Relations entre groupes de tresses et groupes de réflexions complexes

Charlie Hérent

Stage encadré par Olivier Dudas - IMJ-PRG

Mai - Juin 2018

Résumé

L'étude des groupes de tresses et des groupes de réflexions complexes a débuté au XXe siècle et se poursuit de nos jours. *A priori* purement abstraites, ces notions ont beaucoup d'applications que ce soit dans le domaine des mathématiques ou dans ceux de la physique et de l'informatique. Nous présenterons ici ces deux notions sous divers aspects et montrerons les liens étroits qui existent entre elles. Nous évoquerons également les recherches actuelles sur ces groupes dont notamment l'étude de leurs automorphismes.

Table des matières

Je tiens vivement à remercier Monsieur Dudas, mon maître de stage, pour son soutien et sa grande disponibilité. Je souhaite également remercier le personnel de l'Université Paris-Diderot (UFR de Mathématiques Sophie Germain) qui m'a très bien accueilli pendant les deux mois de stage.

1 Introduction

Les groupes de tresses ont principalement été introduits par Emil Artin (1898-1962) dont plusieurs problèmes s'y rattachant ont été résolus autour de 1925. De nombreux continuateurs d'Artin ont essayé de classifier les groupes de tresses. On peut notamment citer les travaux de F. A. Garside (1967), de P. Deligne (1972) médaillé Fields en 1970 ou encore ceux de W. Thurston (1988) médaillé Fields en 1982, P. Dehornoy (1995) et I. Dynnikov (1999).

L'étude des groupes de tresses est importante, notamment comme on pourra s'en rendre compte, en cryptographie. Mais plus généralement cette branche de la théorie des groupes possède de nombreuses ramifications dans d'autres théories. C'est particulièrement le cas dans celles de l'étude des groupes de réflexions complexes.

Les groupes de réflexions complexes ont été introduits (indépendamment des groupes de tresses) principalement dans la première partie du XXe siècle par diverses sources et leur classification fut achevée en 1954 par les travaux de G. C. Shephard et J. A. Todd. Ce n'est que vers la fin du XXe siècle que des définitions des groupes de tresses à partir de "réflexions de tresses" sont apparues par le développement de la topologie.
La classification de Shephard et Todd, bien que complète, était éparpillée dans la littérature et était très lourde dans les années 1950. Il fallut alors attendre les travaux de A. M. Cohen vers 1976 qui parvint à proposer une classification beaucoup plus synthétique et allégée de celle de Shephard et Todd, en généralisant les outils utilisés dans la classification des groupes de réflexions réels.

A partir des années 1980, l'étude des groupes de réflexions subit un nouvel essor par les diverses applications qu'ils offrent. En effet, ces groupes jouent un grand rôle dans le développement des algèbres de Hecke (que l'on ne développera pas dans ce rapport) ou encore par leur rôle clés dans plusieurs théorèmes. On peut notamment citer le théorème de Shephard-Todd/Chevalley-Serre et celui de Solomon. L'étude de propriétés autour des groupes de réflexions s'est alors accrue et à cet égard, on peut citer les travaux de M. Broué (1988), de J. Michel et M. Geck (1997) de G. Lusztig (à partir de 1980)...

Aujourd'hui, les études des groupes de tresses, de réflexions complexes et de Coxeter, ont donné naissance à de nombreuses théories portant sur les représentations des groupes. Une des plus étudiées actuellement est celle de Deligne-Lusztig.
Cependant, des recherches portant directement sur l'étude de ces groupes sont encore d'actualité. C'est d'ailleurs le cas de l'étude des automorphismes de ces groupes. On présentera dans ce rapport une courte étude des automorphismes de groupes de réflexions complexes. Et on pourra consulter les travaux de J. L. Dyer et E. K. Grossman (1981), de I. Marin et J. Michel (2010) ou encore ceux de V. G. Bardakov, M. V. Neshchadim et M. Singh (2017) pour les études portant sur les autres groupes.

On présentera tout d'abord les groupes de tresses dans la partie 2. Puis, nous introduirons dans la partie 3, les groupes de réflexions réels tout d'abord et ensuite complexes. On dressera la classification de Shephard-Todd de ces groupes en démontrant une partie du théorème de classification. Enfin, nous verrons dans une partie 4, les liens qui existent entre les groupes de tresses et les groupes de réflexions, on introduira, à ce moment là, les groupes de Coxeter. Dans la partie 5, nous ferons l'étude annoncée portant sur les automorphismes des groupes de réflexions complexes. En finalité, nous donnerons en partie 6, quelques utilisations des groupes présentées dans les premières parties de ce rapport.

2 Groupes de tresses

Nous définirons de trois manières les groupes de tresses, "dits de type A_{n-1}" dans la classification de Dynkin. On privilégiera tout d'abord, une représentation géométrique qui permettra de visualiser le concept. Puis, nous présenterons une définition topologique, permettant une manipulation plus complète de la notion. Enfin, nous donnerons une définition purement algébrique du concept.

2.1 Une définition géométrique

Géométriquement, une tresse à n brins (où $n \in \mathbb{N}^*$) peut être représentée par n ficelles (brins) attachées en $2n$ points distincts de $\mathbb{R}^3$ dont n points sont situés sur un premier disque pour une extrémité des ficelles et n autres points sur un deuxième disque pour l'autre extrémité des ficelles comme sur la figure ci-dessous.

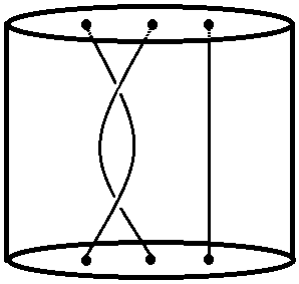

FIGURE 1 – Exemple de tresse à 3 brins

Comme on peut le remarquer sur la figure, une tresse n'est pas qu'une permutation des points d'attaches. C'est à la fois une permutation et l'histoire de cette permutation (i.e. comment les brins s'entrelacent). Formalisons mathématiquement cette définition.

Définition 1. On appelle T une *tresse géométrique à n brins*, tout $(n+1)$-uplet T tel que $T = (\sigma, \gamma_1, ..., \gamma_n)$ qui vérifie :

$$\begin{cases} \sigma \in \mathfrak{S}_n \\ \forall i \in [\![1, n]\!], \gamma_i \in \mathcal{C}([0,1], \mathbb{R}^3) \text{ avec } \gamma_i(0) = (i, 0, 1) \text{ et } \gamma_i(1) = (\sigma(i), 0, 0) \\ \forall z \in [0,1],\ i \neq j \implies \gamma_i(z) \neq \gamma_j(z) \end{cases}$$

Dans la définition ci-dessus, les γ_i sont des chemins dans $\mathbb{R}^3$ correspondants aux brins numérotés de 1 à n. Par rapport à la figure 1, les chemins (brins) partent du disque supérieur (ce dernier étant sur le plan $z = 1$) et arrivent sur le disque inférieur (ce dernier étant sur le plan $z = 0$).

On peut remarquer que si l'on étire les brins de la figure 1 sans les couper entre eux, cela ne change pas fondamentalement la tresse. La tresse ainsi déformée et la tresse initiale seront dites *isotopes*.

Définition 2. Soient $T = (\sigma, \gamma_1, ..., \gamma_n)$ et $T' = (\sigma', \gamma'_1, ..., \gamma'_n)$ deux tresses géométriques à n brins.
• On dira que T et T' sont *directement isotopes* si et seulement si : $\sigma = \sigma'$ et pour tout $t \in [0,1]$ $T(t) = (\sigma, \delta_1, ..., \delta_n)$ est une tresse géométrique avec : $\forall i \in [\![1, n]\!],\ \delta_i = (1-t)\gamma_i + t\gamma'_i$
• On dira que T et T' sont *isotopes* si et seulement si : il existe une suite finie $T_0, ..., T_m$ de tresses géométriques telles que $T_0 = T$ et $T_m = T'$ et $\forall i \in [\![1, m-1]\!]$, T_i et T_{i+1} sont directement isotopes.

La relation **"être isotope à"** est clairement une relation binaire, symétrique, réflexive et transitive sur l'ensemble des tresses géométriques à n brins. C'est donc une **relation d'équivalence**, dont on notera $\mathcal{T}_n$ l'ensemble des classes d'équivalences. Si T et T' sont isotopes

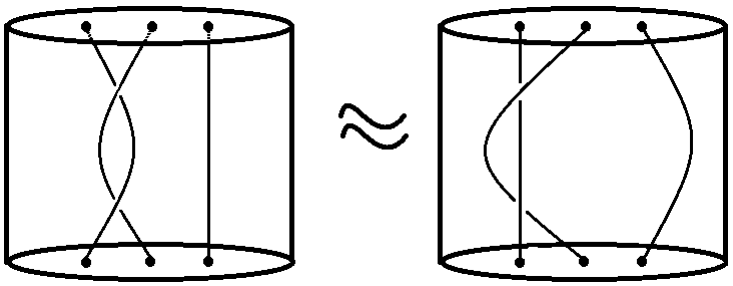

FIGURE 2 – Exemple de tresses à 3 brins isotopes

(donc dans la même classe), on notera $T \equiv T'$.

