varphi \circ \tilde{\alpha} \circ (\varphi_0)^{-1} \in \mathrm{Aut}(G)$ et $\psi(x_0) = x$, ce qui termine la preuve. □

Ainsi, étant donné un groupe abélien fini G, s'il existe deux isomorphismes $\phi_1 : G \to (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z})$ et $\phi_2 : G \to (\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d'_m\mathbf{Z})$ avec $d_1 | \cdots | d_n$ et $d'_1 | \cdots | d'_m$, alors $d_n = d'_m$ est l'exposant de G, et si $H_1 = \phi_1^{-1}(\mathbf{Z}/d_n\mathbf{Z})$ et $H_2 = \phi_2^{-1}(\mathbf{Z}/d'_m\mathbf{Z})$, alors il existe $\psi \in \mathrm{Aut}(G)$ tel que $H_2 = \psi(H_1)$ d'après le résultat précédent, et donc G/H_1 et G/H_2 sont isomorphes. Appelons $\pi_1 : (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z}) \to (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_{n-1}\mathbf{Z})$ et $\pi_2 : (\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d'_m Z) \to (\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d'_{m-1} Z)$ les projections sur les $n-1$ et $m-1$ premières coordonnées. Alors, $H_1 = \phi_1^{-1}(\ker \pi_1)$ et $H_2 = \phi_2^{-1}(\ker \pi_2)$. En appliquant le théorème de factorisation à $\phi_1 \circ \pi_1$ et $\phi_2 \circ \pi_2$, on en déduit que $G/H_1 \simeq (\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_{n-1}\mathbf{Z})$ et $G/H_2 \simeq (\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d'_{m-1} Z)$. Une récurrence finie permet alors de conclure.

3 Groupes finis généraux : Théorèmes de Sylow et un peu de zoologie

On s'intéresse à présent aux groupes finis qui ne sont plus nécessairement abéliens. On rentre alors en contact avec une faune nettement plus variée et riche. Notre objectif modeste sera de savoir décrire les groupes de petit cardinal ou bien dont l'ordre est d'une forme assez spéciale. Les outils centraux sont les théorèmes de Sylow qui permettent de comprendre certains sous-groupes d'un groupe fini G à l'aide de considérations arithmétiques élémentaires.

3.1 Théorème de Cauchy

On donne pour commencer le cas général du théorème de Cauchy.

Théorème 3.1

Soit G un groupe fini d'ordre n, et soit p un facteur premier de n. Alors il existe un élément d'ordre p dans G.

Preuve. Nous cherchons à voir que l'équation $g^p = e$ a au moins deux solutions dans G, puisque $g = e$ est solution évidente. L'idée est de s'intéresser à une question un peu plus générale : les p-uplets d'éléments de G dont le produit vaut e. Considérons

$$X = \{(g_1, \dots, g_p) \in G^p \ :\ g_1 \dots g_p = e\}.$$

3. Plus généralement, toute matrice de la forme $\begin{pmatrix} I_{n-k} & 0 \\ 0 & A \end{pmatrix}$, où $A \in \mathrm{GL}(\mathbf{Z}/d\mathbf{Z})$, produit un automorphisme de G via son action linéaire sur les coordonnées.

Notons que si $g_1 \dots g_p = e$, alors $g_2 \dots g_p g_1 = g_1^{-1}(g_1 \dots g_p)g_1 = e$. Ainsi, en notant $c = (1\ 2\ \cdots\ p)$, nous avons $(g_1, \dots, g_p) \in X \Rightarrow (g_{c(1)}, \dots, g_{c(p)}) \in X$, *i.e.* X est stable par permutation circulaire. On dispose donc d'une action de $H := \mathbf{Z}/p\mathbf{Z}$ sur X donnée par :

$$\overline{k}.(g_1, \dots, g_p) = (g_{c^k(1)}, \dots, g_{c^k(p)}).$$

Notons qu'un élément $x \in X$ est fixé par H si et seulement s'il est de la forme $x = (g, \dots, g)$ avec $g \in G$ vérifiant $g^p = e$. Notons X^H l'ensemble des points fixes de H. L'équation aux classes pour cette action nous donne

$$\sharp X = \sharp X^H + \sum_{x \in \mathcal{R}} \sharp H.x.$$

où $\mathcal{R}$ est un système de représentants des H-orbites non-réduites à un point fixe. Or, p étant premier, pour tout $x \in \mathcal{R}$, comme $H_x \subsetneq H$, on a $H_x = \{\overline{0}\}$. D'où $\sharp H.x = \sharp(H/H_x) = p$. L'équation aux classes implique donc que

$$\sharp X \equiv \sharp X^H \bmod p.$$

D'autre part, on peut dénombrer facilement X : il suffit de l'écrire sous la forme

$$X = \{(g_1, \dots, g_{p-1}, (g_1 \dots g_{p-1})^{-1}),\ g_1, \dots, g_{p-1} \in G\}.$$

Ainsi, $\sharp X = |G|^{p-1}$. En particulier, il est divisible par p, et donc $\sharp X^H$ est divisible par p. Comme $(e, \dots, e) \in X^H \neq \emptyset$, on en déduit $\sharp X^H \geqslant p \geqslant 2$, ce qui termine la preuve. □

3.2 Théorèmes de Sylow

Soit p un nombre premier. Soit G un groupe fini d'ordre $n \geqslant 1$. Supposons que p divise n. On écrit $n = p^\alpha m$, où $p \wedge m = 1$ et $\alpha > 0$.

Définition 3.1

On appelle **p-Sylow** de G tout sous-groupe $H < G$ d'ordre p^α. Plus généralement, un **p-sous groupe** de G est un sous-groupe de G dont l'ordre est une puissance de p, c'est-à-dire de la forme p^β, avec nécessairement $\beta \leqslant \alpha$ par le théorème de Lagrange.

Le théorème de Cauchy montre que si p divise l'ordre de G, alors G admet des sous-p-groupes (avec $\beta = 1$). Le premier théorème de Sylow raffine ceci.

Théorème 3.2 (Sylow 1)

Soit G un groupe fini et p un facteur premier de $|G|$. Alors G contient un p-Sylow.

Une première preuve.

Preuve. On commence par vérifier le théorème dans le cas spécial $G = \mathrm{GL}_n(\mathbf{F}_p)$, qui est un groupe fini d'ordre $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^\alpha m$, où $\alpha = \frac{n(n-1)}{2}$ et $p \wedge m = 1$. En considérant le sous-groupe $S < G$ formé des matrices triangulaires supérieures à diagonale unité :

$$S = \left\{ \begin{pmatrix} 1 & s_{1,2} & \cdots & s_{1,n} \\ & 1 & \cdots & s_{2,n} \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix},\ s_{ij} \in \mathbf{F}_p,\ 1 \leqslant i < j \leqslant n \right\}$$

On dénombre $|S| = p^\alpha$, puisque $\alpha = \frac{n(n-1)}{2}$ est précisément le nombre d'entrées des paramètres s_{ij}. Ceci montre que S est un p-Sylow de G.

Pour passer au cas général, on prouve le lemme suivant, qui sera réutilisé plus loin.

Lemme 3.1
Soient G un groupe fini, $H < G$ un sous-groupe et $S < G$ un p-Sylow de G. Alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ est un p-Sylow de H.

Preuve. Considérons le quotient à droite $X = G/S$. C'est un ensemble fini d'ordre $m = n/p^\alpha$ sur lequel G agit (transitivement) par translation à gauche. On écrit l'équation aux classes pour la restriction à H de cette action :

$$m = \sharp X = \sum_{x \in \mathcal{R}} |H|/|H_x|,$$

où $\mathcal{R} \subset X$ désigne un système de représentants des H-orbites, et H_x le stabilisateur d'un point x de X. Déterminons le stabilisateur H_x d'un point $x = gS$ (un point de X est une classe à droite de S). Pour tout $h \in H$, $h \in H_x \iff hgS = gS \iff g^{-1}hg \in S \iff h \in gSg^{-1}$. Ainsi, $H_x = H \cap (gSg^{-1})$.

Remarque 3.1. Noter que cela ne dépend pas du représentant g de x.

Puisque p est premier à m, l'équation ci-dessus implique qu'un terme de la somme de droite n'est pas divisible par p. Il existe donc $x \in X$ tel que H_x est un p-Sylow de H. Le lemme est donc prouvé en prenant un représentant quelconque g de x. □

Lemme 3.2
Tout groupe fini G est isomorphe à un sous groupe de $\mathrm{GL}_n(K)$, où $n = |G|$ et K est un corps quelconque.

Preuve. Il s'agit de construire un morphisme injectif de G vers un tel groupe linéaire. D'après le théorème de Cayley **ref**, on a un morphisme injectif $G \to \mathfrak{S}_n$. Or, les matrices de permutation donnent également un plongement $\sigma \in \mathfrak{S}_n \mapsto P_\sigma \in \mathrm{GL}_n(K)$. Rappelons que P_σ est la matrice dans la base canonique (e_i) de l'endomorphisme défini par $u_\sigma(e_k) = e_{\sigma(k)}$ pour tout $k \in [\![1, n]\!]$. La composition de ces deux morphismes injectifs reste injective, et son image est un sous-groupe de $\mathrm{GL}_n(K)$ isomorphe à G, comme annoncé. □

On conclut la preuve du théorème en appliquant le Lemme 3.1 à $G = \mathrm{GL}_n(\mathbf{F}_p)$, S le sous-groupe des matrices triangulaires unipotentes, et H un sous-groupe de G isomorphe au groupe fini qui nous intéresse. □

Une deuxième preuve.
Attention il n'y a pas forcément unicité du p-Sylow. Néanmoins,

Théorème 3.3 (Sylow 2)
Soit G un groupe fini et p un facteur premier de $|G|$. Alors, ses p-Sylow sont conjugués deux à deux.

Autrement dit, si S_1 et S_2 sont deux p-Sylow de G, alors il existe $g \in G$ tel que $S_2 = gS_1g^{-1}$.

Preuve. Soient $S_1, S_2 < G$ deux p-Sylow de G. On applique le Lemme 3.1 en prenant $H = S_2$ et $S = S_1$. Nous avons alors existence de $g \in G$ tel que $S_2 \cap (gS_1g^{-1})$ est un p-Sylow de S_2. Par définition, ceci signifie $S_2 \cap (gS_1g^{-1}) = S_2$, *i.e.* $S_2 \subset gS_1g^{-1}$, et donc $S_2 = gS_1g^{-1}$ par cardinalité. □

Une conséquence très importante dans la pratique :

Corollaire 3.1

Soit G un groupe fini et p un facteur premier de $|G|$. Si G admet un unique p-Sylow S, alors $S \triangleleft G$.

Preuve. Pour tout $g \in G$, la conjugaison $i_g : h \in G \mapsto ghg^{-1} \in G$ est un automorphisme de G, en particulier une bijection. Donc pour toute partie finie $A \subset G$, $i_g(A)$ et A ont même cardinal.

Soit S le supposé unique p-Sylow de G et soit $g \in G$. Alors gSg^{-1} est un sous-groupe de G dont l'ordre est le même que celui de S. Par définition, gSg^{-1} est donc lui aussi un p-Sylow. Par unicité, on en déduit $gSg^{-1} = S$, et ceci quel que soit g. D'où le résultat. □

Le dernier résultat permet de dénombrer les p-Sylow, notamment de voir s'il y a unicité.

Théorème 3.4 (Sylow 3)

Soit G un groupe fini d'ordre $p^\alpha m$, avec $p \wedge m = 1$ et $\alpha \geqslant 1$. Soit n_p le nombre de p-Sylow de G. Alors,

1. n_p divise m.
2. $n_p \equiv 1 \bmod p$.

Preuve. Soit $X = \mathrm{Syl}_p(G) \subset \mathcal{P}(G)$ l'ensemble des p-Sylow de G. Comme observé précédemment, si $S \in X$ et $g \in G$, alors $gSg^{-1} \in X$. Ceci montre que G agit sur X par conjugaison et le Théorème 3.3 montre que cette action est transitive.

D'après **ref**, on déduit que pour tout $S \in X$, X est en bijection avec G/G_S, où G_S désigne comme d'habitude le stabilisateur de S. Par définition, pour tout $g \in G$, $g \in G_S \iff gSg^{-1} = S$. Ainsi, le stabilisateur de S est le *normalisateur* de S dans G, $N_G(S) = \{g \in G \ : \ gSg^{-1} = S\}$. Ainsi, $S \subset G_S$, et donc $|G_S| = p^\alpha m'$ avec $m'|m$ puisque $|G_S|$ divise $|G|$. On en tire que $n_p = \sharp X = m/m'$ divise m, prouvant le premier point.

Pour le deuxième, on fixe $S \in X$ et on considère la restriction à S de l'action de G sur X, qui n'est donc plus nécessairement transitive. La formule aux classes va donc dire des choses *a priori* non triviales.

Lemme 3.3

Soit H un p-groupe agissant sur un ensemble fini X. Soit $X^H = \{x \in X \ : \ \forall h \in H, \ h.x = x\}$ l'ensemble des points fixes de H. Alors $\sharp X \equiv \sharp X^H \bmod p$.

Dans la situation présente, $H = S$ et X est l'ensemble des p-Sylow de G. Un point fixe de l'action est donc un p-Sylow $T < G$ tel que pour tout $s \in S$, $sTs^{-1} = T$. La première observation évidente est que S lui-même vérifie ce critère. Étant donné un autre point fixe T, considérons $H = N_G(T) = \{g \in G \mid gTg^{-1} = T\}$ le normalisateur de T dans G. Notons que $S \cup T \subset H$. Puisque $H < G$, on en déduit que S et T sont des p-Sylow de H. D'après le Théorème 3.3 appliqué à H, on en déduit que S et T sont conjugués **dans** H. Or, par définition, $T \triangleleft H$. Puisque S est conjugué à T

dans H, on en déduit $S = T$. Ceci montre que S a un unique point fixe dans X, *i.e.* $X^S = \{S\}$. Le lemme ci-dessus nous donne alors $\sharp X \equiv 1 \bmod p$ comme annoncé. □

Exemple 3.1. Soit G un groupe d'ordre 63. Le nombre n_7 de ses 7-Sylow vérifie simultanément

— $n_7 | 9$

— $n_7 \equiv 1 \bmod 7$.

Ainsi, $n_7 = 1$ et G contient un unique 7-Sylow, qui est donc distingué d'après le Corollaire 3.1. Ainsi, un groupe d'ordre 63 ne peut pas être simple.

3.3 Classification des groupes d'ordre pq

Une application standard des théorèmes de Sylow est le résultat suivant sur les groupes dont l'ordre est produit de deux nombres premiers distincts.

Proposition 3.1

Soit G un groupe d'ordre pq, avec $p < q$ deux nombres premiers.

— Si p ne divise pas $q - 1$, alors $G \simeq \mathbf{Z}/pq\mathbf{Z}$ est cyclique.

— Si p divise $q - 1$, alors G est ou bien cyclique, ou bien de la forme

$$G \simeq (\mathbf{Z}/q\mathbf{Z}) \rtimes_\varphi (\mathbf{Z}/p\mathbf{Z})$$

où $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/q\mathbf{Z}) \simeq \mathbf{Z}/(q-1)\mathbf{Z}$ est non-trivial.

Si φ_1 et φ_2 sont deux tels morphismes, alors il existe un automorphisme $\psi \in \mathrm{Aut}(\mathbf{Z}/p\mathbf{Z})$ tel que $\varphi_2 = \varphi_1 \circ \psi$ et l'application

$$\begin{array}{ccc} (\mathbf{Z}/q\mathbf{Z}) \rtimes_{\varphi_1} (\mathbf{Z}/p\mathbf{Z}) & \to & (\mathbf{Z}/q\mathbf{Z}) \rtimes_{\varphi_2} (\mathbf{Z}/p\mathbf{Z}) \\ (x, y) & \mapsto & (x, \psi(y)) \end{array}$$

est un isomorphisme de groupes. En définitive, à isomorphisme près, il n'existe que deux structures possibles : la structure cyclique, ou la structure de produit semi-direct donnée par un quelconque tel φ.

3.4 Preuve élémentaire pour les groupes d'ordre 6.

On prouve que tout groupe d'ordre 6 *est isomorphe à* $\mathbf{Z}/6\mathbf{Z}$ *ou* $\mathfrak{S}_3$*, avec pour seul pré-requis le théorème de Lagrange.*

Soit G un groupe d'ordre 6. Alors, tout élément de G est d'ordre 1, 2, 3 ou 6. Notons que $G \simeq \mathbf{Z}/6\mathbf{Z}$ si et seulement si G contient un élément d'ordre 6. Supposons donc que tout élément est d'ordre 1, 2 ou 3 et montrons que G est isomorphe à $\mathfrak{S}_3$.

Si tous les éléments $\neq e$ sont d'ordre 2, alors G est abélien puisque $g = g^{-1}$ pour tout g dans G et donc $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$ pour tous $g, h \in G$. Soit alors $H = \langle h \rangle$ un sous-groupe engendré par un élément d'ordre 2. Puisque G est abélien, $H \triangleleft G$ et $|G/H| = 3$. Or pour tout $g \notin H$,$(gH)^2 = g^2H = H$ montrant que gH est d'ordre 2 dans G/H qui est d'ordre 3, une contradiction.

Donc, il existe un élément g d'ordre 3 dans G. Soit $H = \{e, h, h^2\}$ le sous-groupe qu'il engendre. Dans le complémentaire de H, il y a trois éléments. Supposons qu'il existe $g \notin H$ d'ordre 3. Nécessairement, $g^2 \notin H$ car sinon on aurait $g = g^4 = (g^2)^2 \in H$. Finalement, il reste un dernier élément $\tau \notin \langle h \rangle \cup \langle g \rangle$. Alors, τ est d'ordre 2 parce que sinon il serait d'ordre 3 et on ne pourrait avoir $\tau^2 \in \langle h \rangle \cup \langle g \rangle$ par le même argument que précédemment. Le sous-groupe $T = \langle \tau \rangle$ serait alors l'unique sous-groupe d'ordre 2 puisque τ serait l'unique élément d'ordre 2. On aurait donc $T \triangleleft G$. D'où $g\tau g^{-1} \in T$, et

donc $g\tau g^{-1} = \tau$ puisque $T = \{e, \tau\}$. Ainsi, g et τ commuterait et donc leur produit $g\tau$ serait d'ordre 6, contrairement à notre hypothèse.

Finalement, G contient un unique sous-groupe $C = \{e, c, c^2\}$ d'ordre 3, qui est nécessairement distingué par unicité. Le quotient G/C est d'ordre 2. Donc, si $\tau \notin C$, alors $G = C \sqcup \tau C$, avec $\tau^2 = e$. On a alors $\tau c\tau \in C$, d'où $\tau c\tau = c$ ou $\tau c\tau = c^2$. Mais dans le premier cas, c et τ commuteraient, et leur produit serait d'ordre 6 menant à la même contradiction. D'où $\tau c\tau = c^2$.

Au final, G est engendré par deux éléments c et τ d'ordre 3 et 2 respectivement et vérifiant la relation $\tau c\tau = c^2$, soit encore $\tau c = c^2\tau$. On reconnaît la présentation de $\mathfrak{S}_3$. On voit notamment que cette relation suffit à faire tous les calculs puisque tout élément de G est un mot formé sur les deux lettres $\{c, \tau\}$, et puisque $G = \{e, c, c^2, \tau, c\tau, c^2\tau\}$. Le groupe C correspond à $\langle(1\ 2\ 3)\rangle$ et les autres éléments aux transpositions. Par exemple $(c\tau)^2 = c\tau c\tau = cc^2 = e$ est bien d'ordre 2.

3.5 Un peu de botanique : groupes d'ordre au plus 15

Commençons par un bref aperçu. Soit G un groupe fini d'ordre n. On note k_n le nombre de structures de groupes à isomorphisme près. Il y a toujours la structure évidente, le groupe cyclique d'ordre n. Les exemples à ne pas perdre de vue : les groupes symétriques (ordre de la forme $k!$), alternés (ordres de la forme $k!/2$), les groupes diédraux (pour tous les ordres pairs).

Lorsque n est premier, c'est la structure cyclique est la seule par le théorème de Lagrange. Lorsque $n = p^2$, alors G est abélien et on est ramené au théorème de classification des groupes abéliens finis. Si $n = pq$, $p < q$, la Proposition 3.1 donne selon que p divise ou non $q - 1$ la structure cyclique ou une unique structure de produit semi-direct non abélien. Examinons les cas qu'il nous reste pour $n \leqslant 15$.

2. $n = 2$: G est cyclique., $k_2 = 1$.
3. $n = 3$: G est cyclique, $k_3 = 1$.
4. $n = 4$: G est cyclique ou isomorphe à $V_4 = \mathbf{Z}/2\mathbf{Z} \times Z/2\mathbf{Z}$, $k_4 = 2$.
5. $n = 5$: G est cyclique, $k_5 = 1$.
6. $n = 6$: G est cyclique ou isomorphe à $\mathfrak{S}_3$, $k_6 = 2$.
7. $n = 7$: G est cyclique, $k_7 = 1$.
8. $n = 8$: On a trois structures abéliennes et deux non-abéliennes, $\mathbf{H}_8$ et D_8, $k_8 = 5$. On va éclaircir ce point.
9. $n = 9$: G est abélien, donc isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ ou cyclique. $k_9 = 2$.
10. $n = 10$: comme 2 divise $4 = 5 - 1$, la proposition 3.1 implique que $k_{10} = 2$. Comme on a déjà le groupe cyclique et le groupe diédral D_{10}, ce sont les seules possibilités.
11. $n = 11$: G est cyclique.
12. $n = 12$: On a $k_{12} = 5$, éclairci ci-dessous.
13. $n = 13$: G est cyclique, $k_{13} = 1$.
14. $n = 14$: 2 divise $6 = 7 - 1$, d'où $G \simeq \mathbf{Z}/14\mathbf{Z}$ ou D_{14}. $k_{14} = 2$.
15. $n = 15$: 3 ne divise pas $4 = 5 - 1$, G est donc cyclique, $k_{15} = 1$.

Les deux cas épineux sont $n = 8$ et $n = 12$. Clarifions-les.

Proposition 3.2

À isomorphisme près, il existe cinq groupes d'ordre 8, dont trois abéliens

$$\mathbf{Z}/8\mathbf{Z}, \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}, \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

et deux non-abéliens, $\mathbf{H}_8$ et D_8.

Preuve. Le cas abélien est traité immédiatement. Il nous faut montrer qu'il n'y a que ces deux exemples dans le cas non abélien. Soit donc G un groupe non abélien d'ordre 8. Par le théorème de Lagrange, tout élément non trivial est d'ordre 2 ou 4 puisqu'on exclus le cas cyclique. Si tous les éléments étaient d'ordre 2, alors G serait abélien, ce qui est exclus. Il existe donc un élément d'ordre 4, disons g. Soit maintenant $h \notin \langle g \rangle$. Nous pouvons alors lister les éléments de G :

$$G = \{e, g, g^2, g^3, h, gh, g^2h, g^3h\}.$$

Première question : où est h^2 dans cette liste ? Premièrement, il ne peut pas être dans la deuxième moitié puisque si on avait $h^2 = g^k h$, alors on aurait $h = g^k$ ce qui est exclus. Ensuite, si on avait $h^2 = g$ ou $h^2 = g^3$, alors on aurait $h^4 = g^2 \neq e$ et h serait d'ordre 8, ce qui est exclus. Ainsi, ou bien $h^2 = e$, ou bien $h^2 = g^2$.

Même question pour hg. Cette fois, on a nécessairement $hg \in \{gh, g^2h, g^3h\}$. Or, si $hg = gh$, alors G serait abélien, ce qui est exclus. De plus si $hg = g^2h$, alors $hgh^{-1} = g^2$ ce qui est impossible puisque g est d'ordre 4 et g^2 d'ordre 2. Finalement, la seule possibilité est $hg = g^3h$

Cas $h^2 = e$. On flaire le groupe diédral (g correspondant aux rotations, et h à une symétrie). La deuxième observation se traduit de façon équivalente par $(hg)^2 = e$ puisque $g^3 = g^{-1}$ et $h = h^{-1}$. On reconnaît la présentation du groupe diédral.

Cas $h^2 = g^2$. Cette fois h est d'ordre 4. L'élément commun $z = h^2 = g^2$ est nécessairement central puisque $h^3 = hz = zh$ et $g^3 = gz = zg$ et $G = \langle g, h \rangle$. Cette fois-ci, on suspecte fortement $\mathbf{H}_8$ avec z jouant le rôle de -1, g celui de i et h celui de j. Mais dans ce cas k dois correspondre à gh. Nous voyons que $hg = g^3h = z(gh)$ et $(gh)^2 = ghgh = gg^3hh = h^2 = z$. On vérifie alors sans difficulté que $\Phi : \mathbf{H}_8 \to G$ donné par $\Phi(-1) = z$, $\Phi(i) = g$, $\Phi(j) = h$, $\Phi(k) = gh$ (les images des autres éléments suivent nécessairement) est un isomorphisme de groupes. □

Proposition 3.3
Soit G un groupe fini d'ordre 12. Alors, à isomorphisme près, il y a cinq possibilités pour G : deux groupes abéliens, à savoir $\mathbf{Z}/12\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ et trois groupes non abéliens : D_{12}, $\mathcal{A}_4$ et un produit semi-direct appelé groupe dicyclique d'ordre 12 (pour la culture, ce n'est pas dans les attendus du concours, c'est la stratégie de classification qui nous intéresse ici).

Preuve. Ici encore, le cas abélien est direct. On se donne donc un groupe G d'ordre 12 et non abélien. Le théorème de Sylow nous donne alors que $n_3 = 1$ ou 4 et $n_2 = 1$ ou 3.

Supposons que $n_3 = 4$. Alors, deux sous-groupes cycliques distincts et d'ordre premier ne s'intersectant que trivialement, on obtient que la réunion des 3-Sylow de G est formée de 9 éléments : le neutre et 8 éléments d'ordre 3. Dans le complémentaire il nous reste donc trois éléments. Or, le théorème de Sylow nous dit qu'il existe un sous-groupe d'ordre 4 (un 2-Sylow). Ses éléments non triviaux ne pouvant être d'ordre 3, ils sont dans le complémentaire en question et le remplissent entièrement. Conséquence : il n'y a qu'un seul 2-Sylow ($n_2 = 1$) et il est distingué. Appelons le N.

À ce stade, N est soit $\mathbf{Z}/4\mathbf{Z}$, soit V_4. Le quotient G/N est cyclique quant à lui, puisque d'ordre 3. Si H est un sous-groupe d'ordre 3 quelconque de G, alors $H \cap N = \{e\}$ et il se surjecte sur G/N. On a alors une section donnée par ce sous-

groupe, et $G \simeq N \rtimes_\varphi \mathbf{Z}/3\mathbf{Z}$, où $\varphi : \mathbf{Z}/3\mathbf{Z} \to \mathrm{Aut}(N)$ est non-trivial par hypothèse.

1. Si $N = \mathbf{Z}/4\mathbf{Z}$, alors $\mathrm{Aut}(N) \simeq \mathbf{Z}/2\mathbf{Z}$. Or il n'existe pas de morphisme non-trivial de $\mathbf{Z}/3\mathbf{Z}$ vers $\mathbf{Z}/2\mathbf{Z}$: ce cas ne se produit pas.
2. Si $N = V_4$, alors $\mathrm{Aut}(V_4) \simeq \mathfrak{S}_3$. Se donner un tel morphisme non trivial, c'est se donner un élément d'ordre 3 dans $\mathfrak{S}_3$, c'est-à-dire un 3-cycle. Comme tous les 3-cycles sont conjugués, on peut montrer que le résultat de l'opération de produit semi-direct est indépendant du choix de φ. Nous obtenons ainsi un premier exemple. Il se trouve que c'est le groupe $\mathcal{A}_4$ comme on peut le soupçonner avec l'apparition d'un sous-groupe V_4 correspondant aux double-transpositions. On peut s'en convaincre de la façon suivante :

   Considérons l'action par conjugaison de G sur $\mathrm{Syl}_3(G)$. Elle est transitive par le deuxième théorème de Sylow. Comme l'ensemble sur lequel agit G est de cardinal 4, et que G est d'ordre 12, le stabilisateur de tout point doit être d'ordre 3. Or, un point donné est un 3-Sylow S, donc le stabilisateur de ce point contient S (l'action de S par conjugaison sur G fixe S), donc est égal à S par cardinalité. Par conséquent, le noyau de l'action est l'intersection de tous les 3-Sylow, donc $\{e\}$. Le morphisme correspondant à l'action est alors un morphisme *injectif* $G \to \mathfrak{S}_4$. Ce dernier étant d'ordre 24, l'image de G est d'indice 2, elle est donc distinguée, et donc isomorphe à $\mathcal{A}_4$.

Rappelons que tout ceci se plaçait sous l'hypothèse $n_3 = 4$. Supposons maintenant que $n_3 = 1$, c'est-à-dire qu'il existe un sous-groupe $N \lhd G$ d'ordre 3. Cette fois, c'est le quotient G/N qui est d'ordre 4, donc isomorphe soit à $\mathbf{Z}/4\mathbf{Z}$, soit à V_4. Dans l'un ou l'autre des cas, si H est un 2-Sylow quelconque, $H \cap N = \{e\}$ pour des raisons d'ordre, et donc la projection π se restreint en un isomorphisme de H sur G/N, dont la réciproque est une section. Ainsi, $G \simeq N \rtimes_\varphi (G/N)$ pour une certaine loi de produit semi-direct. Notons que $\mathrm{Aut}(N) = \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z}) = \mathbf{Z}/2\mathbf{Z}$.

1. Supposons que G/N soit cyclique. Dans ce cas, la loi est décrite par un morphisme non-trivial $\varphi : \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$. Un tel φ est unique, donné par $\varphi(\overline{1}) = \varphi(\overline{3}) = \overline{1}$ et $\varphi(\overline{0}) = \varphi(\overline{2}) = \overline{0}$. L'unique structure est alors celle de $(\mathbf{Z}/3\mathbf{Z}) \rtimes_\varphi (\mathbf{Z}/4\mathbf{Z})$.
2. Supposons que $G/N \simeq V_4 = \{e, a, b, c\}$. Il s'agit de déterminer les morphismes non-triviaux $\varphi : V_4 \to \mathbf{Z}/2\mathbf{Z}$. Un tel φ est déterminé par son noyau, et inversement, un sous-groupe d'ordre 2 de V_4 déterminer un morphisme vers $\mathbf{Z}/2\mathbf{Z}$. Il y a donc 3 morphismes non-triviaux, dont les noyaux sont $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, et si φ_1, φ_2 sont de tels morphismes, alors il existe $\psi \in \mathrm{Aut}(V_4)$ tel que $\varphi_2 = \varphi_1 \circ \psi$. Rappelons que $\mathrm{Aut}(V_4) \simeq \mathfrak{S}_3$, qui correspond aux permutations de $\{a, b, c\}$. Pour les mêmes raisons qu'à la Proposition 3.1, les trois morphismes donnent des lois de produit semi-directes isomorphes.

Notons que ces deux dernières structures sont non isomorphes puisque la première contient un élément d'ordre 4, contrairement à la deuxième. Puisque D_{12} est dans cette liste, c'est nécessairement $D_{12} \simeq (\mathbf{Z}/3\mathbf{Z}) \rtimes_\varphi V_4$. Essayons de mieux comprendre pourquoi.

Dans les deux cas, $G = N \rtimes_\varphi H$, avec N cyclique d'ordre 3 et H d'ordre 4. Fixons $n \in N$ un générateur, et $h \in \mathrm{Ker}\,\varphi$, $h \neq e$. Alors par définition, $hnh^{-1} = n$ et donc $nh = hn$. Soit $N' = \langle nh \rangle$, c'est un sous-groupe cyclique d'ordre 6, nécessairement distingué dans G. On a alors une suite exacte courte

$$1 \to N' \to G \to \mathbf{Z}/2\mathbf{Z} \to 1.$$

C'est ici que les chemins se séparent :

— si $H = \mathbf{Z}/4\mathbf{Z}$, alors h est le seul élément d'ordre 2 de G (le vérifier explicitement), et donc il n'y a qu'une seule copie de $\mathbf{Z}/2\mathbf{Z}$ et elle est contenue dans N' : cette suite exacte courte n'est *pas* scindée.

— Si $H = V_4$, on choisit $k \in H$ tel que $\varphi(k) \neq \mathrm{id}_N$. Alors $k \notin N'$ et $k^2 = e$, le sous-groupe $H' = \{e, k\}$ vérifie bien $H' \cap N' = \{e\}$, et donc la suite exacte courte est scindée et $G \simeq (\mathbf{Z}/6\mathbf{Z}) \rtimes_{\varphi'} (\mathbf{Z}/2\mathbf{Z})$. La seule structure possible non-abélienne est celle de D_{12}, comme attendu (rappelons que $\mathrm{Aut}(\mathbf{Z}/6\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z}$, un seul φ' non-trivial possible donc).

Le cas H cyclique est celui du groupe dicyclique d'ordre 12. □

4 Groupes orthogonaux

4.1 Généralités

Soit q une forme quadratique sur un K-espace vectoriel de dimension finie E, de forme polaire b. On rappelle qu'on passe de l'une à l'autre via les formules de polarisation. La proposition suivante suit directement de la bilinéarité de b.

Proposition 4.1
Une forme quadratique q sur E, de forme polaire b, définit une application linéaire

$$\begin{array}{rccc} \varphi_b : & E & \to & E^* \\ & x & \mapsto & \ell_x \end{array}$$

où ℓ_x est la forme linéaire définie par $\ell_x(v) = b(x, v)$ pour tout $v \in E$.

Définition 4.1
On définit le **noyau** d'une forme quadratique q sur E par $\ker q := \ker \varphi_b$. Une forme quadratique est dite **non-dégénérée** si $\ker q = \{0\}$, *i.e.* si l'application φ_b réalise un isomorphisme de E sur E^*.