Nous allons maintenant définir la composée de deux tresses à n brins. On notera multiplicativement cette composition. Intuitivement, la composition de deux tresses sera la juxtaposition de la deuxième tresse placée sous la première dans l'espace.

Définition 3. Soient $T = (\sigma, \gamma_1, ..., \gamma_n)$ et $T' = (\sigma', \gamma'_1, ..., \gamma'_n)$ deux tresses géométriques à n brins. On définit la tresse géométrique produit $T \times T' = (\psi, \delta_1, ..., \delta_n)$ par :

$$\begin{cases} \psi = \sigma' \circ \sigma \\ \forall i \in [\![1, n]\!], \forall z \in [0,1]\ \delta_i(\frac{z}{2}) = \gamma_i(z) \text{ et } \delta_i(\frac{z+1}{2}) = \gamma'_{\sigma(i)}(z) \end{cases}$$

Lemme 1. • *Soit $T = (\sigma, \gamma_1, ..., \gamma_n)$ une tresse géométrique et ϕ une application continue de $[0,1]$ dans $[0,1]$ telle que $\phi(0) = 0$ et $\phi(1) = 1$. On note T' la tresse définie par : $T' = (\sigma, \gamma'_1, ..., \gamma'_n)$ où $\forall i \in [\![1, n]\!]$, $\gamma'_i = \gamma_i \circ \phi$. Alors on a $T \equiv T'$ (T et T' sont isotopes).*
• *Le produit $\times$ de compositions de tresses géométriques est compatible avec la relation $\equiv$ d'isotopie.*
• *Le produit $\times$ est associatif modulo la relation d'isotopie i.e. si T, T' et T'' sont des tresses à n brins, alors $(T \times T') \times T'' \equiv T \times (T' \times T'')$*

Démonstration. • Pour le premier point, on peut simplement remarquer que les tresses T et T' sont les mêmes vues comme objets géométriques dans l'espace. Les brins de T' sont en effet parcourus non plus suivant l'identité, mais suivant le paramétrage de la fonction ϕ. Ce qui ne change pas les figures dans $\mathbb{R}^3$. On peut donc conclure sur l'isotopie de T et T'.
• Si S, T, S', T' sont des tresses géométriques à n brins telles que $S \equiv S'$ et $T \equiv T'$ alors $S \times T \equiv S' \times T'$. En effet, notons $S = S_0$, ..., $S_m = S'$ la suite finie de tresses géométriques telle que S_i et S_{i+1} sont directement isotopes (définition isotopie). De même avec $T = T_0$,...,$T_k = T'$. Supposons que $m > k$, et posons $\forall i \in [\![k+1, m]\!]$ $T_i = T_k = T'$. On remarque que $S_i \times T_i$ est directement isotope à $S_{i+1} \times T_{i+1}$ pour tout $i \in [\![1, m-1]\!]$. Donc comme $S_0 \times T_0 = S \times T$ et $S_m \times T_m = S' \times T'$ on a donc $S \times T \equiv S' \times T'$. Démonstration analogue dans les cas $k = m$ et $m < k$.
• Pour le troisième point, il suffit d'appliquer le premier point avec la fonction ϕ définie par : pour $z \in [0,1]$ $\phi(\frac{z}{4}) = \frac{z}{2}$, puis $\phi(\frac{1+z}{4}) = \frac{2+z}{4}$ et $\phi(\frac{1+z}{2}) = \frac{3+z}{4}$. □

Théorème 1. *Muni de la loi $\times$ l'ensemble $\mathcal{T}_n$ est un groupe.*

Démonstration. Montrons donc que $\mathcal{T}_n$ admet un élément neutre, est stable pour la loi $\times$ et que tout élément admet un inverse. Nous savons déjà que la loi $\times$ est associative par le lemme 1.

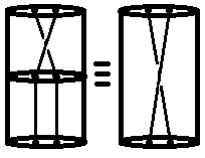

FIGURE 4 – Produit $T \times e \equiv T$

On peut voir le produit $T \times e \equiv T$ comme un étirement des brins par le bas (voir figure ci-contre).
La stabilité pour la loi $\times$ découle de la définition du produit de deux tresses géométriques à n brins.
L'inverse d'une tresse pour la loi $\times$ sera l'image de la tresse par un miroir. Formalisons mathématiquement cela.

Posons l'application ϕ telle que $\phi(z) = 1 - z$ pour tout $z \in [0,1]$. Prenons $T := (\sigma, \gamma_1, ..., \gamma_n)$

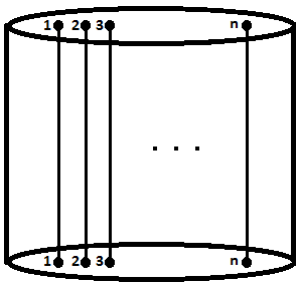

FIGURE 3 – Tresse triviale e - Élément neutre pour $\times$

une tresse géométrique à n brins, et construisons T^{-1} de la manière suivante : $T^{-1} := (\sigma^{-1}, \gamma'_1, ..., \gamma'_n)$ où l'on a $\gamma'_i = \gamma_{\sigma_i^{-1}} \circ \phi$ (brin obtenu par l'image miroir). On va montrer que $T \times T^{-1} \equiv e$. On note $T \times T^{-1} = (\psi, \delta_1, ..., \delta_n)$. On remarque tout d'abord que nécessairement $\psi = Id$ car $\sigma^{-1} \circ \sigma = Id$.
Soient $t \in [0, \frac{1}{2}]$ et $P(t) = (Id, p_1(t), ..., p_n(t))$ une tresse géométrique telle que $p_i(t)$ soit définie par :

$$p_i(t)(z) := \begin{cases} \delta_i(z) & \text{si } z \in [0,t] \cup [1-t,1] \\ \delta_i(t) & \text{si } z \in [t, 1-t] \end{cases}$$

On en déduit que $T \times T^{-1}$ est isotope à la tresse triviale puisque l'application qui à $t \in [0, \frac{1}{2}]$ associe $P(t)$ est continue et que $P(0) = e$ et $P(\frac{1}{2}) = T \times T^{-1}$. Soit $\sigma \in \mathfrak{S}_n$. On définit :

$$\mathfrak{T}(\sigma) := \left\{(\gamma_1, ..., \gamma_n) \in (\mathcal{C}([0,1], \mathbb{R}^3))^n \mid \forall i \in [\![1, n]\!], \gamma_i(0) = (i, 0, 1),\ \gamma_i(1) = (\sigma(i), 0, 0)\right\}$$

On peut remarquer que c'est un espace affine et même un espace affine normé si on le munit de la topologie de convergence uniforme. Comme $\mathfrak{T}(Id)$ est un espace affine normé, on remarque que les composantes connexes par lignes brisées (donc les classes d'isotopie) coïncident avec les composantes connexes par arcs.
Une preuve analogue montre que $T \times e \equiv e \times T \equiv T$ et que l'on a donc une structure de groupe par ce qui précède. □

Définition 4. On appellera *tresse géométrique pure à n brins*, toute tresse T géométrique à n brins qui vérifie : $T = (Id, \gamma_1, ..., \gamma_n)$ (c'est à dire $\sigma = Id$).
On notera $\mathcal{P}_n$ l'ensemble des tresses géométriques pures à n brins modulo la relation d'isotopie.

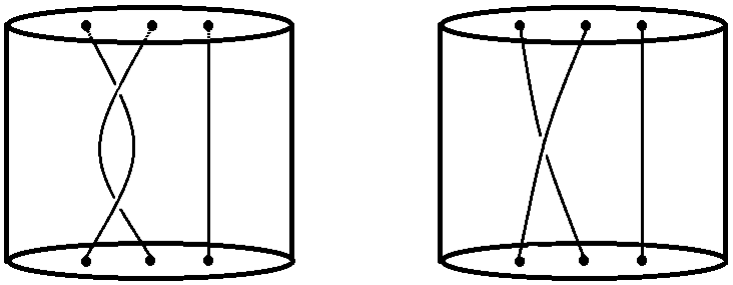

FIGURE 5 – Exemple d'une tresse pure à gauche et d'une tresse impure à droite

Autrement dit, une tresse géométrique est pure si elle vérifie : si un brin a pour départ le point $(i, 0, 1)$ alors il aura pour point d'arrivée le point $(i, 0, 0)$.
On peut vérifier que muni du produit $\times$, l'ensemble $\mathcal{P}_n$ est un sous-groupe de $\mathcal{T}_n$. On peut aussi voir $\mathcal{P}_n$ comme étant le noyau du morphisme surjectif : $\mathcal{T}_n \to \mathfrak{S}_n$.

2.2 Une définition topologique

On peut donner une définition topologique des groupes de tresses en utilisant le groupe fondamental d'un espace topologique. Pour définir cet outil, nous devons rappeler la définition d'une classe d'homotopie.

Définition 5. Soit X un espace topologique. On appelle *lacet* tout chemin continu fermé (i.e. une application $\gamma : [0,1] \to X$ continue telle que $\gamma(0) = \gamma(1)$).
• Un lacet sera dit de base $p \in X$ s'il vérifie en outre $\gamma(0) = \gamma(1) = p$.
• On dira que deux lacets γ_0 et γ_1 (de base p) sont *homotopes* s'il existe une homotopie de l'un vers l'autre i.e. une application continue $H : [0,1]^2 \to X$ telle que :

$$\begin{cases} \forall t \in [0,1],\ H(t,0) = \gamma_0(t) \\ \forall t \in [0,1],\ H(t,1) = \gamma_1(t) \\ \forall x \in [0,1],\ H(0,x) = H(1,x) = p \end{cases}$$

La relation **"être homotope à"** est clairement une relation binaire, symétrique, réflexive et transitive sur l'ensemble des lacets de base $p \in X$ d'un espace topologique X. C'est donc une **relation d'équivalence**. On note $[\gamma]$ la classe d'équivalence pour la relation d'homotopie (classe d'homotopie) d'un lacet γ de base p. On notera $\pi_1(X,p)$ l'ensemble des classes d'homotopie pour la relation décrite ci-dessus. Si γ_0 et γ_1 sont homotopes, on notera $\gamma_0 \sim \gamma_1$.

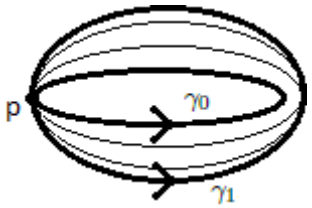

FIGURE 6 – Deux lacets γ_0 et γ_1 de base p homotopes

Définition 6. On définit le produit $\cdot$ de deux lacets γ_0 et γ_1 de base p par :

$$\gamma_0 \cdot \gamma_1(t) := \begin{cases} \gamma_0(2t) & \text{si } t \in [0, \frac{1}{2}] \\ \gamma_1(2t-1) & \text{si } t \in [\frac{1}{2}, 1] \end{cases}$$

On peut voir ce produit comme une concaténation (ou une juxtaposition) des lacets.
Le produit parcourt alors d'abord γ_0 et ensuite γ_1. On remarque alors que le produit de deux lacets de base p est encore un lacet de base p.

Théorème 2. *Soit (X,p) un espace topologique pointé en un point $p \in X$. L'ensemble $\pi_1(X,p)$ muni de la loi $\cdot$ forme un groupe. On appelle alors $\pi_1(X,p)$ groupe fondamental*[1] *associé à (X,p).*

Démonstration. • Soient γ_0 et γ_1 deux lacets de base p. On a alors $[\gamma_0] \cdot [\gamma_1] = [\gamma_0 \cdot \gamma_1]$. En effet, si $\gamma_0 \sim \gamma_0'$ et $\gamma_1 \sim \gamma_1'$ (le prime ne désignant **pas** la dérivation) d'homotopies respectives H_0 et H_1. On remarque alors que $\gamma_0 \cdot \gamma_1 \sim \gamma_0' \cdot \gamma_1'$ en prenant l'homotopie concaténée $H_0 \cdot H_1$ définie par :

$$\begin{cases} \forall x \in [0,1] : \forall t \in [0, \frac{1}{2}],\ (H_0 \cdot H_1)(t,x) = H_0(2t,x) \text{ et } \forall t \in [\frac{1}{2}, 1],\ (H_0 \cdot H_1)(t,x) = H_1(2t-1,x) \\ \forall x \in [0,1] :\ (H_0 \cdot H_1)(0,x) = (H_0 \cdot H_1)(1,x) = p \end{cases}$$

Le produit ne dépendant donc pas du représentant choisi dans la classe d'homotopie, on a bien l'égalité de classe : $[\gamma_0] \cdot [\gamma_1] = [\gamma_0 \cdot \gamma_1]$. Ainsi, le produit $\cdot$ est une loi interne bien définie sur $\pi_1(X,p)$.

1. Il est aussi appelé *groupe de Poincaré* ou *premier groupe d'homotopie* de X basé en p.

• La loi $\cdot$ est clairement associative (la concaténation étant définie par la gauche dans le produit).
• Le lacet constant égal à p (noté e) étant clairement l'élément neutre pour la loi $\cdot$ de concaténation :

$$\gamma \cdot e \sim e \cdot \gamma \sim \gamma$$

• Soit $[\gamma] \in \pi_1(X,p)$, on construit γ^{-1} de la manière suivante : $\gamma^{-1}(t) = \gamma(1-t)$ pour $t \in [0,1]$. On peut vérifier que $[\gamma]\cdot[\gamma^{-1}] \sim [\gamma^{-1}]\cdot[\gamma] \sim e$. Montrons que $[\gamma]\cdot[\gamma^{-1}] \sim e$ (l'autre relation se traite de manière analogue). On a déjà : $[\gamma]\cdot[\gamma^{-1}] \sim [\gamma\cdot\gamma^{-1}]$. Il s'agit de voir que $\gamma\cdot\gamma^{-1}$ est homotope au lacet constant en p. Pour cela, on prend H l'homotopie définie par :

$$\begin{cases} \forall t \in [0,1],\ H(t,0) = \gamma\cdot\gamma^{-1}(t) \\ \forall t \in [0,1],\ H(t,1) = e(t) \\ \forall x \in [0,1],\ H(t,x) = (\gamma_x \cdot \gamma_x^{-1})(t) \end{cases}$$

où γ_x est défini par :

$$\gamma_x(t) = \begin{cases} \gamma(t) & \text{si } t \in [0, 1-x] \\ \gamma(1-x) & \text{si } t \in [1-x, 1] \end{cases}$$

Autrement dit, γ_x vaut γ sur $[0,1-x]$ puis stationne en $\gamma(1-x)$ dès que $t \in [1-x,1]$.
Ainsi on a bien $[\gamma]\cdot[\gamma^{-1}] \sim [\gamma\cdot\gamma^{-1}] \sim [e]$, et on en déduit que $(\pi_1(X,p),\cdot)$ est un groupe. □

Lemme 2. *Soit X un espace topologique et $x_0, x_1 \in X$ tels que x_0 et x_1 sont dans une même composante connexe par arcs de X.*
Alors on a l'isomorphisme de groupes : $\pi_1(X,x_0) \simeq \pi_1(X,x_1)$

Démonstration. L'idée de la preuve se résume au schéma ci-contre.
Comme x_0 et x_1 sont dans la même composante connexe par arcs de X, il existe $h : [0,1] \to X$ un chemin continu de x_0 vers x_1 ($h(0) = x_0$ et $h(1) = x_1$). On note $h^{-1}(t) = h(1-t)$ le chemin inverse de h. Donc si γ est un lacet de base x_1 alors $h\cdot\gamma\cdot h^{-1}$ (où $\cdot$ est étendue des lacets aux chemins) est un lacet de base x_0. On peut alors définir l'application $\gamma_h : \pi_1(X,x_0) \to \pi_1(X,x_1)$ par :

$$\gamma_h([\gamma]) = [h\cdot\gamma\cdot h^{-1}]$$

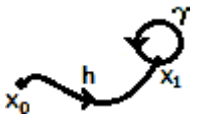

FIGURE 7 – Changement de base du lacet γ

On remarque tout d'abord que γ_h est un morphisme de groupes :

$$\gamma_h([f]\cdot[g]) = \gamma_h([f\cdot g]) = [h\cdot f\cdot g\cdot h^{-1}] = [h\cdot f\cdot h^{-1}\cdot h\cdot g\cdot h^{-1}] = \gamma_h([f])\cdot\gamma_h([g])$$

De plus, γ_h est un isomorphisme puisque : $\gamma_h \cdot \gamma_{h^{-1}}([f]) = \gamma_h([h^{-1}\cdot f\cdot h]) = [f]$. De même, on a : $\gamma_{h^{-1}}\cdot\gamma_h([f]) = [f]$. Donc on a bien montré que $\pi_1(X,x_0) \simeq \pi_1(X,x_1)$. □

Ainsi, si X est connexe par arcs, on ne mentionnera pas forcement le point x_0 et on notera (par abus de langage) $\pi_1(X)$ le groupe fondamental en n'importe quel point de X.