Ainsi, $\ker q = E^\perp = \{x \in E \ : \ \forall v \in E,\ b(x, v) = 0\}$.

Exercice 4.1
Étant donné un isomorphisme φ entre E et E^*, expliciter une forme bilinéaire b telle que $\varphi = \varphi_b$. Donner un exemple où b n'est pas symétrique.

Exercice 4.2
Montrer qu'une forme quadratique q induit une forme quadratique non-dégénérée sur l'espace quotient $E/\ker q$.

Exemple 4.1.
1. Le noyau de la forme quadratique sur $E = K^2$ donnée par $q(x) = x_1^2$ est la droite $\{x_1 = 0\}$.
2. Si $K = \mathbf{R}$ et b est un produit scalaire euclidien, alors q est non-dégénérée.
3. Sur $E = \mathbf{R}^3$, la forme quadratique $q(x) = x_1^2 + x_2^2 - x_3^2$ est non-dégénérée.
4. Sur $E = M_n(\mathbf{R})$, la forme quadratique $q(M) = \mathrm{Tr}(M^2)$ est non-dégénérée.

Définition 4.2

Soit $e = (e_1, \ldots, e_n)$ une base de E. On définit la matrice de q relativement à e la matrice $M_e(q) = (b(e_i, e_j))_{ij}$. On note que c'est une matrice symétrique.

Remarque 4.1. La matrice de q est la matrice de l'application linéaire $\varphi_b : E \to E^*$, avec (e_i) pour base de départ et sa *base duale* (e_i^*) pour base d'arrivée.

Proposition 4.2

Si $X, Y \in K^n$ sont les vecteurs coordonnées dans la base e de $x, y \in E$ respectivement, et si M est la matrice de q dans cette même base, alors $b(x, y) = {}^tXMY$.

Si P est la matrice de passage vers une autre base $f = (f_1, \ldots, f_n)$ de E, alors la matrice se transforme en $M_f(b) = {}^tPM_e(b)P$. Rappelons que c'est ce qui conduit à la

Définition 4.3

Deux matrices symétriques $M, N \in \mathcal{M}_n(K)$ sont dit **congruentes** s'il existe $P \in \mathrm{GL}_n(K)$ telle que $N = {}^tPMP$.

Passons maintenant à la définition des groupes orthogonaux. Notez bien que nous sommes toujours dans un cadre très général (K est quelconque, pas d'hypothèse sur la forme quadratique q).

Définition 4.4

Étant donnée une forme quadratique q sur E, on définit son **groupe orthogonal**, noté $O(q)$, comme étant le sous-groupe de $\mathrm{GL}(E)$ défini par

$$O(q) = \{u \in \mathrm{GL}(E) \mid \forall x \in E,\ q(u(x)) = q(x)\}.$$

Remarque 4.2. Ceci recoupe la définition du groupe orthogonal euclidien $O(n)$ qui est le groupe orthogonal de la forme quadratique $q(x) = \sum x_i^2$ sur $E = \mathbf{R}^n$, une fois qu'on a identifié $\mathrm{GL}(\mathbf{R}^n)$ et $\mathrm{GL}_n(\mathbf{R})$ via la base canonique de $\mathbf{R}^n$.

Remarque 4.3. On note que pour tout $u \in \mathrm{GL}(E)$ et toute base e de E, on a $u \in O(q)$ si et seulement si $M_e(u)M_e(q)\,{}^tM_e(u) = M_e(q)$.

Cône isotrope, plans hyperboliques, théorème de Witt

On pourra consulter le Ch. VIII de [Per96] pour plus de détails. On suppose que le corps de base K est de caractéristique différente de 2.

Définition 4.5

Soit (E, q) un K-espace vectoriel muni d'une forme quadratique q. On dit qu'un vecteur $x \in E$ est isotrope si $q(x) = 0$. On dit qu'un sous-espace vectoriel $F \subset E$ est totalement isotrope si $\forall x \in F$, $q(x) = 0$.

L'ensemble des vecteurs isotropes de (E, q) n'est pas un sous-espace vectoriel en général. C'est un cône, c'est-à-dire stable par multiplication par un scalaire.

Définition 4.6

On dit qu'un plan P muni d'une forme quadratique q est un plan hyperbolique s'il

existe une base $\mathcal{B} = (e_1, e_2)$ de P dans laquelle

$$\mathrm{Mat}_{\mathcal{B}}(q) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On notera que les droites $K.e_1$ et $K.e_2$ sont isotropes et que si (x_1, x_2) sont les coordonnées dans la base (e_1, e_2), alors $q(x) = 2x_1x_2$. De façon équivalente, un plan (P, q) est hyperbolique si et seulement s'il contient deux droites isotropes et non orthogonales.

Lemme 4.1

Soit (E, q) un K-espace vectoriel muni d'une forme quadratique q non-dégénérée. Soit $x \in E$ un vecteur isotrope non-nul. Alors, il existe un plan $P \subset E$ tel que $(P, q|_P)$ est hyperbolique.

Preuve. Soit $b(.,.)$ la forme polaire de q. Alors, puisque q est non-dégénérée, il existe $y \in E$ tel que $b(x, y) \neq 0$. Quitte à renormaliser y, nous pouvons supposer $b(x, y) = 1$. De plus, y ne peut pas être colinéaire à x, sans quoi on aurait $b(x, y) = 0$. Ainsi, $P = \mathrm{Vect}(x, y)$ est un plan. En prenant $z = y - \frac{q(y)}{2}x$, on a $q(z) = 0$ et (x, z) est une base de P dans laquelle la matrice de q se met sous la forme attendue. □

Proposition 4.3

Soit $F \subset E$ un sous-espace totalement isotrope de dimension k. Alors, il existe des plans hyperboliques $P_1, \ldots, P_k$, deux-à-deux orthogonaux, et tels que $F \subset P_1 \oplus \cdots \oplus P_k$.

Démonstration. [Per96], Ch. VIII, Cor. 3.5. □

Remarque 4.4. La somme $P_1 \oplus \cdots \oplus P_k$ est un sous-espace non-dégénéré, donc en somme directe avec son orthogonal.

Théorème 4.1 (Witt)

Soit (E, q) un espace quadratique. Soient $F, F' \subset E$ deux sous-espaces tels qu'il existe une isométrie linéaire $v : (F, q|_F) \to (F', q|_{F'})$, c'est à dire que $v : F \to F'$ est une application linéaire vérifiant $q(v(x)) = q(x)$ pour tout $x \in F$. Alors, il existe $u \in O(q)$ tel que $v = u|_F$.

Démonstration. [Per96], Ch. VIII, Th. 4.3. □

Corollaire 4.1

Soient $F, F' \subset E$ deux sous-espaces. Alors,

$$\exists u \in O(q) \mid u(F) = F' \iff q_F \text{ et } q_{F'} \text{ sont équivalentes.}$$

La deuxième condition signifiant concrètement qu'on peut trouver des bases de F et F' dans lesquelles la matrice de la restriction de q est la même.

Définition 4.7

Un sous-espace totalement isotrope maximal est un sous-espace $F \subset E$ totalement isotrope maximal pour cette propriété, *i.e.* tel que pour tout F' totalement isotrope, si $F \subset F'$, alors $F = F'$.

Corollaire 4.2

Tous les sous-espaces totalement isotropes maximaux (SETIM) de (E, q) ont la même dimension $\nu(q)$, l'indice de la forme quadratique.

En appliquant la proposition 4.3 à un SETIM de E, on obtient que E est somme orthogonale de $\nu(q)$ plans hyperboliques et d'un sous-espace anisotrope G.

4.2 Formes quadratiques sur un espace complexe

Théorème 4.2

À congruence près, il n'existe qu'une seule forme quadratique non-dégénérée sur un espace vectoriel complexe de dimension finie. Cela revient à dire qu'on peut trouver des coordonnées complexes dans lesquelles elle s'écrit $z_1^2 + \cdots + z_n^2$.

Rappelons que si q est une forme quadratique non-dégénérée sur un K-espace E, et si $F \subset E$ est un sous-espace de E tel que $q|_F$ est non-dégénérée, alors $E = F \oplus F^\perp$. Ceci est automatique quand E est réel et q définie positive mais pas en général.

Exercice 4.3

Donner des exemples où q est non-dégénérée et $F \cap F^\perp \neq \{0\}$.

Preuve. La preuve peut alors facilement se faire par récurrence sur $n := \dim E \geqslant 1$. L'initialisation est immédiate. Supposons maintenant l'hypothèse au rang n, c'est à dire que pour tout F de dimension n, et toute forme quadratique q' non-dégénérée sur F, il existe une base $\mathcal{B}$ de F dans laquelle q' s'écrit $z_1^2 + \cdots + z_n^2$. Soit maintenant E de dimension $n+1$ et soit q une forme quadratique non-dégénérée sur E. Comme q est non-dégénérée, elle est non-nulle et il existe $x \in E$ tel que $q(x) \neq 0$. Ainsi, la restriction de q à la droite $\mathbf{C}.x$ est non-dégénérée, et donc, si $H = (\mathbf{C}.x)^\perp$, alors on a $E = \mathbf{C}.x \oplus H$ et la somme directe est orthogonale. D'après l'hypothèse de récurrence, il existe une base $(e_1, \ldots, e_n)$ de H telle que $b(e_i, e_j) = \delta_{ij}$, pour tous $1 \leqslant i, j \leqslant n$, où b est la forme polaire de q. Comme $q(x) \neq 0$, on peut choisir $\lambda \in \mathbf{C}$ tel que $\lambda^2 = q(x)$ et poser $e_0 = x/\lambda$. La base $(e_0, \ldots, e_n)$ convient pour (E, q), ce qui achève la récurrence. □

Exercice 4.4

Expliciter un changement de coordonnées adéquat pour la forme quadratique $2z_1z_2 + z_3^2$.

4.3 Formes quadratiques sur un espace réel, signature

Un espace euclidien est un espace vectoriel **réel** E de **dimension finie** muni d'un **produit scalaire**, c'est à dire une forme bilinéaire $\langle ., . \rangle$ qui est symétrique, définie et positive. On note $\|.\|$ la norme sur E qui dérive de ce produit scalaire.

Plus généralement, on peut considérer un espace *pseudo-euclidien*, c'est à dire un espace vectoriel réel E muni d'une forme quadratique q non-dégénérée, dont on note (p, q) la signature. On a donc $p + q = \dim E$.

Point algèbre linéaire : connaissant l'expression des coordonnées dans la nouvelle base, comment retrouver cette base ? Donc faire le lien entre la matrice de passage dans E et celle entre les bases duales correspondantes.

Proposition 4.4
$O(q)$ est compact si et seulement si q est définie positive ou négative.

La preuve ne présente pas de grosse difficulté et est laissée en exercice. Penser à appliquer la proposition 4.3.

Rappelons le théorème d'inertie de Sylvester qui permet de définir la signature des formes quadratiques sur un espace vectoriel réel. On le formule volontairement dans le langage des actions de groupes.

Théorème 4.3 (Théorème d'inertie de Sylvester)
On note $\mathcal{S}_n(\mathbf{R})$ l'espace des matrices symétriques réelles de taille $n \geqslant 1$. Considérons l'action par congruence

$$\begin{array}{rcl} \mathrm{GL}_n(\mathbf{R}) \times \mathcal{S}_n(\mathbf{R}) & \to & \mathcal{S}_n(\mathbf{R}) \\ (P, S) & \mapsto & PM\,{}^tP. \end{array}$$

Soit $\Sigma = \{(p,q,r) \in \mathbf{N}^3 \mid p+q+r = n\}$. Alors, l'ensemble

$$\left\{ \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & \mathbf{0}_r \end{pmatrix},\ (p,q,r) \in \Sigma \right\} \subset \mathcal{S}_n(\mathbf{R})$$

est un système de représentants des orbites de $\mathrm{GL}_n(\mathbf{R})$ sur $\mathcal{S}_n(\mathbf{R})$.

Définition 4.8
Soit q une forme quadratique sur $\mathbf{R}^n$. Sa signature est l'unique $(p,q,r) \in \Sigma$ tel que pour toute base $\mathcal{B}$ de $\mathbf{R}^n$, $\mathrm{Mat}_{\mathcal{B}}(q)$ est dans la $\mathrm{GL}_n(\mathbf{R})$-orbite de la matrice $\mathrm{diag}(I_p, -I_q, \mathbf{0}_r)$.

Remarque 4.5. Bien-sûr, cette formulation est strictement équivalente à la classique, qui dit qu'il existe un changement linéaire de coordonnées (pas unique) qui permet d'écrire $q(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$.

Remarque 4.6. La forme quadratique est non-dégénérée si et seulement si $r = 0$. Dans ce cas, on raccourcira en disant que la forme quadratique est de signature (p,q) (et non $(p,q,0)$).

Définition 4.9
Soient $n \geqslant 1$ et $p, q \geqslant 0$ tels que $p+q = n$. On définit

$$O(n) = \left\{ M \in \mathrm{GL}_n(\mathbf{R}) \mid M\,{}^tM = I_n \right\}$$

et

$$O(p,q) = \left\{ M \in \mathrm{GL}_n(\mathbf{R}) \mid M I_{p,q}\,{}^tM = I_{p,q} \right\}$$

où

$$I_{p,q} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}.$$

On notera que $O(n,0) = O(0,n) = O(n)$.

Exercice 4.5
Interpréter ces groupes dans le contexte de l'action de groupe précédente.

Exercice 4.6
Vérifier que si Q est une forme quadratique non-dégénérée sur $\mathbf{R}^n$, de signature (p, q), alors son groupe orthogonal $O(Q)$ est conjugué à $O(p, q)$.

Proposition 4.5
Le groupe orthogonal $O(n)$ a deux composantes connexes, qui sont $\mathrm{SO}(n) = O(n) \cap \mathrm{SL}_n(\mathbf{R})$ et $O(n) \setminus \mathrm{SO}(n)$.

Preuve. On notera déjà que pour toute $M \in O(n)$, on a $|\det(M)| = 1$ et que $O(n) \not\subseteq \mathrm{SL}_n(\mathbf{R})$. Ainsi, $\det|_{O(n)} : O(n) \to \{\pm 1\}$ est surjective et continue. Il y a donc au moins deux composantes connexes. De plus, $\mathrm{SO}(n)$ est d'indice 2 dans $O(n)$.

Vérifions que $\mathrm{SO}(n)$ est connexe. Pour cela, il y a différentes approches. On renvoie à [MT97] (Ch. 4) pour une approche très géométrique qui s'appuie sur la connexité de la sphère $\mathbf{S}^n$. Nous allons plutôt utiliser le Théorème 4.8 ci-dessous (indépendant de ce résultat). Toute matrice $A \in \mathrm{SO}(n)$ diagonalise par bloc comme dans l'énoncé. Puisque $\det(A) = 1$, il y a un nombre pair de ε_k qui valent -1. Ainsi, en regroupant les -1 par paires, il existe $P \in O(n)$ telle que

$$PAP^{-1} = \begin{pmatrix} I_k & & & & & & \\ & R_\pi & & & & & \\ & & \ddots & & & & \\ & & & R_\pi & & & \\ & & & & R_{\theta_1} & & \\ & & & & & \ddots & \\ & & & & & & R_{\theta_\ell} \end{pmatrix}$$

En notant pour $t \in [0, 1]$

$$A_t = P^{-1} \begin{pmatrix} I_k & & & & & & \\ & R_{\pi t} & & & & & \\ & & \ddots & & & & \\ & & & R_{\pi t} & & & \\ & & & & R_{\theta_1 t} & & \\ & & & & & \ddots & \\ & & & & & & R_{\theta_\ell t} \end{pmatrix} P,$$

$(A_t)_{t\in[0,1]}$ est un chemin continu dans $\mathrm{SO}(n)$ tel que $A_0 = I_n$ et $A_1 = A$, ce qui montre que $\mathrm{SO}(n)$ est connexe par arc.

Comme $|O(n)/\mathrm{SO}(n)| = 2$, on a $O(n) = \mathrm{SO}(n) \sqcup g\,\mathrm{SO}(n)$ pour tout $g \in O(n)$ tel que $g \notin \mathrm{SO}(n)$ (une réflexion quelconque par exemple). Le produit matriciel étant continu, $g\,\mathrm{SO}(n)$ est également connexe, ce qui montre que $O(n)$ est la réunion disjointe de deux parties connexes, qui sont donc ses composantes connexes, d'où le résultat. □

On peut décrire, par analogie avec le cas défini positif, le groupe orthogonal d'une forme quadratique de signature $(1, 1)$:

Exercice 4.7

Montrer par un calcul explicite que le groupe $O(1,1)$ a quatre composantes connexes que l'on décrira.

Vérifier que la composante de l'identité est le sous-groupe des *rotations hyperboliques* qui, dans une base où la forme quadratique s'écrit $q(x_1,x_2)=x_1^2-x_2^2$, se met sous la forme :

$$O(1,1)_0=\left\{\begin{pmatrix}\cosh(t) & \sinh(t)\\ \sinh(t) & \cosh(t)\end{pmatrix},\ t\in\mathbf{R}\right\}.$$

Proposition 4.6

Le centre de $O_n(\mathbf{R})$ est $\{\pm I_n\}$.