Définition 7. On appelle *n-ième espace de configuration (de Fadell)* sur $\mathbb{C}$, l'ensemble :

$$\mathcal{M}_n := \{(z_1, \cdots, z_n) \in \mathbb{C}^n \mid z_i \neq z_j \text{ pour } i \neq j\}$$

Remarque 1. Si l'on définit une famille d'hyperplans $H_{i,j}$ de $\mathbb{C}^n$ de la manière suivante : $H_{i,j} := \{z_i = z_j\}$ avec $i \neq j$ et que l'on pose $D := \bigcup_{1\leq i<j\leq n} H_{i,j}$. Alors on obtient : $\mathcal{M}_n = \mathbb{C}^n \backslash D$.

On va maintenant définir les groupes de tresses pures et de tresses en général à l'aide du groupe fondamental et de l'espace de configuration.

Définition 8. On définit le groupe de tresses pures à n brins par : $\mathscr{P}_n := \pi_1(\mathcal{M}_n)$

Autrement dit, si on se donne $T \in \mathscr{P}_n$, alors on peut voir T comme une boucle dans $\mathcal{M}_n$ qui commence et fini au même point de $\mathcal{M}_n$ par l'application suivante :

$$\begin{array}{rl} T: & [0,1] \longrightarrow \mathcal{M}_n \\ & t \longmapsto (\gamma_1(t), \cdots, \gamma_n(t)) \end{array}$$

Définition 9. On définit le groupe de tresses à n brins par : $\mathscr{T}_n := \pi_1(\mathcal{N}_n)$ où $\mathcal{N}_n = \mathcal{M}_n / \mathfrak{S}_n$

Si l'on a compris le cas des tresses pures, alors il suffit simplement de voir que quotienter par $\mathfrak{S}_n$ permet pour les γ_i d'arriver sur leur point de départ modulo une permutation. Ici les boucles commencent et finissent sur un point qui n'est plus un point de $\mathcal{M}_n$ mais une classe d'équivalence.
On retrouve donc la notion de groupe de tresses explicitée dans la partie précédente.

2.3 Une définition algébrique

On suppose connue la notion de groupe libre.
On pourra consulter [8] pour plus de détails concernant les propriétés des groupes libres.
Rappelons la définition d'une *présentation par générateurs et relations* d'un groupe :

Définition 10. Soit G un groupe (de neutre noté 1), engendré par un ensemble $X = (x_i)_{i \in I}$. Soit R une partie du groupe libre $L(X)$. On note $N(R)$ le sous-groupe distingué de $L(X)$ engendré par R. On dit que $\langle X \mid H \rangle$ (où $H = \{r = 1 \mid r \in R\}$), est une *présentation* de G, si G est isomorphe au groupe-quotient $L(X)/N(R)$. On appelle ainsi X l'ensemble des *générateurs* et R l'ensemble des *relations* entre générateurs dans la présentation de G.

Remarque 2. Lorsque R est fini, on dit que G est de présentation finie.

Définition 11. Pour $n \geq 2$, le groupe de tresses à n brins $\mathbb{T}_n$ est le groupe engendré par $n-1$ générateurs : $\sigma_1, \cdots \sigma_{n-1}$ soumis aux relations suivantes :

$$\forall i, j \in [\![1, n-1]\!] \left\{ \begin{array}{ll} |i-j| = 1 & \Longrightarrow \ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \\ |i-j| > 1 & \Longrightarrow \ \sigma_i \sigma_j = \sigma_j \sigma_i \end{array} \right.$$

Autrement dit :

$$\mathbb{T}_n := \langle \sigma_1, \cdots \sigma_{n-1} \mid \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \text{ pour } |i-j| = 1 \text{ et } \sigma_i \sigma_j = \sigma_j \sigma_i \text{ pour } |i-j| > 1 \rangle$$

2.4 Lien entre les trois définitions

On reprend la définition géométrique des tresses à n brins et on va montrer qu'elle coïncide avec la définition algébrique ci-dessus. Nous allons montrer que la définition géométrique vérifie la *présentation* algébrique.

Sans perte de généralité, nous projetterons donc désormais les tresses dans $\mathbb{R}^2$ en conservant les informations de superpositions des brins.
On note σ_i la tresse géométrique à n brins définie par la figure 8. C'est à dire, la tresse ayant comme permutation $\sigma = (i \ i+1)$ et qui possède pour brins γ_j égaux aux segments reliant les points $(j, 0, 1)$ à $(j, 0, 0)$ lorsque $j \notin \{i, i+1\}$. Et les brins γ_i et γ_{i+1} comme sur la figure :

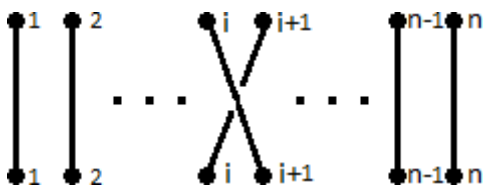

FIGURE 8 – La tresse géométrique notée σ_i

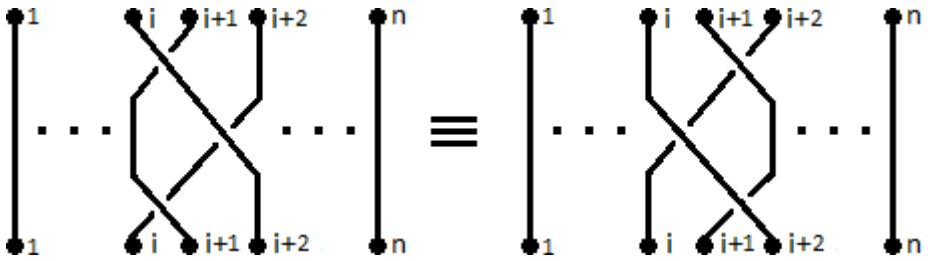

FIGURE 9 – Le premier type de relations de tresses : $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$

On peut alors vérifier, avec la définition géométrique des tresses à n brins, que l'égalité (premier type de relations dans la présentation algébrique) : $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ est vraie pour $|i-j| = 1$.

De même, avec la deuxième type de relations de tresses, on obtient les trois diagrammes ci-dessous qui sont isotopes. On a fait figurer le diagramme qui se situe au centre pour montrer une étape intermédiaire dans la déformations des brins, qui conduit à l'isotopie des deux diagrammes du haut de la figure :

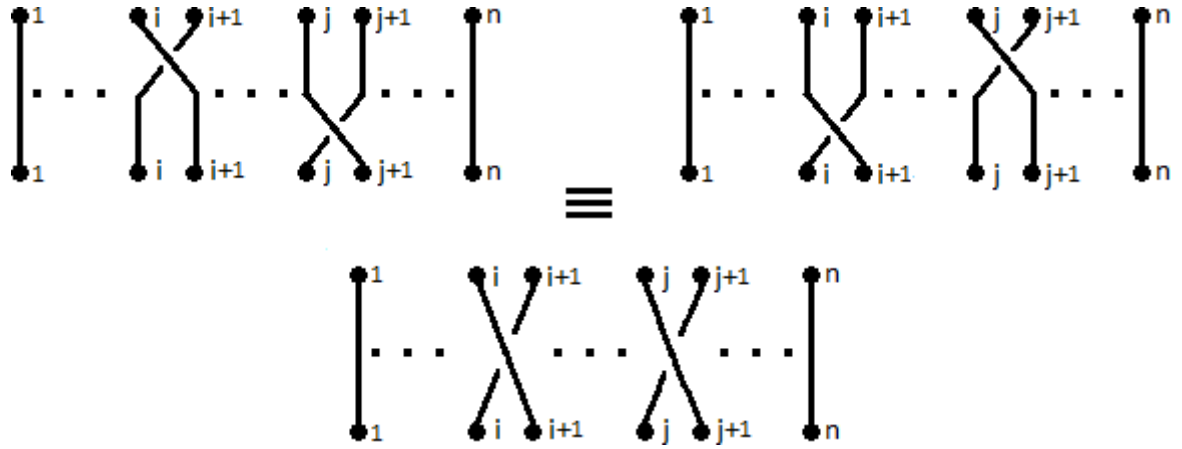

FIGURE 10 – Le deuxième type de relations de tresses : $\sigma_i\sigma_j = \sigma_j\sigma_i$

On a donc vérifié que la définition géométrique vérifie les relations de la définition algébrique. Cependant, sont-ce les seules relations vérifiées par la définition géométrique ? i.e. Le groupe de tresses géométriques à n brins admet-il la présentation algébrique donnée dans la partie précédente ? De même, la définition topologique admet-elle une telle présentation ?
Ou encore : est-ce que les trois définitions de groupes de tresses coïncident ? La réponse est **oui**, mais cela est assez difficile à montrer et constitue le **théorème d'Artin** que ne l'on démontrera pas, par soucis d'espace. On pourra consulter [10] pour une preuve du résultat.

Théorème 3. ***Théorème d'Artin***
On a les isomorphismes de groupes : $\mathcal{T}_n \simeq \mathscr{T}_n \simeq \mathbb{T}_n$

Dans la suite, nous adopterons la notation $\mathcal{T}_n$ pour parler du groupe de tresses à n brins indépendamment de la définition choisie, puisqu'elles sont équivalentes.

3 Groupes de réflexions

Nous présenterons tout d'abord les groupes de réflexions réels afin de comprendre le principe géométrique derrière la définition de groupe de réflexions. Puis nous aborderons les groupes de réflexions complexes.

3.1 Groupes de réflexions réels

Dans tout cette sous partie, on considère V un $\mathbb{R}$-espace vectoriel de dimension finie : $n := Dim(V)$.

Définition 12. Une **réflexion** (réelle) de V est un endomorphisme $s \in L(V)$ différent de l'identité, d'ordre fini, qui fixe un hyperplan.

Remarque 3. Si l'on prend s une réflexion et H un hyperplan fixé par cette réflexion. Si l'on prend S un supplémentaire de H dans V et que l'on écrit la matrice de s dans une base adaptée à la décomposition $V = H \bigoplus S$:

$$\left(\begin{array}{c|c} I_{n-1} & 0 \\ \hline 0 & \alpha \end{array}\right) \text{ avec } \alpha \in \mathbb{R}^*$$

On a nécessairement $\alpha \in \mathbb{R}^*$ car $tr(s) = \alpha + (n-1) \in \mathbb{R}$ et car la définition précédente impose que l'ordre de s est fini. Cette même condition impose qu'il existe $n \in \mathbb{N}$ tel que $\alpha^n = 1$. C'est à dire $\alpha \in \{-1, 1\}$. Comme la définition retire le cas de l'identité, on a nécessairement : $\alpha = -1$. On en déduit que s est d'ordre 2.

Définition 13. Un groupe de réflexions réel est un sous-groupe fini de $\mathrm{GL}(V)$ engendré par des réflexions.

Exemple 1. Le groupe $\mathfrak{S}_n$ se plonge classiquement dans $\mathrm{GL}(V)$ par les matrices de permutations. Ainsi, on peut voir $\mathfrak{S}_n$ comme un groupe de réflexions réel où une transposition $(i\ j)$ correspond à la symétrie orthogonale d'hyperplan $(e_i - e_j)^\perp$ avec $(e_1, \cdots, e_n)$ la base canonique de $\mathbb{R}^n$.

Exemple 2. Un groupe $G \subseteq \mathrm{GL}(V)$ peut être engendré par un nombre fini de réflexions mais être infini. Par exemple, il suffit de prendre $G := \langle s_H, s_{H'} \rangle \subseteq \mathrm{GL}(\mathbb{R}^2)$ où H et H' sont deux droites de $\mathbb{R}^2$ formant un angle multiple irrationnel de π et où s_H désigne la réflexion de $\mathbb{R}^2$ d'hyperplan H.

3.2 Groupes de réflexions complexes

Dans tout cette sous partie, on considère V un $\mathbb{K}$-espace vectoriel de dimension finie : $n := Dim(V)$. On note V^* le dual de V.

On peut remarquer que le groupe $\mathrm{GL}(V)$ agit sur $V \times V^*$ de la manière suivante :
Soient $r = (v, v^*) \in V \times V^*$ et $g \in \mathrm{GL}(V)$, on définit l'action de groupe :

$$g \cdot r := (g(v), v^* \circ g^{-1})$$

Cette action nous sera utile pour des propriétés ultérieures.

3.2.1 Endomorphisme de rang 1 attaché à un élément de $(V \setminus \{0\}) \times (V^* \setminus \{0\})$

Soit $r \in (V \setminus \{0\}) \times (V^* \setminus \{0\})$, on construit un endomorphisme de rang 1 de V grâce à $r = (v, v^*)$:

$$\overline{r} : x \mapsto v^*(x)v$$

On note $H_r := \ker(\overline{r})$ le noyau, $L_r := Im(\overline{r})$ l'image et $tr(r)$ la trace de l'endomorphisme $\overline{r}$.

Remarque 4. • On voit aisément que l'on a : $H_r = \ker(v^*)$, puis $L_r = \mathbb{K}v$ et $tr(r) = v^*(v)$.
• On voit également que : $L_r \subseteq H_r \Leftrightarrow tr(r) = 0$

On se donne $(e_1, \cdots, e_{n-1})$ une base du noyau de $\overline{r}$ qui est de dimension $n-1$ en vertu du théorème du rang puisque $rg(\overline{r}) = 1$. On peut compléter cette base avec le vecteur v qui n'est pas dans $\ker(\overline{r})$. En écrivant la matrice de s_r dans la base $(e_1, \cdots, e_{n-1}, v)$ on obtient :

$$\left(\begin{array}{c|c} I_{n-1} & 0 \\ \hline 0 & z_r \end{array}\right)$$

Lemme 3. • *Soit $g \in \mathrm{GL}(V)$ et $r \in V \times V^*$.*
L'endomorphisme de rang 1 obtenu à partir de $g \cdot r := (g(v), v^* \circ g^{-1})$ est : $g\overline{r}g^{-1}$
• *Deux éléments $r_1 = (v_1, v_1^*)$ et $r_2 = (v_2, v_2^*)$ de $(V \setminus \{0\}) \times (V^* \setminus \{0\})$ définissent le même endomorphisme de rang 1 de $V \Leftrightarrow \exists \lambda \in \mathbb{K} \setminus \{0\}$ tel que $v_2 = \lambda v_1$ et $v_2^* = \frac{1}{\lambda} v_1^*$*

Démonstration. • Soit $x \in V$, on a par définition : $\overline{g \cdot r}(x) = v^*(g^{-1}(x))g(v)$. Comme $v^*(g^{-1}(x)) \in \mathbb{K}$, on a par linéarité de g : $\overline{g \cdot r}(x) = g(v^*(g^{-1}(x))v)$. De plus, $g\overline{r}g^{-1}(x) = g(v^*(g^{-1}(x))v)$. D'où : $\overline{g \cdot r} = g\overline{r}g^{-1}$.
• Si $r_1 = (v_1, v_1^*)$ et $r_2 = (v_2, v_2^*)$ de $(V \setminus \{0\}) \times (V^* \setminus \{0\})$ définissent le même endomorphisme de rang 1 de V, alors on a pour tout $x \in V$: $v_1^*(x)v_1 = v_2^*(x)v_2$ (E). Comme par définition on a v_2^* qui n'est pas la forme linéaire nulle, il existe $x_0 \in V$ tel que $v_2^*(x_0) \neq 0$. On obtient ainsi $v_2 = \frac{v_1^*(x_0)}{v_2^*(x_0)} v_1$ D'où $v_2 = \lambda v_1$ avec $\lambda = \frac{v_1^*(x_0)}{v_2^*(x_0)}$. Supposons que $v_1^*(x_0) = 0$ alors on aurait $v_2^*(x_0)v_2 = 0$ par (E). Et donc comme $v_2^*(x_0) \neq 0$, on aurait $v_2 = 0$, ce qui est exclut. Donc $\lambda \neq 0$.
En réécrivant (E) on obtient : $v_1^*(x)v_1 = \lambda v_2^*(x)v_1$ pour tout $x \in V$. C'est à dire : $v_1^*(x) = \lambda v_2^*(x)$ et donc $v_2^* = \frac{1}{\lambda} v_1^*$. La réciproque est évidente. □

3.2.2 Définition de s_r et cas particuliers

Soit $r = (v, v^*) \in (V \setminus \{0\}) \times (V^* \setminus \{0\})$, on note s_r l'endomorphisme de V défini par :

$$s_r := 1 - \overline{r}$$

Autrement dit, pour $x \in V$ on a :

$$s_r(x) = x - v^*(x)v$$

Remarque 5. Pour $g \in \mathrm{GL}(V)$ on a : $s_{g \cdot r} = g s_r g^{-1}$ (cela sera prouvé dans le lemme 6).