Preuve. Soit $A\in\mathcal{Z}(O_n(\mathbf{R}))$. Soit $\Delta\subset\mathbf{R}^n$ une droite vectorielle et soit $X\in\Delta$ un vecteur unitaire de Δ (pour le produit scalaire euclidien standard). Soit B la matrice dans la base canonique de la réflexion orthogonale par rapport à $H=X^\perp$. Concrètement, elle peut être donnée par PDP^{-1} où $P\in O_n(\mathbf{R})$ est telle que $Pe_1=X$ (une telle matrice existe car X est normé) et

$$D=\begin{pmatrix}-1 & 0\\ 0 & I_{n-1}\end{pmatrix}.$$

Comme $\mathrm{Ker}(B+\lambda I_n)=\Delta$, nous avons $A\Delta=\Delta$, et ceci pour toute droite vectorielle de $\mathbf{R}^n$. On utilise alors le résultat général suivant (à retenir).

Lemme 4.2

Soit E un espace vectoriel sur un corps K quelconque. Soit $u\in\mathcal{L}(E)$ un endomorphisme stabilisant toute droite vectorielle de E. Alors, il existe $\lambda\in K$ tel que $u=\lambda\,\mathrm{id}_E$.

Preuve. Pour tout $x\in E$, nous avons donc $\lambda_x\in K$ tel que $u(x)=\lambda_x x$. Notons que λ_x est unique pour $x\neq 0$. Soient maintenant $x,y\in E$ non-nuls.

1. S'ils sont proportionnels, alors il existe $\mu\in K$ tel que $y=\mu x$, et on a $\lambda_y y=u(y)=\mu u(x)=\mu\lambda_x x=\lambda_x y$. D'où $\lambda_y=\lambda_x$.
2. S'ils sont non-proportionnels, considérons $z=x+y$. Alors, $u(z)=\lambda_z z=u(x)+u(y)=\lambda_x x+\lambda_y y$, d'où $\lambda_z=\lambda_x=\lambda_y$ puisque la famille (x,y) est libre.

Dans tous les cas, $\lambda_x=\lambda_y$, il existe donc $\lambda\in K$ tel que $u(x)=\lambda x$ pour tout $x\in E$. □

Ainsi, A est nécessairement une homothétie de rapport $\lambda\in\mathbf{R}^*$. Comme $A\in O_n(\mathbf{R})$, on doit avoir $\lambda=\pm 1$, et inversement, $\pm I_n\in\mathcal{Z}(O_n(\mathbf{R}))$. D'où $\mathcal{Z}(O_n(\mathbf{R}))=\{\pm I_n\}$. □

Plus généralement :

Proposition 4.7

Le centre de $O(p,q)$ est $\{\pm I_n\}$.

Preuve. On procède comme dans le cas défini positif. Soit b une forme bilinéaire non-dégénérée de signature (p, q) sur $\mathbf{R}^n$, soit G son groupe orthogonal. On se donne $\Delta \subset \mathbf{R}^n$ une droite vectorielle et il s'agit de construire un élément $g \in G$ tel que Δ est une droite propre de g. On distingue deux cas :

1. Δ est non-isotrope. Dans ce cas, $\mathbf{R}^n = \Delta \oplus \Delta^\perp$ [a]. On définit alors g comme étant l'endomorphisme tel que pour tout $x \in \Delta$, $g(x) = -x$ et pour tout $y \in \Delta^\perp$, $g(y) = y$, alors $g \in G$ et $\Delta = E_{-1}(g)$.
2. Δ est isotrope. Dans ce cas, fixons $e_1 \in \Delta$ non-nul. D'après le Lemme 4.1, il existe $e_2 \in \mathbf{R}^n$ isotrope tel que $b(e_1, e_2) = 1$. Le plan $P = \mathrm{Vect}(e_1, e_2)$ est alors non-dégénéré de signature $(1, 1)$ et $\mathbf{R}^n = P \oplus P^\perp$. On complète (e_1, e_2) en une base $\mathcal{B} = (e_1, e_2, \ldots, e_n)$ telle que $(e_3, \ldots, e_n)$ est une base de $P^\perp$. On définit $g \in \mathcal{L}(\mathbf{R}^n)$ comme étant l'endomorphisme tel que

$$\mathrm{Mat}_{\mathcal{B}}(g) = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda^{-1} & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix},$$

   avec $|\lambda| \notin \{0, 1\}$ quelconque. On a alors $g \in G$ et $E_\lambda(g) = \Delta$.

Ainsi, tout élément $h \in \mathcal{Z}(G)$ doit commuter à l'élément g que l'on vient de construire, et doit donc préserve la droite Δ. Par le Lemme 4.2, on en déduit que h est scalaire, et comme dans le cas défini positif, que $h \in \{\pm \mathrm{id}\}$. L'autre inclusion étant à nouveau évidente, ceci conclut la preuve. □

a. Lorthogonal est pris relativement à b.

Exercice 4.8

Combien de composantes connexes y a-t-il dans le groupe $O(2, 1)$ muni de la topologie induite par celle d'espace vectoriel normé de $M_3(\mathbf{R})$?

4.4 Cas défini positif

On rappelle dans un espace euclidien $(E, \langle , \rangle)$, on a la notion d'*adjoint* d'un endomorphisme : pour tout $u \in \mathcal{L}(E)$, il existe un unique $u^* \in \mathcal{L}(E)$, appelé adjoint de u, tel que

$$\forall x, y \in E,\ \langle u(x), y\rangle = \langle x, u^*(y)\rangle.$$

Un endormophisme est dit auto-adjoint si $u = u^*$, et, en notant q la forme quadratique $q(x) = \langle x, x\rangle$, on a $u \in O(q) \iff uu^* = u^*u = \mathrm{id}_E$.

Ceci s'interprète matriciellement : l'adjoint de u est l'endomorphisme caractérisé par $\mathrm{Mat}_{\mathcal{B}}(u^*) = {}^t\mathrm{Mat}_{\mathcal{B}}(u)$ pour toute base orthonormée $\mathcal{B}$ de E.

Un endomorphisme auto-adjoint $u \in \mathcal{L}(E)$ est dit défini positif si $\forall x \in E \setminus \{0\}$, $\langle u(x), x\rangle > 0$. Ceci revient à dire que la forme quadratique $q_u(x) = \langle u(x), x\rangle$ est définie positive.

Exercice 4.9

Montrer qu'inversement, étant donnée une forme quadratique définie positive q' sur E, il existe un endomorphisme auto-adjoint $u \in \mathcal{L}(E)$, défini et positif, tel que $q' = q_u$.

Théorème 4.4

Tout endomorphisme auto-adjoint u d'un espace euclidien E est diagonalisable en base orthonormée.

Preuve. Le point de départ est le suivant. Il permet de faire une récurrence sur la dimension de l'espace en nous restreignant à l'orthogonal d'un espace propre non-nul.

Lemme 4.3

Toutes les valeurs propres de u sont réelles.

Preuve. On considère une matrice M de u par rapport à une base orthonormée arbitraire et on considère $\lambda \in \mathrm{Sp}_{\mathbf{C}}(u)$ une valeur propre complexe de u. On a alors existence de $X \in \mathbf{C}^n \setminus \{0\}$ tel que $MX = \lambda X$. Nous avons alors d'une part ${}^t\overline{X}MX = \lambda\, {}^t\overline{X}X$, et d'autre part ${}^t\overline{X}MX = {}^t({}^t\overline{X}MX)$, puisque Mest symétrique à coefficients réels. On en déduit $\lambda = \overline{\lambda}$ puisque $X \neq 0 \Rightarrow {}^t\overline{X}X > 0$. □

On pour par récurrence sur $n \geqslant 1$ la propriété $\mathcal{P}(n)$: "Pour tout espace euclidien E de dimension n, tout endomorphisme autoadjoint de E est diagonalisable en base orthonormée."

Initialisation : Immédiate.

Hérédité : Soit $n > 1$. Supposons $\mathcal{P}(n-1)$ et montrons la propriété au rang n. Soit E un espace euclidien de dimension n et soit u un endomorphisme auto-adjoint de E. Par le lemme, u admet une valeur propre réelle, dont on peut choisir un vecteur propre $v \in E\setminus\{0\}$. Puisque u est auto-adjoint et préserve $\mathbf{R}.v$, il préserve l'hyperplan $H = v^{\perp}$. On applique l'hypothèse de récurrence à la restriction $u|_H$ (qui est auto-adjoint) : il existe $(e_1, \ldots, e_{n-1})$ une base orthonormée de H formée de vecteurs propres. Par construction, $(e_1, \ldots, e_{n-1}, v)$ est une base orthonormée de E formée de vecteurs propres, ce qui termine la récurrence. □

On note $\mathcal{S}_n(\mathbf{R})$ le sous-espace des matrices symétriques de $M_n(\mathbf{R})$ et $\mathcal{S}_n^{++}(\mathbf{R}) \subset \mathcal{S}_n(\mathbf{R})$ l'ensemble des matrices symétriques définies positives. Ce n'est pas un sous-espace vectoriel, mais un cône convexe.

Exercice 4.10

Démontrer que la restriction de l'application exponentielle à $\mathcal{S}_n(\mathbf{R})$ est un homéomorphisme $\exp|_{\mathcal{S}_n(\mathbf{R})} : \mathcal{S}_n(\mathbf{R}) \to \mathcal{S}_n^{++}(\mathbf{R})$. (On pourra expliciter son inverse.)

Théorème 4.5 (Décomposition polaire)

Pour toute matrice $M \in \mathrm{GL}_n(\mathbf{R})$, il existe un unique couple $(S, N) \in \mathcal{S}_n^{++}(\mathbf{R}) \times O_n(\mathbf{R})$ tel que $M = SN$.

De plus, l'application $\phi : (S, N) \in \mathcal{S}_n^{++}(\mathbf{R}) \times O_n(\mathbf{R}) \mapsto SN \in \mathrm{GL}_n(\mathbf{R})$ est un homéomorphisme.

Démonstration. On renvoie à [CG13], Ch. 5. □

Lien avec la forme polaire des nombres complexes.

Ce résultat est à comparé à la forme polaire d'un nombre complexe non nul : pour tout $z \in \mathbf{C}^*$, il existe un unique $(\rho, u) \in \mathbf{R}_+^* \times \mathbf{U}$ tel que $z = \rho u$, où $\mathbf{U} = \{z \in \mathbf{C} \mid |z| = 1\} = \{e^{i\theta},\ \theta \in \mathbf{R}\}$. Par analogie, $\mathbf{R}_+^*$ joue le rôle de $\mathcal{S}_n^{++}(\mathbf{R})$ et $\mathbf{U}$ celui de $O_n(\mathbf{R})$.

Ceci s'observe concrètement pour $n = 2$ en identifiant $\mathbf{C}$ avec les matrices de similitudes. Rappelons que l'application

$$\begin{array}{rccc} \Phi : & \mathbf{C} & \to & M_2(\mathbf{R}) \\ & a+ib & \mapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array}$$

est un morphisme d'anneaux, continu, dont l'image, notée $\mathrm{Sim}(\mathbf{R}^2)$, est formée des matrices de similitude. On notera que $\Phi(\overline{z}) = {}^t\Phi(z)$ et $\det \Phi(z) = |z|^2$ pour tout $z \in \mathbf{C}$, et notamment $\mathrm{Sim}(\mathbf{R}^2) \setminus \{0\} = \Phi(\mathbf{C}^*) \subset \mathrm{GL}_2(\mathbf{R})$. Pour $z = a + ib \in \mathbf{C}^*$, le couple (S, N) donné par le théorème 4.5 est alors

$$S = \begin{pmatrix} |z| & 0 \\ 0 & |z| \end{pmatrix} \text{ et } N = \frac{1}{|z|}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in O_2(\mathbf{R}).$$

Théorème 4.6

Tout sous-groupe compact de $\mathrm{GL}_n(\mathbf{R})$ est conjugué à un sous-groupe de $O_n(\mathbf{R})$.

(On pourra consulter [Ale99].)

Définition 4.10

Soit $v \in E \setminus \{0\}$. On appelle réflexion orthogonale par rapport à v la symétrie s_v selon l'hyperplan $H = v^\perp$ et parallèlement à $D = \mathbf{R}.v$.

Comme son nom l'indique, c'est un élément du groupe orthogonal $O(E)$. De plus, on a l'expression suivante très commode en pratique :

$$s_v(x) = x - 2\frac{\langle x, v\rangle}{\langle v, v\rangle}v.$$

Théorème 4.7

Le groupe $O(E)$ est engendré par les réflexions orthogonales. En fait, on peut se restreindre à au plus $\dim E$ réflexions.

Preuve. [Per96], Chap. 4, Th. 2.4. □

Remarque 4.7. Lorsque $\dim E = 2$, nous avons déjà vu au §**ref** que tout élément de $O(E)$ est soit une rotation, soit une symétrie. On sait que la composée de deux symétries est une rotation (signe du déterminant). La proposition 4.11 ci-dessous montre bien que les symétries (qui son les réflexions en dimension 2) engendrent $O(2)$ et que tout élément est produit de une (symétrie) ou deux réflexions (rotation).

Exercice 4.11

Montrer que $O(E)$ agit transitivement sur la grassmanienne. Est-ce vrai dans d'autres signatures ?

Théorème 4.8

Tout endomorphisme orthogonal est diagonalisable sur $\mathbf{C}$ avec des valeurs propres de module 1. Ce qui signifie pour tout $u \in O(E)$, il existe une base orthonormée $\mathcal{B}$

de E telle que

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \varepsilon_1 & & & & & \\ & \ddots & & & & \\ & & \varepsilon_k & & & \\ & & & R_{\theta_1} & & \\ & & & & \ddots & \\ & & & & & R_{\theta_\ell} \end{pmatrix}$$

où $\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}$ et $R_{\theta_1}, \ldots, R_{\theta_\ell}$ sont des rotations dans les plans correspondants de la base.

Cas des endomorphismes normaux et semi-simples

Définition 4.11

On appelle endomorphisme normal d'un espace euclidien E tout endomorphisme u qui commute à son adjoint u^*.

Cette définition englobe plusieurs situations déjà rencontrées : les endomorphismes auto-adjoints, les endomorphismes orthogonaux ainsi que les endomorphismes "anti-adjoint", *i.e.* vérifiant $u^* = -u$ sont des cas spéciaux d'endomorphismes normaux.

Définition 4.12

Un endomorphisme d'un espace vectoriel E sur un corps quelconque K est dit *semi-simple* si tout sous-espace stable admet un supplémentaire stable.

Nous renvoyons à [CL05] pour plus de détails. Nous retiendrons ici le fait suivant.

Proposition 4.8

Si K est de caractéristique nulle, alors un endomorphisme de E est semi-simple si et seulement s'il est diagonalisable sur une extension de K.

Pour éviter de parler d'extension des scalaires, on pourra se contenter de penser aux matrices à coefficients dans K. Cette proposition nous dit qu'il existe une extension L de K telle que toute matrice d'un endomorphisme semi-simple de E est diagonalisable dans $M_n(L)$.

Théorème 4.9

Soit E un espace euclidien. Alors, tout endormorphisme normal $u \in \mathcal{L}(E)$ est semi-simple. Il est donc diagonalisable sur $\mathbf{C}$ et se met sous la forme

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_k & & & \\ & & & S_1 & & \\ & & & & \ddots & \\ & & & & & S_\ell \end{pmatrix}$$

où $\lambda_1, \ldots, \lambda_k \in \mathbf{R}$ et $S_1, \ldots, S_\ell$ sont des matrices de similitudes :

$$\forall r \in \{1, \ldots, \ell\},\ S_r = \begin{pmatrix} a_r & -b_r \\ b_r & a_r \end{pmatrix}$$

Exercice 4.12
Trouver une matrice de passage complexe qui transforme la matrice de l'endomorphisme normal du théorème précédent en une matrice complexe diagonale.

Théorème 4.10
Le groupe $\mathrm{SO}_3(\mathbf{R})$ est simple. Plus généralement, $\mathrm{PSO}_n(\mathbf{R})$ est simple pour $n \geqslant 5$.

Rappelons que $\mathrm{PSO}_n(\mathbf{R})$ est défini comme le quotient de $\mathrm{SO}_n(\mathbf{R})$ par son centre, soit concrètement

$$\mathrm{PSO}_n(\mathbf{R}) = \begin{cases} \mathrm{SO}_n(\mathbf{R}) & \text{si } n \text{ est impair,} \\ \mathrm{SO}_n(\mathbf{R})/\{\pm I_n\} & \text{si } n \text{ est pair.} \end{cases}$$

Remarque 4.8. Pourquoi quotiente-t-on par le centre ?

Preuve. [Per96], Ch. 4, §6 §7. □

Le cas $n = 4$ est une exception remarquable, qui peut-être expliquée par l'existence d'une structure algébrique au moins tout aussi remarquable sur un espace euclidien de dimension 4.

4.5 Utilisation des quaternions en dimension 3 et 4

4.5.1 Retour sur l'orientation

Déterminants par rapport à une base comme forme n linéaire alternée.

Définition 4.13
Une **orientation** sur un espace vectoriel réel de dimension finie égale à n est la donnée d'une classe d'équivalence de bases de cet espace, pour la relation $(e_i) \sim (f_i) \iff \det_{(e_i)}(f_1, \ldots, f_n) > 0$.

Noter qu'en général, $\det_{(e_i)}(f_1, \ldots, f_n) \in \mathbf{R}^*$, et qu'il y a deux classes d'équivalence données par le signe de ce déterminant. Cette définition revient donc à choisir de façon cohérente quelles sont les bases positivement orientées, et quelles sont celles qui sont négativement orientées.

Soit maintenant E un espace euclidien muni d'une orientation. On peut distinguer ses bases orthonormées directes et ses bases orthonormées indirectes. La matrice de passage entre une b.o.n.d. (e_i) et une base quelconque (f_i) est dans $\mathrm{SO}(n)$ si et seulement si (f_i) est elle aussi une b.o.n.d.

Définition 4.14
Soit $(E, \langle , \rangle)$ un espace euclidien, muni d'une orientation. On appelle **produit mixte** l'unique forme n-linéaire alternée $\det : E \times \cdots \times E \to \mathbf{R}$ qui coïncide avec $\det_{(e_i)}$ pour toute base orthonormée directe (e_i) de E.

Exercice 4.13
Vérifier que ceci est bien défini.

Remarque 4.9. On note souvent $[u_1, \ldots, u_n]$ le produit mixte de n vecteurs d'un espace euclidien orienté. Géométriquement, il représente le volume algébrique du parallélépipède défini par les vecteurs $u_1, \ldots, u_n$.

4.5.2 Angles orientés dans un plan euclidien

Soit $(E, \langle ., . \rangle)$ un plan euclidien orienté.

Proposition 4.9
Pour tous $u, v \in E$, on a la relation

$$\langle u, v \rangle^2 + \det(u, v)^2 = \|u\|^2 \|v\|^2.$$

Il existe donc un unique $\theta \in \mathbf{R}/2\pi\mathbf{Z}$ tel que

$$\begin{cases} \langle u, v \rangle & = \|u\|.\|v\| \cos(\theta) \\ \det(u, v) & = \|u\|.\|v\| \sin(\theta). \end{cases}$$

Preuve. La relation provient du fait qu'elle est vraie dès que (u, v) est une base orthonormée, et de la formule $(ab + cd)^2 + (ad - bc)^2 = (a^2 + c^2)(b^2 + d^2)$. □

Définition 4.15
On appelle **angle orienté** de deux vecteurs $u, v \in E \setminus \{0\}$ l'unique $\theta \in \mathbf{R}/2\pi\mathbf{Z}$ donné par la proposition précédente. On le note $\widehat{(u, v)}$.

On note $O(E) = \{u \in \mathrm{End}(E) \ : \ u^* u = \mathrm{id}\}$ et $\mathrm{SO}(E) = O(E) \cap \mathrm{SL}(E)$. Pour tout $\theta \in \mathbf{R}/2\pi\mathbf{Z}$, on note

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

la matrice de rotation d'angle θ.

Proposition 4.10
Pour tout $u \in \mathrm{SO}(E)$, il existe un unique $\theta \in \mathbf{R}/2\pi\mathbf{Z}$ tel que $\mathrm{Mat}_{(e_i)}(u) = R_\theta$ pour toute base orthonormée directe (e_1, e_2) de E. De façon équivalente, θ est déterminé comme l'angle orienté entre x et $u(x)$ pour tout $x \in E \setminus \{0\}$.

On appelle **angle** (orienté) de u un tel θ. On vérifie que l'application $u \in \mathrm{SO}(E) \mapsto \theta \in \mathbf{R}/2\pi\mathbf{Z}$ est un isomorphisme de groupes.

Remarque 4.10. On note que pour une base indirecte (e_i), on a $\mathrm{Mat}_{(e_i)}(u) = R_{-\theta}$.

Pour tout $\theta \in \mathbf{R}/2\pi\mathbf{Z}$, on note

$$S_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} = R_\theta . \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Notons $p : \mathbf{R}/2\pi\mathbf{Z} \to \mathbf{R}/\pi\mathbf{Z}$ la projection naturelle.

Lemme 4.4
Soient D_1, D_2 deux droites de E. Il existe un unique $\overline{\theta} \in \mathbf{R}/\pi\mathbf{Z}$ tel que pour tous vecteurs v_1, v_2 tels que $D_1 = \mathbf{R}.v_1$ et $D_2 = \mathbf{R}.v_2$, on a $p(\widehat{(v_1, v_2)}) = \overline{\theta}$.

Preuve. On se donne deux vecteurs normés arbitraires v_1, v_2 dirigeant D_1, D_2 respectivement. Comme $\widehat{(v_1, -v_2)} = \widehat{(v_1, v_2)} + \pi \bmod 2\pi$, on observe que le résultat est le même modulo π, quel que soit le choix des vecteurs directeurs des droites. □

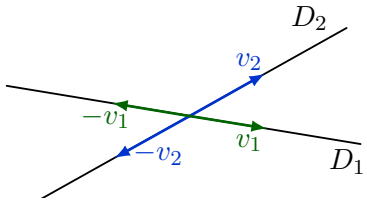

FIGURE 1 – Angle (D_1, D_2)

L'ordre en revanche compte.

Définition 4.16

L'angle non-orienté de deux droites D_1, D_2, prises dans cet ordre, est l'unique $\overline{\theta} \in \mathbf{R}/\pi\mathbf{Z}$ défini par le lemme ci-dessus. On le note (D_1, D_2).

On vérifie que la multiplication par 2 induit un morphisme $\mathbf{R}/\pi\mathbf{Z} \to \mathbf{R}/2\pi\mathbf{Z}$.

Proposition 4.11

Soient $s_1, s_2 \in O^-(E)$ deux symétries, d'axes D_1, D_2 respectivement. La composition $s_2 \circ s_1$ est la rotation d'angle $2(D_1, D_2) \in \mathbf{R}/2\pi\mathbf{Z}$.

Preuve. Comme $\det(s_2 \circ s_1) = 1$, on sait que $r := s_2 \circ s_1$ est une rotation. Son angle est l'angle orienté $\widehat{(x, r(x))}$, pour tout $x \neq 0$. Prenons $v_1 \in D_1$ non nul. On a $r(v_1) = s_2(v_1)$, et l'angle de r est donc l'angle orienté entre v_1 et $s_2(v_1)$. Soit (e_1, e_2) une base orthonormée directe telle que $e_2 = v_2$. Soit $\theta = \widehat{(v_1, v_2)}$. Par définition, on a $v_1 = \sin(\theta)e_1 + \cos(\theta)e_2$ et $s_2(v_1) = -\sin(\theta)e_1 + \cos(\theta)e_2$. On en déduit $\langle v_1, s_2(v_1)\rangle = \cos^2(\theta) - \sin^2(\theta) = \cos(2\theta)$ et $\det(v_1, s_2(v_1)) = 2\cos(\theta)\sin(\theta) = \sin(2\theta)$. Ceci montre que $\widehat{(v_1, s_2(v_1))} = 2\theta \bmod 2\pi$ comme annoncé. □

Proposition 4.12

Soit $u \in O^-(E)$ une symétrie orthogonale de droite fixe $D_u \subset E$. Pour toute base orthonormée directe (e_1, e_2) de E, on a $\mathrm{Mat}_{(e_i)}(u) = S_{2\overline{\theta}}$, où $\overline{\theta} \in \mathbf{R}/\pi\mathbf{Z}$ désigne l'angle non-orienté $\overline{\theta} = (\mathbf{R}.e_1, D_u)$.

Preuve. Soit $s \in O^-(E)$ la symétrie telle que $\mathrm{Mat}_{(e_i)}(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

La droite fixe de s étant $\mathbf{R}.e_1$, la Proposition 4.11 nous donne que $u \circ s$ est la rotation d'angle 2θ. Comme $s = s^{-1}$, nous avons bien

$$\mathrm{Mat}_{(e_i)}(u) = R_{2\theta}.\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_{2\theta}.$$

□

4.5.3 Rotations d'un espace euclidien de dimension 3

On se place à présent dans un espace euclidien orienté de dimension 3.

Proposition 4.13

Tout $u \in \mathrm{SO}(E)$ se met sous la forme

$$\mathrm{Mat}_{(e_i)}(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

où (e_1, e_2, e_3) est une base orthonormée de E.

Preuve. Comme $\dim E = 3$, le polynôme caractéristique χ_u est de degré 3 et admet donc une racine réelle λ. Si $v \in E_\lambda(u) \setminus \{0\}$, alors $\|u(v)\| = \|v\| = |\lambda|\|v\|$, d'où $\lambda = \pm 1$. Suit alors une petite discussion sur $\dim E_\lambda(u)$.

1. $\dim E_\lambda(u) = 3$: Alors $\lambda = 1$ et $u = \mathrm{id}_E$.
2. $\dim E_\lambda(u) = 2$ et $\lambda = 1$: Alors u préserve $E_\lambda(u)^\perp$ qui est une droite, nécessairement propre. La valeur propre vaut également ± 1, mais ceci est exclus car $u \neq \mathrm{id}_E$ et $\det(u) = 1$.
3. $\dim E_\lambda(u) = 2$ et $\lambda = -1$: Le même argument que ci-dessus donne que u est un renversement.
4. $\dim E_\lambda(u) = 1$ et $\lambda = 1$: L'orthogonal $P = E_\lambda(u)^\perp$ est un plan u-invariant et de plus $u|_P \in \mathrm{SO}(P)$ est une rotation de P. Il suffit alors de prendre une base orthonormée subordonnée à la somme directe $E = E_1(u) \oplus P$.
5. $\dim E_\lambda(u) = 1$ et $\lambda = -1$: L'orthogonal $P = E_\lambda(u)^\perp$ serait un plan u-invariant et de plus $u|_P \in O^-(P)$ une symétrie de P, contredisant $\dim E_{-1}(u) = 1$. Ce cas ne se produit pas.

□

Remarque 4.11. L'angle θ n'est pas défini modulo 2π, ni modulo π. Un autre choix de base peut conduire à $-\theta$.

Définition 4.17

On appelle **renversement** une rotation de SO(3) dont l'angle dans une base orthonormée est $\pi \bmod 2\pi$. C'est alors le cas dans toute base orthonormée, et sa matrice est de la forme

$$\mathrm{Mat}(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Remarque 4.12. Un renversement est de la forme $-s$, où s est une réflexion, *i.e.* une symétrie orthogonale par rapport à un plan. Noter que $s \notin \mathrm{SO}(E)$.

Théorème 4.11

Toute rotation $r \in \mathrm{SO}(E)$ est produit d'un ou de deux renversements.

Preuve. Si r est déjà un renversement ou l'identité, il n'y a rien à prouver. On peut donc supposer que l'espace propre associé à la valeur propre 1 de r est une droite, disons $\mathbf{R}.e_1$, et que l'endomorphisme induit par r sur $P := e_1^\perp$ n'est ni id_P, ni $-\mathrm{id}_P$.

Soit (e_2, e_3) une base orthonormée quelconque de P et soit $s \in O^-(E)$ la réflexion par rapport à $\mathrm{Vect}(e_1, e_2)$. Alors, $s(P) = P$ et $s|_P$ est la réflexion par rapport à $\mathbf{R}.e_2$. Comme $u|_P$ est une rotation de P, $r_P \circ s|_P$ est une réflexion de P, précisément celle selon la droite $\mathbf{R}.(\cos(\theta/2)e_2 + \sin(\theta/2)e_3)$ où θ désigne l'angle de $r|_P$ par rapport à

la base (e_2, e_3). De plus, $r \circ s(e_1) = e_1$, donc $s' := r \circ s$ est une réflexion de E. Ainsi, $r = s' \circ s = (-s') \circ (-s)$ est bien la composée de deux renversements. □

4.5.4 Algèbre des quaternions

Proposition 4.14

Il existe une $\mathbf{R}$-algèbre de dimension 4 admettant une base $(1, i, j, k)$ telle que 1 est l'élément neutre de la multiplication, $i^2 = j^2 = k^2 = -1$ et $ijk = -1$.

On note qu'immédiatement, $ij = -ji = k$, $jk = -kj = i$ et $ki = -ik = j$. En particulier, cette algèbre n'est pas commutative. Une approche possible pour son existence est la suivante.

Définition 4.18

On définit $\mathbf{H}$ comme étant le sous-$\mathbf{R}$-espace vectoriel

$$\mathbf{H} = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix},\ \alpha, \beta \in \mathbf{C} \right\} \subset M_2(\mathbf{C}).$$

On observe que ce sous-espace est stable par multiplication et forme donc une sous-$\mathbf{R}$-algèbre de $M_2(\mathbf{C})$ vérifiant la loi de multiplication des quaternions.

Notons

$$X(\alpha, \beta) = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}.$$

Avec la définition précédente, le quaternion $q = a + ib + jc + kd$ s'identifie à la matrice $X(\alpha, \beta)$ de paramètres $\alpha = a + ib$ et $\beta = -c + id$.

On prend des définitions en tout point similaires à celles des nombres complexes.

Définition 4.19

Soit $q = a + ib + jc + kd \in \mathbf{H}$. On définit son conjugué $\overline{q} = a - ib - jc - kd$. On note également $N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2$ son "module" au carré.

On note que si X est la matrice correspondant au quaternion q, alors ${}^t\mathrm{Com}(X)$ correspond à $\overline{q}$. De plus, $\det(X) = a^2 + b^2 + c^2 + d^2 = N(q)$, de façon cohérente avec la formule générale

$$A.{}^t\mathrm{Com}(A) = \det(A) I_n.$$

On vérifie directement les autres propriétés de la conjugaison. Par contre **attention**, $\overline{q_1 q_2} = \overline{q_2}.\overline{q_1}$.

Définition 4.20

On définit $N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2$, qui est une forme quadratique définie positive sur $\mathbf{H}$. Elle dérive du produit scalaire $\langle q_1, q_2 \rangle = \frac{1}{2}(q_1\overline{q_2} + q_2\overline{q_1})$.

Cette forme quadratique vérifie la propriété essentielle : $N(q_1 q_2) = N(q_1)N(q_2)$, comme le module des nombres complexes. Ainsi :

Définition 4.21

La sphère unité $G := \{q \in \mathbf{H} \ : \ N(q) = 1\}$ est un groupe pour la multiplication de $\mathbf{H}$. Après l'identification **ref**, il correspond au groupe de matrices

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}, \ |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

Il s'agit du sous-groupe de $\mathrm{SL}_2(\mathbf{C})$ formé des matrices qui préservent le produit scalaire hermitien $|z_1|^2 + |z_2|^2$ sur $\mathbf{C}^2$.

La multiplicativité de la norme a également pour conséquence que la multiplication (à gauche et à droite) des éléments de G préserve$N$. Pour tout $q_0 \in \mathbf{H}$, on définit, de façon similaire aux groupes, les isomorphismes $\mathbf{R}$-linéaires

$$L_{q_0} : \begin{array}{ccc} \mathbf{H} & \to & \mathbf{H} \\ q & \mapsto & q_0 q \end{array} \quad \text{et} \quad R_{q_0} : \begin{array}{ccc} \mathbf{H} & \to & \mathbf{H} \\ q & \mapsto & q q_0. \end{array}$$

Si $N(q_0) = 1$, alors $N(L_{q_0}(q)) = N(q)$ et $N(R_{q_0}(q)) = N(q)$ pour tout $q \in \mathbf{H}$. Ceci montre que pour tout $q_0 \in G$ $L_{q_0}, R_{q_0} \in O(\mathbf{H}, N)$ sont des endomorphismes orthogonaux de $\mathbf{H}$ par rapport à la forme quadratique N. On obtient ainsi deux actions par isométries de G sur $\mathbf{H}$:

$$\begin{array}{ccc} G & \to & O(\mathbf{H}, N) \\ q & \mapsto & L_q \end{array} \quad \text{et} \quad \begin{array}{ccc} G & \to & O(\mathbf{H}, N) \\ q & \mapsto & R_{q^{-1}}. \end{array}$$

Nous pouvons les combiner pour obtenir une troisième action, "par conjugaison" : pour tout $q_0 \in G$, l'application $S_{q_0} : q \mapsto q_0 q q_0^{-1}$ est une isométrie de $\mathbf{H}$, qui coïncide avec $L_{q_0} \circ R_{q_0^{-1}}$.

Théorème 4.12

Il existe un morphisme continu $G \to \mathrm{SO}(3)$, surjectif et de noyau $\{\pm 1\}$.

Preuve. Pour la surjectivité, il suffit de vérifier que les renversements de $\mathrm{SO}(V)$ sont dans l'image. Soit $q_0 \in G \cap V$ un quaternion pur de norme 1. Considérons son image $f(q_0) =: r$.

C'est une rotation de V qui vérifie $r(q_0) = q_0$, et si $q \in V$ est orthogonal à q_0, alors c'est que $qq_0 = -q_0 q$. Par conséquent, $r(q) = q_0 q q_0^{-1} = -q$, pour tout $q \in q_0^{\perp}$. Ainsi, $f(q_0)$ est bien le renversement associé à q_0, ce qui montre que les renversements sont dans l'image de f.