Lemme 4. *On a les deux points suivants :*
• *Si $tr(r) = 1$ alors $H_r \bigoplus L_r = V$, et l'endomorphisme s_r est la projection sur H_r parallèlement à L_r.*
• *Si $tr(r) = 0$ alors $L_r \subseteq H_r$, puis $\overline{r}^2 = 0$ et l'endomorphisme s_r est une transvection.*

Démonstration. • Pour tout $x \in V$ on a $x = s_r(x) + v^*(x)v$. De plus, $v^*(s_r(x)) = v^*(x) - v^*(x)v^*(v) = 0$ car $v^*(v) = tr(r) = 1$, ainsi $s_r(x) \in H_r$. On a clairement $v^*(x)v \in \mathbb{K}v = L_r$.
Par ailleurs on a $H_r \cap L_r = \{0\}$, en effet il vient si l'on prend $x \in H_r \cap L_r$: $\exists \lambda \in \mathbb{K}$ tel que $x = \lambda v$ et $\overline{r}(x) = \overline{r}(\lambda v) = \lambda v^*(v)v = 0 \implies \lambda = 0$ car $v^*(v) = 1$ et $v \neq 0$. C'est à dire : $x = 0$.
Donc on a bien montré que $H_r \bigoplus L_r = V$. On vérifie aisément que $s_r(x) = 0$ si $x \in L_r$, que $s_r(x) = x$ si $x \in H_r$ et que $s_r^2 = s_r$.
• Soit $x \in L_r$ donc x s'écrit $x = \lambda v$ avec $\lambda \in \mathbb{K}$, on a $\overline{r}(x) = \lambda v^*(v)v = 0$ d'où $x \in \ker(\overline{r}) = H_r$. Ainsi, $L_r \subseteq H_r$. On voit que $\overline{r}^2(x) = v^*(v^*(x)v)v = 0$. On a clairement s_r une transvection où l'on prend la définition de transvection : tout endomorphisme u de V différent de l'identité tel qu'il existe un hyperplan H de V où $u(x) = x$ si $x \in H$ et pour tout $x \in V$, $u(x) - x \in H$. □

3.2.3 Racines et réflexions

Définition 14. Une **racine** de V est un élément r de $(V \setminus \{0\}) \times (V^* \setminus \{0\})$ tel que $tr(r) \neq 0, 1$.

Définition 15. Une **réflexion** de V est un endomorphisme de la forme s_r où r est une racine de V.

On considérera dans toute la suite, sauf mention contraire, une racine $r = (v, v^*)$ et on désignera par s_r sa réflexion associée. On définit : $z_r := 1 - tr(r)$.

Remarque 6. • On peut remarquer que l'on a : $z_r = \det(s_r) \neq 0, 1$ puis que l'on peut réécrire :

$$H_r = \ker(s_r - 1) \text{ et } L_r = Im(s_r - 1) = \ker(s_r - z_r 1)$$

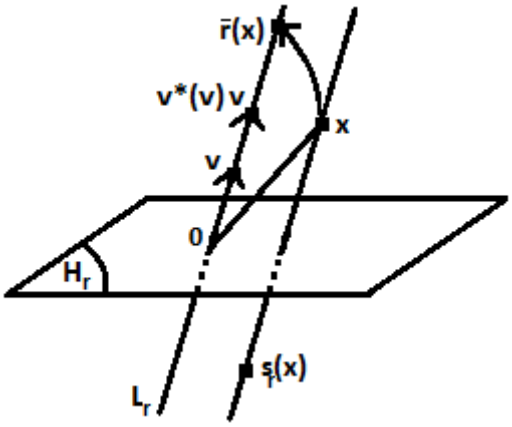

FIGURE 11 – Exemple de réflexion complexe non dégénérée : $tr(r) \neq 0, 1$

• On voit également que l'ordre de s_r est aussi l'ordre de z_r dans $\mathbb{K}^*$.
• On a également par le fait que $\det(s_r) \neq 0$: $s_r \in \mathrm{GL}(V)$ et donc on peut considérer l'action de s_r^n pour tout $n \in \mathbb{N}$ sur une racine $(x, x^*) \in (V \setminus \{0\}) \times (V^* \setminus \{0\})$:

$$s_r^n \cdot (x, x^*) = \left(x - \frac{1 - z_r^n}{1 - z_r} v^*(x)v \ , \ x^* - \frac{1 - z_r^{-n}}{1 - z_r} x^*(v)v^*\right)$$

Lemme 5. *On a : $H_r \bigoplus L_r = V$*

Démonstration. Soit $x \in V$, on peut écrire $x = x - tr(r)^{-1}v^*(x)v + tr(r)^{-1}v^*(x)v$. Clairement $tr(r)^{-1}v^*(x)v \in \mathbb{K}v = L_r$ et $x - tr(r)^{-1}v^*(x)v \in H_r$ car :

$$\overline{r}(x - tr(r)^{-1}v^*(x)v) = v^*(x)v - tr(r)^{-1}v^*(v)v^*(x)v = v^*(x)v - v^*(x)v = 0$$

De plus, $H_r \cap L_r = \{0\}$ car si $x \in H_r \cap L_r$ alors en particulier il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda v$ (car $x \in L_r$) et comme $x \in H_r$ on a $v^*(x)v = 0$ i.e. $\lambda v^*(v)v = 0$. Or $tr(r) \neq 0$ et $v \neq 0$ donc $\lambda = 0$ et ainsi $x = 0$. □

Nous allons voir que l'inverse, le conjugué ou encore la transposée d'une réflexion est encore une réflexion.

Lemme 6. *Soit $g \in \mathrm{GL}(V)$ et $r = (v, v^*)$ une racine, nous avons les points suivants :*
• *Le conjugué d'une réflexion est une réflexion et on a : $gs_rg^{-1} = s_{g \cdot r}$*
• *L'inverse d'une réflexion est une réflexion et on a : $s_r^{-1} = s_{r'}$ avec $r' := (v, -z_r^{-1}v^*)$*
• *La transposée d'une réflexion dans V est une réflexion dans V^* et on a : ${}^t s_r = s_{{}^t r}$ avec ${}^t r := (v^*, v)$*
• *La transposée de l'inverse d'une réflexion dans V est une réflexion dans V^* et on a : ${}^t s_r^{-1} = s_{\check{r}}$ avec $\check{r} := (-z_r^{-1}v^*, v)$*

Démonstration. • Soit $x \in V$, on a $s_{g \cdot r}(x) = x - (v^* \circ g^{-1})(x)g(v) = g[g^{-1}(x) - v^*(g^{-1}(x))v]$. Comme $gs_rg^{-1}(x) = g[g^{-1}(x) - v^*(g^{-1}(x))v]$ on a bien : $gs_rg^{-1} = s_{g \cdot r}$.
Ainsi, le conjugué d'une réflexion est bien une réflexion.
• Soit $x \in V$, on a :

$$(s_r \circ s_{r'})(x) = s_r(x + z_r^{-1}v^*(x)v) = s_r(x) + z_r^{-1}v^*(x)s_r(v) = x - v^*(x)v + z_r^{-1}v^*(x)(v - v^*(v)v)$$

Or on sait que $v^*(v) = tr(v)$ et $1 - tr(r) = z_r$ d'où : $(s_r \circ s_{r'})(x) = x$. On montre de manière analogue que $(s_{r'} \circ s_r)(x) = x$. On a ainsi $s_{r'} \circ s_r = s_r \circ s_{r'} = 1$ et l'inverse d'une réflexion est une réflexion.
• Soit $x^* \in V^*$, par définition de la transposée : ${}^t s_r(x^*) = x^* \circ s_r$. On a pour $x \in V$:

$${}^t s_r(x^*)(x) = x^*(x - v^*(x)v) = x^*(x) - v^*(x)x^*(v) = s_{{}^t r}(x^*)(x)$$

D'où : ${}^t s_r(x^*) = s_{{}^t r}(x^*)$ et ainsi : ${}^t s_r = s_{{}^t r}$. Donc la transposée d'une réflexion dans V est une réflexion dans V^*.
• Le quatrième point résulte de l'application du troisième et du deuxième point. □

Nous allons maintenant prouver un lemme qui permettra d'indicer des ensembles de réflexions de différentes manières.

Lemme 7. *Les applications* (1) *et* (2) *suivantes :*

$$\begin{cases} (1) & r \mapsto s_r \\ (2) & s \mapsto (\ker(s-1)\ ,\ Im(s-1)\ ,\ \det(s)) \end{cases}$$

définissent des bijections entre les ensembles suivants :
• *(i) L'ensemble des orbites de l'action $\cdot$ restreinte à K^* sur l'ensemble des racines de V.*
• *(ii) L'ensemble des réflexions de V.*
• *(iii) L'ensemble des triplets (H, L, z) où H est un hyperplan de V, L un sous-espace de dimension 1 de V tel que $H \bigoplus L = V$ et z un élément de $\mathbb{K}$ différent de 0 et 1.*