Pour déterminer le noyau, il suffit de se convaincre que le centre de $\mathbf{H}$ est la droite réelle (exercice). Enfin, la continuité évidente en prenant les coordonnées réelles associées à la base $(1, i, j, k)$. □

Théorème 4.13

On a un isomorphisme $\mathrm{SO}_4(\mathbf{R})/\{\pm I_4\} \simeq \mathrm{SO}_3(\mathbf{R}) \times \mathrm{SO}_3(\mathbf{R})$, qui est également un homéomorphisme pour les topologies standards de ces groupes.

En particulier $\mathrm{SO}_4(\mathbf{R})/\{\pm \mathrm{id}\}$ n'est pas simple, contrairement aux valeurs $n \geqslant 5$.

Remarque 4.13. Ces groupes sont des variétés, et les morphismes des difféomorphismes locaux.

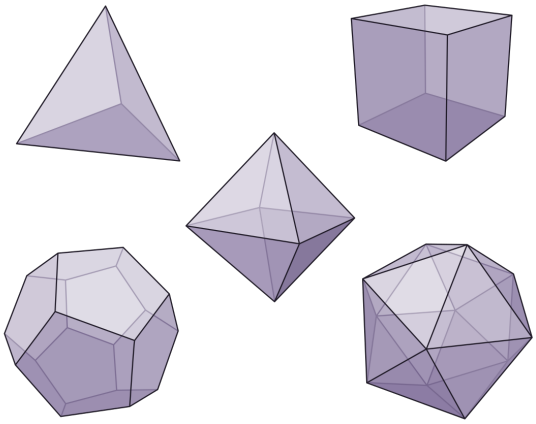

FIGURE 2 – Solides de Platon

4.6 Groupes d'isométries des solides platoniciens

Nous avons considéré dans un chapitre précédent le groupe diédral d'ordre $2n$, qui est isomorphe au groupe des isométries de n'importe quel polygone régulier à n cotés dans le plan euclidien. Il est naturel de s'interroger sur l'analogue tridimensionnel de ces résultats.

Premièrement, quels objets de l'espace jouent le rôle des polygones réguliers ? Ce sont les polyèdres réguliers convexes. Cette notion de régularité est assez délicate à énoncer bien qu'assez intuitive : toutes les faces doivent être des polygones réguliers deux à deux isométriques, la géométrie doit être la même depuis chaque sommet. On renvoie à [Aud06], V.4, V.5 pour plus de détails.

Un fait remarquable connu depuis l'Antiquité est qu'il n'existe que **cinq** polyèdres réguliers dans l'espace : le tétraèdre (4 faces), le cube (6 faces), l'octaèdre (8 faces), le dodécaèdre (12 faces) et enfin l'icosaèdre (20 faces). On les appelle **solides platoniciens**.

Ces objets étant très symétriques, il est naturel de considérer leurs groupes d'isométries. Étant donné un polyèdre P de l'espace euclidien, son groupe d'isométries est $\{f \in \mathrm{Isom}(\mathbf{R}^3) \mid f(P) = P\}$. Notons d'une isométrie étant affine, elle préserve le polyèdre si et seulement si elle préserve l'ensemble de ses sommets (qui sont ses points extrémaux en tant que convexe de $\mathbf{R}^3$). On définit similairement le groupe des isométries directes de P en considérant les f de $\mathrm{Isom}^+(\mathbf{R}^3)$ qui le preservent.

Proposition 4.15

Soit $S \subset \mathbf{R}^3$ un ensemble fini et symétrique, *i.e.* $\forall x,\ x \in S \Rightarrow -x \in S$, et soit $X = \mathrm{Conv}(S)$ son enveloppe convexe. Soit O l'isobarycentre de S. On note s_O la transformation affine isométrique telle que $s_O(O) = O$ et de partie linéaire $-\mathrm{id}$ (la symétrie centrale de centre O). On a alors un isomorphisme

$$\begin{array}{ccc} \mathrm{Isom}(X) & \to & \mathrm{Isom}^+(X) \times \langle s_O \rangle \\ f & \mapsto & \begin{cases} (f, \mathrm{id}) & \text{si } f \in \mathrm{Isom}^+(X) \\ (f \circ s_O, s_O) & \text{si } f \notin \mathrm{Isom}^+(X). \end{cases} \end{array}$$

Ainsi, pour les solides admettant une symétrie centrale, $\mathrm{Isom}(X) \simeq \mathrm{Isom}^+(X) \times \mathbf{Z}/2\mathbf{Z}$, le facteur $\mathbf{Z}/2\mathbf{Z}$ correspondant à l'involution antipodale. Ce sera le cas de tous les solides de Platon, sauf le tétraèdre pour lequel on a un produit semi-direct $\mathrm{Isom}(T) \simeq \mathrm{Isom}^+(T) \rtimes \mathbf{Z}/2\mathbf{Z}$. Pour les autres solides, on se contente donc de lister leurs groupes d'isométries directes.

Pour les mêmes raisons qu'au paragraphe **ref**, puisque deux polyèdres réguliers se déduisent l'un de l'autre par une similitude de $\mathbf{R}^3$, il y a un sens à parler *du* groupe d'isométries d'un solide de Platon donné.

Proposition 4.16

Le groupe d'isométries du tétraèdre est $\mathfrak{S}_4$, son groupe d'isométries directes est $\mathcal{A}_4$.
Le groupe d'isométries directes du cube est isomorphe à $\mathfrak{S}_4$.
Le groupe d'isométries directes de l'octaèdre est le même que celui du cube.
Le groupe des isométries directes du dodécaèdre est $\mathcal{A}_5$.
Le groupe d'isométries directes de l'icosaèdre est le même que celui du dodécaèdre.

Théorème 4.14

Tout sous-groupe fini de $\mathrm{SO}_3(\mathbf{R})$ est conjugué à un sous-groupe cyclique engendré par une rotation d'ordre n, au groupe diédral D_n, ou bien au groupe des isométries directes d'un des cinq solides platoniciens, donc isomorphe à $\mathcal{A}_4$, $\mathfrak{S}_4$ ou $\mathcal{A}_5$.

4.7 Automorphismes extérieurs de $\mathfrak{S}_6$ et isométries du dodécaèdre

5 Représentations linéaires des groupes finis

Fixons G un groupe fini.

Définition 5.1

Une **représentation** linéaire (complexe, de dimension finie) de G est la donnée d'un couple (V, ρ), où V est un espace vectoriel complexe de dimension finie et $\rho : G \to \mathrm{GL}(V)$ un morphisme de groupes. La dimension $\dim V$ est appelée **degré** de la représentation (V, ρ).

Une représentation (V, ρ) de G définit donc une action linéaire de G sur V, au sens des actions de groupes.

Définition 5.2

On dit d'une représentation (V, ρ) qu'elle est **fidèle** si ρ est injective.

En d'autre termes, la représentation est fidèle si l'action correspondante sur V l'est, au sens des actions de groupes.

Exemple 5.1.
1. La représentation triviale $V = \{0\}$, $\rho(g) = \mathrm{id}$ pour tout $g \in G$.
2. V quelconque et $\rho : G \to \mathrm{GL}(V)$ défini par $\rho(g) = \mathrm{id}_V$ pour tout g.
3. Si $G = \mathfrak{S}_n$, $n \geqslant 1$, alors en notant $\rho(\sigma)$ l'endomorphisme de $\mathbf{C}^n$ défini par $\rho(\sigma)(e_i) = e_{\sigma(i)}$, où $(e_1, \ldots, e_n)$ désigne la base canonique de $\mathbf{C}^n$, l'application $\rho : \sigma \in G \mapsto \rho(\sigma) \in \mathrm{GL}(\mathbf{C}^n)$ est une représentation de G.
4. Si $G = \mathbf{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, la présentation matricielle des quaternions **ref** nous donne une représentation fidèle de $\rho : G \to \mathrm{GL}(\mathbf{C}^2) \simeq \mathrm{GL}_2(\mathbf{C})$ telle que

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \rho(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \rho(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \rho(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Commençons par voir en détail le cas des représentations de degré 1.

5.1 Caractères d'un groupe fini

Définition 5.3

On appelle **caractère** de G tout morphisme $\rho : G \to \mathbf{C}^*$.

Remarque 5.1. Notons que pour tout espace vectoriel complexe V de dimension 1, $\mathrm{GL}(V)$ s'identifie canoniquement à $\mathbf{C}^*$.

Définition 5.4

L'ensemble des caractères de G est appelé **groupe dual**, ou groupe des caractères de G. Il est noté $\widehat{G}$, et c'est un groupe pour la loi naturelle $(\chi_1, \chi_2) \mapsto \chi_1 \cdot \chi_2$ définie par

$$\forall g \in G,\ (\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$$

Proposition 5.1

Tout caractère $\chi \in \widehat{G}$ se factorise en $\overline{\chi} : G/D(G) \to \mathbf{C}^*$, où $D(G)$ désigne le sous-groupe dérivé de G. De plus, si $n = |G/D(G)|$, alors χ (donc $\overline{\chi}$ également) est à valeurs dans le groupe $\mu_n(\mathbf{C}) \subset \mathbf{C}^*$ des racines n-èmes de l'unité.

Rappelons que cela signifie que $\chi = \overline{\chi} \circ \pi$, où $\pi : G \to G/D(G)$ désigne la projection canonique.

Preuve. Le premier point vient du fait que $\mathbf{C}^*$ est un groupe abélien (cf feuille de TD1). Le deuxième du théorème de Lagrange : si $g \in G$, alors $\pi(g^n) = \pi(g)^n = \pi(e)$ dans $G/D(G)$, d'où $\chi(g)^n = \overline{\chi}(\pi(g)^n) = 1$. □

Ainsi, les caractères se factorisent toujours en des caractères de l'abélianisé du groupe. Ce qui nous conduit à considérer les caractères des groupes abéliens finis.

Exemple 5.2.
1. Le caractère trivial, *i.e.* la fonction constante égale à 1 sur G.
2. Les caractères de $\mathfrak{S}_n$ sont la signature ou bien le caractère trivial (cf TD6).
3. Pour $G = \mathbf{Z}/n\mathbf{Z}$, le caractère $\chi : \overline{k} \mapsto \exp\left(\frac{2ik\pi}{n}\right)$.

Proposition 5.2

Soit G un groupe abélien fini et soit $H < G$ un sous-groupe. Soit $\chi_0 \in \widehat{H}$ un caractère de H. Alors il existe $\chi \in \widehat{G}$ un caractère de G tel que $\chi_0 = \chi|_H$.

Preuve. On procède par récurrence forte sur $[G : H]$.

Si H est un sous-groupe d'indice 1, alors le résultat est évident puisque $H = G$.

Supposons que pour $1 \leqslant k < |G|$, tout caractère défini sur un sous-groupe H d'indice au plus k s'étend en un caractère de G. Montrons que la proposition est vraie pour les sous-groupes d'indice $k+1$.

Soit donc H un sous-groupe d'indice $k+1$ dans G et soit χ_0 un caractère de H. Comme $k+1 > 1$, $H \neq G$ et on peut choisir $g \notin H$. Soit n l'ordre de gH dans le groupe quotient G/H (bien défini car G est abélien). Ainsi, n est le plus petit entier strictement positif tel que $g^n \in H$. Noter que $n \geqslant 2$.

Soit $H' = \{hg^k,\ h \in H,\ k \in \mathbf{Z}\}$ le sous-groupe engendré par $H \cup \{g\}$. Comme $|H'| > |H|$, on peut lui appliquer l'hypothèse de récurrence, et il nous suffit donc d'étendre χ_0 à H', qui s'étendra alors à tout G par hypothèse de récurrence.

Choisissons $z \in \mathbf{C}^*$ tel que $z^n = \chi_0(g^n)$ et montrons qu'on peut étendre χ_0 en un caractère $\chi_0' : H' \to \mathbf{C}^*$ tel que $\chi_0'|_H = \chi_0$ et $\chi_0'(g) = z$. Tout élément de H'

se met sous la forme hg^k, mais de façon non nécessairement unique. Néanmoins, si $h_1 g^{k_1} = h_2 g^{k_2}$ pour $h_1, h_2 \in H$ et $k_1, k_2 \in \mathbf{Z}$, alors $h_1 h_2^{-1} = g^{k_2 - k_1}$, d'où l'existence de $a \in \mathbf{Z}$ tel que $k_2 - k_1 = an$. Ainsi

$$\begin{aligned}\chi_0(h_2) z^{k_2} = \chi_0(h_2) z^{an} z^{k_1} &= \chi_0(h_2)\chi_0(g^n)^a z^{k_1} \\ &= \chi_0(h_2 g^{an}) z^{k_1} \\ &= \chi_0(h_1) z^{k_1}.\end{aligned}$$

Ainsi, *quelle que soit* l'écriture $h' = hg^k$, $h \in H$, $k \in \mathbf{Z}$ d'un élément de H', la valeur de $\chi_0(h) z^k \in \mathbf{C}^*$ est la même, et nous pouvons bien définir une application

$$\begin{array}{rccc} \chi_0' : & H' & \longrightarrow & \mathbf{C}^* \\ & hg^k & \mapsto & \chi_0(h) z^k \end{array}$$

dont il est immédiat de vérifier que c'est un morphisme de groupes, donc un caractère de H' qui étend χ_0. D'après l'hypothèse de récurrence, il existe un caractère $\chi : G \to \mathbf{C}^*$ tel que $\chi|_{H'} = \chi_0'$, donc *a fortiori* $\chi|_H = \chi_0$ ce qui termine la récurrence. □

Notons $p : \widehat{G} \to \widehat{H}$ le morphisme "restriction", c'est-à-dire $p(\chi) = \chi|_H$ pour tout caractère $\chi \in \widehat{G}$. On vérifie directement que c'est un morphisme, et la proposition précédente dit précisément qu'il est *surjectif*.

Notons $\pi : G \to G/H$ la projection canonique. Soit $i : \widehat{G/H} \to \widehat{G}$ l'application $\overline{\chi} \mapsto \overline{\chi} \circ \pi$. C'est également un morphisme de groupes, cette fois injectif (le vérifier). On vérifie également (voir feuille de TD) que $\operatorname{Ker} p = \operatorname{Im} i$, et finalement on a une suite exacte courte

$$1 \to \widehat{G/H} \to \widehat{G} \to \widehat{H} \to 1.$$

C'est en quelque sorte la suite exacte duale de la suite exacte courte $H \to G \to G/H$, où la première flèche est l'inclusion et la deuxième la projection canonique. En particulier, nous déduisons

$$|\widehat{G}| = |\widehat{G/H}.|\widehat{H}|,$$

pour tout sous-groupe H de G.

Proposition 5.3

Pour tout groupe abélien fini G, $|\widehat{G}| = |G|$.

Remarque 5.2. On verra en exercice que G est toujours isomorphe à son dual, mais pas canoniquement.

L'idée de la preuve est de le vérifier directement dans le cas des groupes cycliques, puis de faire une récurrence en s'aidant de la formule précédente.

Preuve. On procède par récurrence forte sur $|G|$.

L'initialisation est immédiate.

Soit $n \geqslant 1$. Supposons que tout groupe fini abélien d'ordre au plus n est du même ordre que son dual. Montrons que c'est le cas pour les groupes finis abéliens d'ordre $n+1$.

Soit G un tel groupe et soit H un sous-groupe cyclique de G, $H \neq \{e\}$. Un tel sous-groupe existe toujours, il suffit de considérer un élément $g \neq e$ et prendre $H = \langle g \rangle$.

Lemme 5.1

Soit $m \geqslant 1$ et soit $K = \mathbf{Z}/m\mathbf{Z}$. Alors $\widehat{K}$ est isomorphe à K.

Preuve. Rappelons que tout caractère de K est à valeur dans $\mu_m(\mathbf{C})$.

Soit $f : \overline{k} \in K \mapsto \phi_{\overline{k}} \in \widehat{K}$, où l'on définit

$$\begin{array}{rccc} \phi_{\overline{k}} : & K & \longrightarrow & \mathbf{C}^* \\ & \overline{\ell} & \mapsto & \exp\left(\frac{2ik\ell\pi}{m}\right). \end{array}$$

Premièrement, cette expression est bien définie indépendamment des choix des représentants de $\overline{k}$ et $\overline{\ell}$ dans $\mathbf{Z}/m\mathbf{Z}$, et à $\overline{k}$ fixé, $\phi_{\overline{k}}$ est un morphisme de groupes et $\phi_{\overline{k}_1+\overline{k}_2} = \phi_{\overline{k}_1}\phi_{\overline{k}_2}$ montrant que f est un morphisme de groupes.

Soit $g : \widehat{K} \to K$ définie par $g(\chi) =$ l'unique $\overline{k} \in K$ tel que $\chi(\overline{1}) = e^{\frac{2ik\pi}{m}} \in \mu_m(\mathbf{C})$. Si $\overline{k}_1 = g(\chi_1)$ et $\overline{k}_2 = g(\chi_2)$, alors comme $(\chi_1.\chi_2)(1) = \chi_1(1)\chi_2(1)$ on a directement $g(\chi_1.\chi_2) = g(\chi_1)+g(\chi_2)$ et g est un morphisme de groupes. Notons que $\chi(1)$ détermine complètement χ.

Comme $g \circ f = \mathrm{id}_K$ et $f \circ g = \mathrm{id}_{\widehat{K}}$, on en déduit que f et g sont des isomorphismes et que $g = f^{-1}$. □

Comme H est non-trivial, G/H est un groupe abélien d'ordre $\leqslant n$ et on peut lui appliquer l'hypothèse de récurrence. Comme H est cyclique, par le lemme précédent $|\widehat{H}| = |H|$ et nous avons donc

$$|\widehat{G}| = |\widehat{G/H}|.|\widehat{H}| = |G/H|.|H| = |G|,$$

d'après le théorème de Lagrange. Ainsi $|\widehat{G}| = |G|$, ce qui termine la récurrence. □

En fait, les groupes G et $\widehat{G}$ sont isomorphes (cf TD), mais pas canoniquement. Néanmoins, on a, *comme en dualité des espaces vectoriels de dimension finie*, un isomorphisme naturel entre G et son bidual $\widehat{\widehat{G}}$.

Théorème 5.1

Pour tout groupe abélien fini G, il existe un isomorphisme canonique $G \simeq \widehat{\widehat{G}}$.

Preuve. On commence par observer que ces deux groupes ont le même ordre par la proposition précédente. Il suffit donc de construire un morphisme injectif. Prenons alors

$$\begin{array}{rccc} f : & G & \longrightarrow & \widehat{\widehat{G}} \\ & g & \mapsto & \xi_g \end{array}$$

où $\xi_g : \chi \in \widehat{G} \mapsto \chi(g) \in \mathbf{C}^*$. À chaque g fixé, ξ_g est bien un caractère de $\widehat{G}$ (immédiat). Si $g_1, g_2 \in G$, alors pour tout $\chi \in \widehat{G}$, on a $\xi_{g_1g_2}(\chi) = \chi(g_1g_2) = \xi_{g_1}(\chi)\xi_{g_2}(\chi)$, d'où $f(g_1g_2) = f(g_1)f(g_2)$. Enfin, vérifions l'injectivité de f. Prenons $g \neq e$ dans G et soit $H = \langle g \rangle$. D'après le lemme 5.1, il existe un caractère $\chi_0 \in \widehat{H}$ tel que $\chi_0(g) \neq 1$ (tout caractère non trivial convient). D'après la proposition 5.2, il existe un caractère $\chi \in \widehat{G}$ tel que $\chi|_H = \chi_0$. Ainsi, $\xi_g(\chi) = \chi(g) = \chi_0(g) \neq 1$. D'où $g \neq e \Rightarrow \xi_g$ non trivial : f est bien injectif, ce qui conclut par égalité des cardinaux. □

5.2 Retour sur le cas général en tout degré

Définition 5.5

Soit (V, ρ) une représentation de G. Un sous-espace $W \subset V$ définit une **sous-représentation** de (V, ρ) s'il est stable par tous les éléments de g, c'est à dire si $\forall g \in G$, $\rho(g)W = W$ (rappelons que $\rho(g)$ est inversible).

Remarque 5.3. On fait (et on refera) un léger abus de langage en disant que W est une sous-représentation. Il est sous-entendu qu'on lui associe le morphisme $\rho^W : g \in G \mapsto \rho(g)|_W \in \mathrm{GL}(W)$. Rigoureusement, c'est la paire (W, ρ^W) qui est une sous-représentation de (V, ρ).

Exemple 5.3.

1. On reprend la représentation de $\mathfrak{S}_n$ sur $\mathbf{C}^n$ donnée par $\rho(\sigma)(e_i) = e_{\sigma(i)}$. Le vecteur $v = e_1 + \cdots + e_n$ est fixé par toutes les permutations : $\rho(\sigma)v = v$ pour toute $\sigma \in \mathfrak{S}_n$. Par conséquent, la droite $D = \mathbf{C}.v$ définit une sous-représentation de ρ, et ρ^D est la représentation triviale.

   De même, l'hyperplan $H = \{(z_1, \ldots, z_n) \in \mathbf{C}^n \ : \ z_1 + \cdots + z_n = 0\}$ définit une sous-représentation (cette fois non-triviale) de $(\mathbf{C}^n, \rho)$.
2. Plus généralement, étant donnée une action de G sur un ensemble fini X, on lui associe une représentation sur $V = \bigoplus_{x \in X} \mathbf{C}.e_x$, somme directe formelle de droites indexées par X, définie par $\rho(g)e_x = e_{g.x}$ pour tout $g \in G$ et $x \in X$. La droite dirigée par $v = \sum_{x \in X} e_x$ est une sous-représentation, tout comme son orthogonal pour le produit scalaire hermitien dont $(e_x)_{x \in X}$ est une base orthonormée.

   Un cas particulier important est celui où $X = G$ et l'action est celle par translation à gauche. La représentation associée s'appelle **représentation régulière de** G.

Définition 5.6

Une représentation (V, ρ) de G est dite **irréductible** si ses seules sous représentations sont V et $\{0\}$.

Exemple 5.4.

1. Toute représentation de degré 1 est irréductible.
2. On vérifie (cf TD) que la représentation (H, ρ^H) de l'exemple 5.3 est irréductible.

Définition 5.7

Soient (V_1, ρ_1), (V_2, ρ_2) deux représentations de G. Une application linéaire $f : V_1 \to V_2$ telle que, pour tout $g \in G$, $f \circ \rho_1(g) = \rho_2(g) \circ f$ est appelée **morphisme de représentations** de (V_1, ρ_1) sur (V_2, ρ_2). C'est un **isomorphisme de représentations** si f est de plus un isomorphisme linéaire entre V_1 et V_2.

Théorème 5.2 (Lemme de Schur)

Soient (V_1, ρ_1), (V_2, ρ_2) deux représentations **irréductibles** de G. Soit $f : V_1 \to V_2$ un morphisme de représentations. Alors, ou bien $f = 0$, ou bien f est un isomorphisme.

Soit (V, ρ) une représentation irréductible de G. Alors tout automorphisme de représentation de (V, ρ) est une homothétie.

Preuve. Soit $f : V_1 \to V_2$ un morphisme de représentations. Alors $\operatorname{Ker} f$ est une sous-représentation de (V_1, ρ_1). En effet, si $v \in \operatorname{Ker} f$ et $g \in G$, alors $f(\rho_1(g)v) = \rho_2(g)f(v) = 0$, d'où $\rho_1(g)v \in \operatorname{Ker} f$. Comme (V_1, ρ_1) est irréductible, on en déduit $\operatorname{Ker} f = \{0\}$ ou $\operatorname{Ker} f = V_1$. Dans le deuxième cas, f est l'application nulle. Supposons que ce n'est pas le cas. Alors, f est injective. De plus, $\operatorname{Im} f$ est une sous-représentation de (V_2, ρ_2) puisque pour tous $v \in V_1$ et $g \in G$, on a $\rho_2(g)f(v) = f(\rho_1(g)v) \in \operatorname{Im} f$. Par irréducibilité de (V_2, ρ_2), on en déduit $\operatorname{Im} f = \{0\}$ ou $\operatorname{Im} f = V_2$. C'est donc que f est surjective, donc un isomorphisme de représentations.

Soit $f : (V, \rho) \to (V, \rho)$ un automorphisme de représentation. Soit $\lambda \in \operatorname{Sp}_{\mathbf{C}} f$ une valeur propre complexe. Vérifions que l'espace propre associé $E_\lambda(f)$ est une sous-représentation de f : si $f(v) = \lambda v$, alors pour tout $g \in G$, $f(\rho(g)v) = \rho(g)f(v) = \lambda\rho(g)v$, d'où $\rho(g)v \in E_\lambda(f)$. Comme $\lambda \in \operatorname{Sp}_{\mathbf{C}} f$, on a $E_\lambda(f) \neq \{0\}$ par définition, d'où $E_\lambda(f) = V$ par irréducibilité, *i.e.* f est une homothétie de rapport λ. □

Théorème 5.3 (Mashke)

Soit (V, ρ) une représentation de G et soit $W \subset V$ une sous-représentation. Alors il existe une sous-représentation W' telle que $V = W \oplus W'$.

Ainsi, un sous-espace stable par tous les éléments de G admet un supplémentaire avec la même propriété.

Preuve. On commence par construire un produit scalaire hermitien $\rho(G)$-invariant via une méthode standard de moyennisation. Soit $\langle ., . \rangle$ un produit scalaire hermitien quelconque sur V. Définissons $\langle ., . \rangle_0$ par

$$\forall u, v \in V,\ \langle u, v \rangle_0 = \sum_{g \in G} \langle \rho(g)u, \rho(g)v \rangle.$$

On vérifie directement que $\langle ., . \rangle_0$ est sesquilinéaire, vérifie $\langle v, u \rangle_0 = \overline{\langle u, v \rangle_0}$ et est défini positif. Si $h \in G$ est donné, alors pour tous $u, v \in V$, on a

$$\langle \rho(h)u, \rho(h)v \rangle_0 = \sum_{g \in G} \langle \rho(gh)u, \rho(gh)v \rangle = \sum_{g \in G} \langle \rho(g)u, \rho(g)v \rangle = \langle u, v \rangle_0$$

puisque la translation $g \in G \mapsto gh \in G$ est bijective. Ceci montre que $\langle ., . \rangle_0$ est bien invariant par tous les éléments de $\rho(G) \subset \mathrm{GL}(V)$.

Maintenant, si W est une sous-représentation, prenons $W' = W^\perp$, où l'orthogonal est pris relativement au produit scalaire hermitien $\langle ., . \rangle_0$. Vérifions que W' est bien une sous-représentation. Soit $u \in W'$. Alors pour tout $v \in W$ et pour tout $g \in G$, on a $\langle \rho(g)u, v \rangle_0 = \langle u, \rho(g^{-1})v \rangle_0$, et comme $\rho(g^{-1})v \in W$, on a bien $\langle \rho(g)u, v \rangle_0 = 0$. Ceci pour tout $v \in W$, d'où $\rho(g)u \in W^\perp$, d'où $\rho(g)W^\perp = W^\perp$ pour tout $g \in G$. Le produit scalaire étant défini positif, $V = W \oplus W^\perp$, ce qui termine la preuve. □

Théorème 5.4

Soit G un groupe fini et soit (V, ρ) une représentation de G. Alors il existe $(V_1, \rho_1), \ldots, (V_k, \rho_k)$ des représentations irréductibles de G, et des entiers $a_1, \ldots, a_k \geqslant 1$, tels qu'on ait un isomorphisme de représentations

$$V \simeq V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$$

où $V_i^{\oplus a_i}$ désigne la représentation $(\underbrace{V_i \oplus \cdots \oplus V_i}_{a_i \text{ fois}}, \rho_i \oplus \cdots \oplus \rho_i)$.

Cette décomposition est unique (à isomorphisme près), au sens où pour tout autre isomophisme $V \simeq W_1^{\oplus b_1} \oplus \cdots \oplus W_r^{\oplus b_r}$ où $r \geqslant 1$, les W_j sont irréductibles, et $b_1, \ldots, b_r \geqslant 1$, on a nécessairement $r = k$ et une permutation $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ telle que pour tout $1 \leqslant i \leqslant k$, on a $b_i = a_{\sigma(i)}$ et $W_i \simeq V_{\sigma(i)}$.

Preuve. Existence : Mashke, par récurrence sur $\dim V$. Sans difficulté, le faire en exercice en rédigeant très proprement (cf rapport du jury).

Unicité : L'ingrédient est le lemme de Schur.

Notons provisoirement $V = \bigoplus_{1 \leqslant i \leqslant k} (\bigoplus_{1 \leqslant j \leqslant a_i} V_{i,j})$, où pour chaque i, les $V_{i,1}, \ldots, V_{i,a_i}$ sont des sous-représentations de V, toutes isomorphes à V_i. Supposons qu'on ait également $V = \bigoplus_{1 \leqslant \ell \leqslant r} (\bigoplus_{1 \leqslant m \leqslant b_\ell} W_{\ell,m})$, où $W_{\ell,1}, \ldots, W_{\ell,b_\ell}$.

Notons que tous i, j, la projection $p_{i,j} : V \to V_{i,j}$ parallèlement à la somme de tous les autres espaces dans la première décomposition est un morphisme de représentations. De même pour les projections $\pi_{\ell,m} : V \to W_{\ell,m}$.

D'après le lemme de Schur, pour tous i, j et ℓ, m, les restrictions $p_{i,j}|_{W_{\ell,m}} : W_{\ell,m} \to V_{i,j}$ et $\pi_{\ell,m}|_{V_{i,j}} : V_{i,j} \to W_{\ell,m}$ sont soit identiquement nulles, soit des isomorphismes. Comme ces restrictions ne peuvent être toutes nulles, ceci implique que pour tout $i \in [\![1, a_k]\!]$, il existe un unique $\ell \in [\![1, b_r]\!]$ tel que $V_{i,j} \simeq W_{\ell,m}$ pour tous j et m. Et inversement, pour tout $\ell \in [\![1, b_r]\!]$, il existe un unique $i \in [\![1, a_k]\!]$ tel que $W_{\ell,m} \simeq V_{i,j}$ pour tous m et j.

Ainsi $k = r$ et il existe une permutation $\sigma \in \mathfrak{S}_k$ telle que $V_{i,j} \simeq W_{\sigma(i),m}$ pour tous $i \in [\![1, k]\!]$ et j, m. Quitte à réordonner les $W_{\ell,m}$, on peut supposer $\sigma = \mathrm{id}$. Reste à voir que nécessairement $a_i = b_i$ pour tout i.

Pour tout $i \in [\![1, k]\!]$, notons $p_i = \sum_{1 \leqslant j \leqslant a_i} p_{i,j}$ et $\pi_i = \sum_{1 \leqslant m \leqslant b_i} \pi_{i,m}$. Notons également $\tilde{V}_i = \bigoplus_{1 \leqslant j \leqslant a_i} V_{i,j}$ et $\tilde{W}_i = \bigoplus_{1 \leqslant m \leqslant b_i} W_{i,m}$. D'après la même application du lemme de Schur, nous avons pour tous $i \neq i'$

$$\forall j \in [\![1, a_i]\!],\ p_{i'}(V_{i,j}) = \{0\},\ \text{d'où } p_{i'}(\tilde{V}_i) = \{0\}$$
$$\forall m \in [\![1, b_i]\!],\ \pi_{i'}(W_{i,m}) = \{0\},\ \text{d'où } \pi_{i'}(\tilde{W}_i) = \{0\}.$$

Ainsi $\tilde{V}_i \subset \tilde{W}_i$ et $\tilde{W}_i \subset \tilde{V}_i$, d'où l'égalité des dimensions et donc $a_i = b_i$ puisque $\dim V_{i,j} = \dim W_{i,m}$ (à chaque i donné, les représentations irréductibles sont isomorphes). □

Ces bases théoriques étant posées, on voudrait maintenant des outils plus pratiques pour déterminer les sous-représentations irréductibles et leur multiplicité au sein d'une représentation (V, ρ) donnée.

5.3 Caractères des représentations

Définition 5.8

Soit (V, ρ) une représentation de G. On définit son **caractère** comme étant la fonction $\chi_\rho : G \to \mathbf{C}$ donnée par l'expression $\chi_\rho(g) = \mathrm{Tr}\, \rho(g)$, pour tout $g \in G$.

Remarque 5.4. Le caractère d'une représentation de degré 1 est un caractère de G au sens de la section 5.1. En degré $\geqslant 2$, le caractère d'une représentation peut s'annuler et n'est **pas** en général un morphisme de G vers $\mathbf{C}^*$.

Exemple 5.5. Voir le TD pour les caractères de représentations standard de D_{2n} et $\mathbf{H}_8$ sur $\mathbf{C}^2$.

On commence par quelques observations plus ou moins immédiates.

Proposition 5.4

Soit $\chi = \chi_\rho : G \to \mathbf{C}$ le caractère d'une représentation (V, ρ) de G.

1. $\chi(e) = \dim V$
2. $\chi(hgh^{-1}) = \chi(g)$ pour tous $g, h \in G$
3. $\chi(g^{-1}) = \overline{\chi(g)}$ pour tout $g \in G$.

Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations isomorphes. Alors $\chi_{\rho_1} = \chi_{\rho_2}$.

Preuve. Pour le premier point, ceci vient du fait que $\rho(e) = \mathrm{id}_V$. Pour le deuxième, c'est le fait que $\operatorname{Tr} uv = \operatorname{Tr} vu$ pour tous $u, v \in \mathrm{End}(V)$. Pour le troisième, si $n = |G|$, le théorème de Lagrange nous assure $g^n = e$ pour tout $g \in G$, ainsi le polynôme $X^n - 1$ est annulateur de $\rho(g)$ pour tout g, ce qui assure $\mathrm{Sp}_{\mathbf{C}}\, \rho(g) \subset \mu_n(\mathbf{C})$ (et $\rho(g)$ est $\mathbf{C}$-diagonalisable). Si on note $\lambda_1, \dots, \lambda_d$ les valeurs propres de $\rho(g)$ comptées avec multiplicité ($d = \dim V$), alors celles de $\rho(g^{-1})$ sont $\overline{\lambda_1}, \dots, \overline{\lambda_d}$, d'où $\chi(g^{-1}) = \overline{\chi(g)}$.