Démonstration. Il s'agit de montrer que le premier et le second point sont en bijection par (1) et que le second et le troisième point sont en bijection par (2).
- L'application (1) est bien définie entre les ensembles (i) et (ii), cela est justifié par les parties précédentes de ce rapport. Soit donc $r = (v_1, v_1^*)$ une racine représentante de son orbite sous l'action de $\mathbb{K}^*$. De même, soit une autre racine représentante $r' = (v_2, v_2^*)$. Supposons que $s_r = s_{r'}$ et donc, pour tout $x \in V$: $x - v_1^*(x)v_1 = x - v_2^*(x)v_2$. C'est à dire $v_1^*(x)v_1 = v_2^*(x)v_2$ (E) pour tout $x \in V$. Comme par définition on a v_2^* qui n'est pas la forme linéaire nulle, il existe $x_0 \in V$ tel que $v_2^*(x_0) \neq 0$. On obtient ainsi $v_2 = \frac{v_1^*(x_0)}{v_2^*(x_0)} v_1$ D'où $v_2 = \lambda v_1$ avec $\lambda = \frac{v_1^*(x_0)}{v_2^*(x_0)}$. Supposons que $v_1^*(x_0) = 0$ alors on aurait $v_2^*(x_0)v_2 = 0$ par (E). Et donc comme $v_2^*(x_0) \neq 0$, on aurait $v_2 = 0$, ce qui est exclut. Donc $\lambda \neq 0$. Ainsi s_r et $s_{r'}$ sont dans la même orbite de l'action $\cdot$ restreinte à $\mathbb{K}^*$.
On a prouvé que (1) est donc **injective**. Elle est clairement **surjective** par définition d'une réflexion de V.
- L'application (2) est bien définie entre les ensembles (ii) et (iii), cela est justifié par les parties précédentes de ce rapport. Soient s_r et $s_{r'}$ deux réflexions de V. Supposons que :

$$\begin{cases} \ker(s_r - 1) = \ker(s_{r'} - 1) \\ Im(s_r - 1) = Im(s_{r'} - 1) = \mathbb{K}v \\ \det(s_r) = \det(s_{r'}) \end{cases}$$

On sait que $\ker(s_r - 1) \bigoplus Im(s_r - 1) = V$ par le lemme 5. Donc, comme $s_r(x) = s_{r'}(x) = x$ sur $\ker(s_r - 1) = \ker(s_{r'} - 1)$ et qu'il existe $\lambda, \lambda' \in \mathbb{K}$ tels que $s_r(x) = \lambda x$ et $s_{r'}(x) = \lambda' x$ lorsque $x \in Im(s_r - 1) = Im(s_{r'} - 1) = \mathbb{K}v$: on a nécessairement $\lambda = \lambda'$ car $\det(s_r) = \det(s_{r'})$. D'où s_r et $s_{r'}$ coïncident sur $\ker(s_r - 1) \bigoplus Im(s_r - 1) = V$ et l'application (2) est donc **injective**.
Montrons donc la surjectivité de (2) : Soit (H, L, z) un triplet comme le point *(iii)*. Soit $v \in L$ un vecteur non nul de L (possible car sinon H ne serait pas un hyperplan car on aurait $H \bigoplus L = H = V$).
Comme $H \bigoplus L = V$, on peut prendre une base $(e_1, \cdots e_{n-1})$ de H et la compléter avec v pour former une base de V. Ainsi, on peut considérer e^* l'application coordonnée sur L telle que :

$$\begin{aligned} e^* : \ & V \longrightarrow \mathbb{K} \\ & x = a_1 e_1 + \cdots a_{n-1} e_{n-1} + a_n v \longmapsto a_n \end{aligned}$$

C'est une application linéaire à valeurs dans $\mathbb{K}$, donc un élément de V^*. On a naturellement :

$$e^*(v) = 1$$

Posons $v^* \in V^*$ telle que pour $x \in V$ on ait $v^*(x) = (1 - z)e^*(x)$.
Ainsi on obtient par linéarité : $v^*(v) = 1 - z$, i.e. $z = 1 - v^*(v)$ et on a bien $v^*(v) \neq 0, 1$ car

$z \neq 0, 1$.
On pose $\overline{r}$ telle que $\overline{r}(x) = v^*(x)v$ et on a bien $tr(r) \neq 0, 1$ par ce qui précède et l'on peut considérer s_r la réflexion associée à la racine $r = (v, v^*)$.
Il reste à vérifier que l'application (2) envoie bien s_r sur le triplet (H, L, z).
On a $\ker(s_r - 1) = \ker(\overline{r})$ et $x \in \ker(\overline{r}) \Leftrightarrow v^*(x) = 0 \Leftrightarrow x \in H$. Donc, $\ker(s_r - 1) = H$ et de même, $Im(s_r - 1) = \mathbb{K}v = L_r$. Par ailleurs, $\det(s_r) = z_r$ avec ici $z_r := 1 - tr(r) = 1 - v^*(v) = z$.
Donc (2) envoie bien s_r sur (H, L, z) et on a ainsi prouvé la **surjectivité**. □

Remarque 7. Une réflexion est diagonalisable (voir paragraphe précédent la remarque 6). Donc, sa restriction à un sous-espace stable l'est également.

Lemme 8. • *Soit V' un sous-espace de V stable par la réflexion s_r.*
Alors il vient, soit : V' est fixé par s_r (c'est à dire $V' \subseteq H_r$) soit : V' contient L_r et ainsi $V' = L_r \bigoplus (H_r \cap V')$.
• *Supposons que $V = V_1 \bigoplus V_2$ où V_1 et V_2 sont des sous-espaces stables par la réflexion s_r alors : soit H_r contient V_1 soit H_r contient V_2.*

Démonstration. • Si V' ne contient pas L_r alors $V' \subseteq H_r$ car $H_r \bigoplus L_r = V$. Donc V' est fixé par s_r car pour tout $x \in H_r$ $s_r(x) = x$.
Si V' contient L_r, on a bien $V' = L_r \bigoplus (H_r \cap V')$, en effet : $L_r \cap (H_r \cap V') = \{0\}$ et pour tout $x \in V'$ il vient : $x = x - v^*(x)v + v^*(x)v$. Comme $v^*(x)v \in L_r \subseteq V'$ on a $x - v^*(x)v \in V'$ par structure d'espace vectoriel. Donc comme de plus $x - v^*(x)v \in H_r$ on a bien $x - v^*(x)v \in (H_r \cap V')$ et le résultat.
• On applique le premier point à $V' = V_1$: soit H_r contient $V' = V_1$ et c'est terminé soit ce n'est pas le cas et donc V_1 contient L_r et on applique alors à nouveau le premier point à $V' = V_2$ ainsi nécessairement H_r contient V_2 car sinon V_2 contiendrait L_r. Et on aurait $L_r \subseteq V_1 \cap V_2$ ce qui est impossible par hypothèse car $V_1 \cap V_2 = \{0\}$. □

3.2.4 Orthogonalité et parallélisme entre racines

Définition 16. Soit $r = (v, v^*)$ une racine de V et $g \in \mathrm{GL}(V)$. On dira que r est une **racine propre** de g s'il existe $\lambda \in \mathbb{K}^*$ tel que : $g \cdot r = \lambda \cdot r = (\lambda v, \frac{1}{\lambda} v^*)$

Lemme 9. *Soit $r_1 = (v_1, v_1^*)$ et $r_2 = (v_2, v_2^*)$ deux racines de V. On a équivalence entre :*

$$\begin{cases} (i)\ s_{r_1} \cdot r_2 = r_2 \\ (ii)\ s_{r_2} \cdot r_1 = r_1 \\ (iii)\ L_{r_1} \subseteq H_{r_2} \text{ et } L_{r_2} \subseteq H_{r_1} \end{cases}$$

*Si l'une des conditions équivalentes ci-dessus est vérifiée, on dira alors que r_1 et r_2 sont **orthogonales**.*

Démonstration. • Montrons que $(i) \Leftrightarrow (iii)$: on sait que $s_{r_1} \cdot r_2 = (s_{r_1}(v_2), v_2^* \circ s_{r_1}^{-1})$.
- Supposons (i), on obtient donc $s_{r_1}(v_2) = v_2$ et $v_2^* \circ s_{r_1}^{-1} = v_2^*$. La première égalité nous donne que $L_{r_2} \subseteq H_{r_1}$ car si $x \in L_{r_2}$ alors il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda v_2$ et on obtient par linéarité : $s_{r_1}(x) = \lambda s_{r_1}(v_2) = \lambda v_2 = x$ i.e. $x \in H_{r_1}$ et on a montré que $L_{r_2} \subseteq H_{r_1}$.
Soit $x \in L_{r_1}$ alors il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda v_1$. On obtient avec la deuxième égalité :

$$v_2^*(x) = \lambda v_2^*(v_1) = v_2^* \circ s_{r_1}^{-1}(\lambda v_1) = \lambda v_2^* \circ s_{r_1}^{-1}(v_1)$$