Enfin, soit $f : V_1 \to V_2$ un isomorphisme de représentations. Si $(e_1, \dots, e_n)$ est une base de V_1 et si $\varepsilon_i = f(e_i)$, alors pour tout $g \in G$, $\mathrm{Mat}_{(e_i)} \rho_1(g) = \mathrm{Mat}_{(\varepsilon_i)} \rho_2(g)$ (il suffit de l'écrire). Ainsi, $\rho_1(g)$ et $\rho_2(g)$ ont la même trace. □

Définition 5.9

Une fonction $f : G \to \mathbf{C}$ telle que $f(hgh^{-1}) = f(g)$ pour tous $g, h \in G$ est dite **centrale**. On note $\mathcal{C}(G)$ le $\mathbf{C}$-espace vectoriel des fonctions centrales sur G à valeurs complexes.

Une fonction centrale est donc une fonction qui est **constante sur les classes de conjugaison** de G. En notant $\mathcal{R}$ la relation $g_1 \mathcal{R} g_2 \iff \exists h \in G \ : \ g_2 = h g_1 h^{-1}$ et en notant $p : G \to G/\mathcal{R}$ la projection canonique, toute fonction centrale $f : G \to \mathbf{C}$ induit une fonction $\overline{f} : G/\mathcal{R} \to \mathbf{C}$ telle que $f = \overline{f} \circ p$, et inversement, pour toute fonction $\phi : G/\mathcal{R} \to \mathbf{C}$, la fonction $f = \phi \circ p : G \to \mathbf{C}$ est centrale et induit ϕ au quotient.

L'application $\{f \mapsto \overline{f}\}$ définit ainsi un isomorphisme linéaire entre $\mathcal{C}(G)$ et $\mathcal{F}(G/\mathcal{R}, \mathbf{C})$, ce dernier désignant l'espace des fonctions de $G/\mathcal{R}$ vers $\mathbf{C}$. En notant k le nombre de classes de conjugaison de G, ceci montre que $\dim_{\mathbf{C}} \mathcal{C}(G) = k$.

On définit sur $\mathcal{C}(G)$ le produit scalaire hermitien donné pour toutes $\phi, \psi \in \mathcal{C}(G)$ par

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \psi(g)$$

On a alors la propriété fondamentale suivante dont on pourra admettre la démonstration en première lecture, puis consulter la preuve en annexe **ref**.

Proposition 5.5

Soit (V, ρ) une représentation de G. Alors

$$\boxed{(V, \rho) \text{ est irréductible si et seulement si } \langle \chi_\rho, \chi_\rho \rangle = 1}.$$

Soient (V_1, ρ_1), (V_2, ρ_2) deux représentations irréductibles. Alors

$$\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle = \begin{cases} 1 & \text{si } (V_1, \rho_1) \simeq (V_2, \rho_2) \\ 0 & \text{sinon.} \end{cases}$$

On pourra noter que dans le deuxième point, si V_1 et V_2 sont isomorphes, alors elles ont le même caractère, qui est donc de norme 1 par irréducibilité d'après le premier point.

Les caractères des représentations irréductibles de G (deux à deux non isomorphes) forment donc une famille orthonormée de $\mathcal{C}(G)$.

Corollaire 5.1

À isomorphisme près, il y a au plus k représentations irréductibles de G, où k désigne toujours le nombre de classes de conjugaison de G.

Remarque 5.5. Notons qu'*a priori*, il n'était pas évident du tout qu'il n'y a qu'un nombre fini de représentations irréductibles. Non seulement elles sont en nombre fini, mais on obtient ainsi une borne explicite.

Encore mieux (cf annexe pour la preuve) :

Proposition 5.6

À isomorphisme près, il y a exactement k représentations irréductibles de G. De façon équivalente, les caractères des représentations irréductibles de G forment une base orthonormée de $\mathcal{C}(G)$, pour la structure hermitienne introduite plus haut.

On en déduit immédiatement :

Corollaire 5.2

Une représentation est déterminée, à isomorphisme près, par son caractère : si V et W ont même caractère, alors elles sont isomorphes.

Preuve. Soient $V_1, \dots, V_k$ les représentations irréductibles de G, de caractères respectifs $\chi_1, \dots, \chi_k$. D'après le théorème 5.4, il existe $a_1, \dots, a_k$ des entiers positifs ou nuls tels que $V \simeq \bigoplus_{1 \leqslant i \leqslant k} V_i^{\oplus a_i}$ où on convient que V_i n'apparaît pas dans la décomposition quand $a_i = 0$. On a alors $\chi_V = \sum a_i \chi_i$, et donc $a_i = \langle \chi_V, \chi_i \rangle$ puisque $(\chi_1, \dots, \chi_k)$ est une base orthonormée de $\mathcal{C}(G)$. La multiplicité de V_i dans V est donc déterminée par le caractère de V, d'où le résultat d'après le théorème 5.4. □

5.4 Mise en pratique : table des caractères

On note toujours G notre groupe fini et on considère $(V_1, \rho_1), \dots, (V_k, \rho_k)$ les représentations irréductibles de G, où $k = \dim_{\mathbf{C}} \mathcal{C}(G)$ désigne toujours le nombre de classes de conjugaison de G.

Remarque 5.6. On notera qu'il y a (encore) un abus ici. Les ρ_i sont des représentants des classes d'isomorphismes des représentations irréductibles de G.

On notera $\mathbf{1}$ la (classe d'isomorphisme de la) représentation irréductible $(\mathbf{C}, \rho)$ avec $\rho(g) = \mathrm{id}_{\mathbf{C}}$ pour tout $g \in G$. C'est celle qui correspond au caractère trivial χ donné par $\chi(g) = 1$ pour tout $g \in G$.

Proposition 5.7

On a la relation

$$|G| = \sum_{i=1}^{k} (\dim V_i)^2.$$

Preuve. Considérons la représentation régulière $(V_{\mathrm{reg}}, \rho_{\mathrm{reg}})$, cf **ref**. On a $\dim V_{\mathrm{reg}} = |G|$. La multiplicité a_i de V_i est donnée par

$$a_i = \langle \chi_{\mathrm{reg}}, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \overline{\chi_{\mathrm{reg}}(g)}, \chi_i(g) \rangle.$$

Or pour tout $g \neq e$, la translation $h \in G \mapsto gh \in G$ est une permutation de G sans point fixe. La matrice de permutation associée est donc de diagonale nulle,

d'où $\chi_{\text{reg}}(g) = 0$ pour tout $g \neq e$. De plus, comme $\rho_{\text{reg}}(e) = \text{id}_{V_{\text{reg}}}$, on a $\chi_{\text{reg}}(e) = \dim V_{\text{reg}} = |G|$. Ainsi, on a

$$a_i = \frac{1}{|G|}|G|\chi_i(e) = \dim V_i,$$

puisque $\chi_i(e) = \dim V_i$ pour la même raison. Nous avons donc

$$V_{\text{reg}} \simeq \bigoplus_{i=1}^{k} V_i^{\oplus \dim V_i},$$

et l'identité suit en prenant les dimensions. □

On retiendra notamment que $\chi_{\text{reg}} = \sum_{i=1}^{k} (\dim V_i)\chi_i$ et que

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{si } g = e \\ 0 & \text{sinon.} \end{cases}$$

Pour classer les caractères des représentations irréductibles de G, on les place sur les lignes d'un tableau à double entrée dont les colonnes donnent leurs valeurs sur chaque classe de conjugaison de G. On commence donc en pratique par déterminer les classes de conjugaison de G.

On commence par rechercher les représentations de dimension 1, c'est à dire les caractères de G.

Table des caractères de $\mathfrak{S}_3$ La décomposition en produit de cycles à support disjoints permet de déterminer les classes de conjugaison. Toute permutation de $\mathfrak{S}_3$ est soit id, soit une transposition $(i\ j)$, soit un 3-cycle $(i\ j\ k)$. Il y a donc trois classes de conjugaison, donc trois classes d'isomorphismes de représentations irréductibles.

Comme toujours on a la représentation trivial $\mathbf{1}$. On sait que le seul autre caractère de $\mathfrak{S}_3$ est la signature ε. La troisième représentation irréductible (V, ρ) est nécessairement de degré 2 puisque $|\mathfrak{S}_3| = 6 = 1 + 1 + (\dim V)^2$. On peut déterminer son caractère en utilisant la relation $\chi_{\text{reg}} = \chi_{\mathbf{1}} + \chi_\varepsilon + 2\chi_\rho$ ou bien l'orthogonalité des colonnes.

	$\{\text{id}\}$	$\{(i\ j)\}$	$\{i\ j\ k\}$
$\mathbf{1}$	1	1	1
ε	1	-1	1
ρ	2	0	-1
ρ^{nat}	3	1	0

Pas de mystère, ρ est la représentation induite par la représentation naturelle de $\mathfrak{S}_3$ sur $\mathbf{C}^3$ sur le plan V d'équation $z_1 + z_2 + z_3 = 0$. Pour s'en convaincre, on peut noter $\rho^{\text{nat}} : \mathfrak{S}_3 \to \text{GL}(\mathbf{C}^3)$ la représentation définie par $\rho^{\text{nat}}(\sigma)e_i = e_{\sigma(i)}$ pour tout $\sigma \in \mathfrak{S}_3$ et $i \in \{1, 2, 3\}$. Si $D = \mathbf{C}.(e_1 + e_2 + e_3)$, alors $\mathbf{C}^3 = D \oplus V$ est une somme directe de représentations, et ρ^{nat} induit la représentation triviale sur D. On a donc $\chi_{\text{nat}} = 1 + \chi_V$, or $\chi_{\text{nat}}(\sigma)$ est le nombre de point fixe de σ puisque la matrice de $\rho^{\text{nat}}(\sigma)$ dans la base (e_1, e_2, e_3) est la matrice de permutation P_σ. Ainsi $\chi_V = \chi_\rho$ comme on peut le voir sur la ligne rajoutée dans le tableau, assurant que ρ est bien isomorphe à la représentation induite par ρ^{nat} sur V.

Noter que cet argument est valable pour d'autres valeurs que $n = 3$.

Table des caractères de $\mathcal{A}_4$ On a 4 classes de conjugaison : celle du neutre, les doubles transpositions, la classe de (1 2 3) et la classe de (1 3 2). Noter qu'on ne peut conjuguer que par une permutation de $\mathcal{A}_4$.

Soit $\chi : \mathcal{A}_4 \to \mathbf{C}^*$ un caractère. On sait qu'il factorise par le sous-groupe dérivé, qui rappelons-le est le sous-groupe des doubles transpositions noté V_4. Comme $\mathcal{A}_4/V_4$ est d'ordre 3, il est isomorphe à $\mathbf{Z}/3\mathbf{Z}$. Comme $(1\ 2\ 3) \notin V_4$, sa classe $(1\ 2\ 3)V_4 \neq V_4$, c'est donc un générateur de $\mathcal{A}_4/V_4$, nous pouvons donc fixer comme isomorphisme $f : \mathbf{Z}/3\mathbf{Z} \to \mathcal{A}_4/V_4$ l'application définie par

$$\begin{aligned} f(\overline{0}) &= V \\ f(\overline{1}) &= (1\ 2\ 3)V \\ f(\overline{2}) &= (1\ 3\ 2)V \end{aligned}$$

puisque $((1\ 2\ 3)V)^2 = (1\ 3\ 2)V$. Maintenant il y a trois caractères de $\mathbf{Z}/3\mathbf{Z}$, à savoir le caractère trivial, celui qui envoie $\overline{1}$ sur j et enfin celui qui envoie $\overline{1}$ sur j^2. D'où les trois premières lignes de la table des caractères

	$\{\mathrm{id}\}$	V_4	$\mathcal{C}_{(1\ 2\ 3)}$	$\mathcal{C}_{(1\ 3\ 2)}$
$\mathbf{1}$	1	1	1	1
χ_j	1	1	j	j^2
χ_{j^2}	1	1	j^2	j
ρ	3	-1	0	0
ρ^{nat}	4	0	1	1

La dernière s'obtient par la méthode usuelle : le degré d de ρ vérifie $12 = 1 + 1 + 1 + d^2$, d'où $d = 3$, puis par orthogonalité des colonnes. On reconnaît de nouveau le caractère de la représentation induite par ρ^{nat} sur l'hyperplan $V \subset \mathbf{C}^4$ d'équation $z_1 + z_2 + z_3 + z_4 = 0$.

Table des caractères de $\mathbf{H}_8$ On a cinq classes de conjugaison. Tout d'abord, les éléments centraux définissent chacun une classe de conjugaison à un élément. Ensuite, si $q \in \{\pm i, \pm j, \pm k\}$ est non central et si q_0 est un autre élément de $\mathbf{H}_8$, on vérifie directement que $q_0 q q_0^{-1} = q$ si $q_0 \in \{\pm 1, \pm q\}$ et $q_0 q q_0^{-1} = -q$ sinon. En effet, tout quaternion non central de $\mathbf{H}_8$ est de carré -1, donc son inverse est son opposé et la multiplication de $\mathbf{H}$ fait que le produit de deux éléments distincts de $\{i, j, k\}$ vaut plus ou moins le troisième. Ainsi, les trois autres classes de conjugaison sont $\{\pm i\}$, $\{\pm j\}$ et $\{\pm k\}$.

Déterminons les caractères de $\mathbf{H}_8$. On a déjà vu que le groupe dérivé de $\mathbf{H}_8$ est $\mathcal{Z}(\mathbf{H}_8) = \{\pm 1\}$. L'abélianisé $\mathbf{H}_8/\{\pm 1\}$ est isomorphe au groupe de Klein V_4. En effet, ses éléments sont les classes modulo ± 1, donc $\overline{1}$, $\overline{i}$, $\overline{j}$ et $\overline{k}$ avec comme loi de composition :

— Tout élément est de carré $\overline{1}$

— Le produit de deux éléments distincts dans $\{\overline{i}, \overline{j}, \overline{k}\}$ est le troisième élément.

On reconnaît V_4. Tout caractère de $\mathbf{H}_8$ induit donc un caractère de V_4 par le théorème de factorisation, et inversement tout caractère de V_4 nous donnera un caractère de $\mathbf{H}_8$.

On sait que $\widehat{V_4}$ et V_4 sont isomorphes (non canoniquement), on doit donc avoir quatre caractères pour V_4. Comme tout élément est d'ordre 2, un caractère $\chi : V_4 \to \mathbf{C}^*$ sera à valeurs dans $\{\pm 1\}$. Si on se donne trois signes $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{\pm 1\}$ tels que $\varepsilon_1 \varepsilon_2 = \varepsilon_3$ alors la fonction $V_4 \to \mathbf{C}^*$ telle que $\chi(\overline{1}) = 1$, $\chi(\overline{i}) = \varepsilon_1$, $\chi(\overline{j}) = \varepsilon_2$ et $\chi(\overline{k}) = \varepsilon_3$ sera un morphisme de groupes et on décrit ainsi tous les caractères de $V_4 = \mathbf{H}_8/D(\mathbf{H}_8)$, les signes possibles étant $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$ et $(-1, -1, 1)$.

En notant $\pi : \mathbf{H}_8 \to \mathbf{H}_8/D(\mathbf{H}_8) = V_4$ la projection canonique, tout caractère $\overline{\chi} : V_4 \to \mathbf{C}^*$ donne naissance à un caractère $\chi = \overline{\chi} \circ \pi : \mathbf{H}_8 \to \mathbf{C}^*$ et tous s'obtiennent ainsi. Nous avons donc les quatre premières lignes de la table des caractères.

D'après la relation entre l'ordre du groupe et les degrés des représentations, la cin-

quième représentation irréductible est nécessairement de degré 2.

	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
$\mathbf{1}$	1	1	1	1	1
$(1,-1,-1)$	1	1	1	-1	-1
$(-1,1,-1)$	1	1	-1	1	-1
$(-1,-1,1)$	1	1	-1	-1	1
ρ	2	-2	0	0	0

La dernière ligne peut s'obtenir via l'orthogonalité des colonnes. On reconnaît le caractère de la représentation standard $\rho : \mathbf{H}_8 \to \mathrm{GL}_2(\mathbf{C})$.

Références

[Ale99] M. Alessandri. *Thémes de géométrie - Groupes en situation géométrique.* Agrégation de Mathématiques. Dunod, 1999.

[Aud06] M. Audin. *Géométrie L3M1.* Enseignement sup, Mathématiques. EDP Sciences, 2006.

[CG13] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries.* Mathématiques en devenir. Calvage et Mounet, 2013.

[CL05] A. Chambert-Loir. *Algèbre corporelle.* Éditions de l'École Polytechnique, 2005.

[MT97] R. Mneimné and F. Testard. *Introduction à la théorie des groupes de Lie classiques.* Broché, 1997.

[Per96] D. Perrin. *Cours d'Algèbre.* Maths - Agreg. Ellipses, 1996.