(par le fait que l'inverse d'une réflexion est une réflexion et en utilisant la linéarité des endomorphismes). Par le lemme 6, on sait que $s_{r_1}^{-1} = s_r'$ avec $r' = (v_1, -z_{r_1}^{-1} v_1^*)$. Donc $s_{r_1}^{-1}(v_1) = v_1 + z_{r_1}^{-1} v_1^*(v_1) v_1$.
Comme $v_1^*(v_1) = tr(r_1) = 1 - z_{r_1}$, on obtient :

$$s_{r_1}^{-1}(v_1) = z_{r_1}^{-1} v_1$$

Ainsi :

$$v_2^*(x) = z_{r_1}^{-1} \lambda v_2^*(v_1) = z_{r_1}^{-1} v_2^*(x)$$

D'où comme $z_{r_1}^{-1} \neq 1$ car r_1 est une racine de V, on a nécessairement $v_2^*(x) = 0$ i.e. $x \in H_{r_2}$ et on a montré que $L_{r_1} \subseteq H_{r_2}$. D'où $(i) \implies (iii)$.
- Réciproquement, supposons que $L_{r_1} \subseteq H_{r_2}$ et $L_{r_2} \subseteq H_{r_1}$.
On a $s_{r_1}(v_2) = v_2$ car on a $v_2 \in L_{r_2} \subseteq H_{r_1}$. De plus, on a $v_2^* \circ s_{r_1}^{-1} = v_2^*$. En effet, soit $x \in V$ on a bien $v_2^* \circ s_{r_1}^{-1}(x) = v_2^*(x)$ car :

$$v_2^* \circ s_{r_1}^{-1}(x) = v_2^*(x + z_{r_1}^{-1} v_1^*(x) v_1) = v_2^*(x) + z_{r_1}^{-1} v_1^*(x) v_2^*(v_1)$$

Or $v_1 \in L_{r_1} \subseteq H_{r_2}$ donc $v_2^*(v_1) = 0$ et ainsi $v_2^* \circ s_{r_1}^{-1}(x) = v_2^*(x)$. D'où on a bien $s_{r_1} \cdot r_2 = r_2$ et on a montré que $(iii) \implies (i)$ et ainsi l'équivalence.
• En échangeant les notations r_1 et r_2 et par symétrie du problème, on a aussi $(ii) \Leftrightarrow (iii)$.
On a donc montré que les trois conditions sont équivalentes. □

Lemme 10. *Soit $r_1 = (v_1, v_1^*)$ et $r_2 = (v_2, v_2^*)$ deux racines de V. On a équivalence entre :*

$$\begin{cases} (i)\ s_{r_1} \cdot r_2 = z_{r_1} r_2 \\ (ii)\ s_{r_2} \cdot r_1 = z_{r_2} r_1 \\ (iii)\ L_{r_1} = L_{r_2} \text{ et } H_{r_1} = H_{r_2} \end{cases}$$

*Si l'une des conditions équivalentes ci-dessus est vérifiée, on dira alors que r_1 et r_2 sont **parallèles**.*

Démonstration. Comme dans la preuve précédente, montrons que $(i) \Leftrightarrow (iii)$.
- Supposons (i), on obtient donc $s_{r_1}(v_2) = z_{r_1} v_2$ et $v_2^* \circ s_{r_1}^{-1} = z_{r_1}^{-1} v_2^*$. Soit $x \in L_{r_2}$, donc il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda v_2$. On a ainsi par la première égalité : $s_{r_1}(x) = z_{r_1} \lambda v_2 = z_{r_1} x$ i.e. $x \in \ker(s_{r_1} - z_{r_1} 1) = L_{r_1}$ par la remarque 6. D'où $L_{r_2} \subseteq L_{r_1}$.
Par égalité des dimensions de L_{r_1} et L_{r_2}, on en déduit que $L_{r_1} = L_{r_2}$.
Soit $x \in H_{r_1}$. On a par ailleurs :

$$v_2^* \circ s_{r_1}^{-1}(x) = v_2^*(x + z_{r_1}^{-1} v_1^*(x) v_1) = v_2^*(x) + z_{r_1}^{-1} v_1^*(x) v_2^*(v_1) = v_2^*(x)$$

Et par la deuxième égalité on obtient ainsi :

$$z_{r_1}^{-1} v_2^*(x) = v_2^*(x)$$

C'est à dire nécessairement $v_2^*(x) = 0$ car r_2 est une racine. Et ainsi $x \in H_{r_2}$. D'où : $H_{r_1} \subseteq H_{r_2}$ et par égalité des dimensions : $H_{r_1} = H_{r_2}$. On a donc bien montré que $(i) \implies (iii)$.
- Supposons (iii), on sait donc qu'il existe $\lambda \in \mathbb{K}$ tel que $v_2 = \lambda v_1$ (par $L_{r_1} = L_{r_2}$). Ainsi, on a :

$$s_{r_1}(v_2) = \lambda s_{r_1}(v_1) = \lambda(v_1 - v^*(v_1) v_1) = \lambda v_1 (1 - tr(r_1)) = z_{r_1} v_2$$

Soit $x \in H_{r_1}$, il vient immédiatement :

$$v_2^* \circ s_{r_1}^{-1}(x) = v_2^*(x + z_{r_1}^{-1} v_1^*(x) v_1) = v_2^*(x) + z_{r_1}^{-1} v_1^*(x) v_2^*(v_1) = 0$$

car $H_{r_1} = H_{r_2}$ (c'est à dire $v_1^*(x) = v_2^*(x) = 0$). Et ainsi, $v_2^* \circ s_{r_1}^{-1} = z_{r_1}^{-1} v_2^*$ sur H_{r_1}.
Soit $x \in L_{r_1} = L_{r_2}$, donc il existe $\lambda \in \mathbb{K}$ tels que $x = \lambda v_1$. On a d'une part :

$$z_{r_1}^{-1} v_2^*(x) = \lambda z_{r_1}^{-1} v_2^*(v_1)$$

Et d'autre part :

$$v_2^* \circ s_{r_1}^{-1}(x) = v_2^*(x + z_{r_1}^{-1} v_1^*(x) v_1) = v_2^*(x) + z_{r_1}^{-1} v_1^*(x) v_2^*(v_1) = \lambda z_{r_1}^{-1} v_2^*(v_1)$$

Don comme $H_{r_1} \bigoplus L_{r_1} = V$, on a montré que pour tout $x \in V$ $z_{r_1}^{-1} v_2^*(x) = v_2^* \circ s_{r_1}^{-1}(x)$. Donc on a bien montré que $s_{r_1} \cdot r_2 = z_{r_1} r_2$ c'est à dire $(iii) \implies (i)$ et donc l'équivalence.
• De même, par symétrie du problème en échangeant les rôles de r_1 et r_2 ce qui précède montre que $(ii) \Leftrightarrow (iii)$ et ainsi que les trois conditions sont équivalentes. □

Lemme 11. *Soit $r_1 = (v_1, v_1^*)$ et $r_2 = (v_2, v_2^*)$ deux racines de V. On a équivalence entre :*

$$\begin{cases} (i)\ s_{r_1} s_{r_2} = s_{r_2} s_{r_1} \\ (ii)\ r_1 \text{ est une racine propre de } s_{r_2} \\ (iii)\ r_2 \text{ est une racine propre de } s_{r_1} \\ (iiii)\ r_1 \text{ et } r_2 \text{ sont soit orthogonales soit parallèles.} \end{cases}$$

Démonstration. • Montrons que $(i) \Leftrightarrow (ii)$:
- Supposons (i), on sait que r_1 est une racine propre de $s_{r_2} \Leftrightarrow$ il existe $\lambda \in \mathbb{K}^*$ tel que :

$$(\lambda v_1, \lambda^{-1} v_1^*) = (s_{r_2}(v_1), v_1^* \circ s_{r_2}^{-1})$$

On sait que :

$$s_{r_1}(v_1) = v_1 - tr(r_1)v_1 = z_{r_1} v_1$$

Donc on obtient :

$$s_{r_2} s_{r_1}(v_1) = z_{r_1} s_{r_2}(v_1)$$

Et comme :

$$s_{r_1} s_{r_2}(v_1) = s_{r_2}(v_1) - v_1^*(s_{r_2}(v_1))v_1$$

Par l'égalité fournie par (i) on obtient ainsi :

$$z_{r_1} s_{r_2}(v_1) = s_{r_2}(v_1) - v_1^*(s_{r_2}(v_1))v_1$$

Et donc :

$$s_{r_2}(v_1) = \frac{v_1^*(s_{r_2}(v_1))}{1 - z_{r_1}} v_1$$

Si on avait $v_1^*(s_{r_2}(v_1)) = 0$ alors $s_{r_2}(v_1) \in H_{r_1}$ et donc $s_{r_1} s_{r_2}(v_1) = s_{r_2}(v_1)$ or on a vu ci-dessus que $s_{r_2} s_{r_1}(v_1) = z_{r_1} s_{r_2}(v_1)$ et encore par l'égalité (i) on aurait ainsi : $s_{r_2}(v_1) = z_{r_1} s_{r_2}(v_1)$ et donc nécessairement :

$$s_{r_2}(v_1) = 0$$

C'est à dire $v_1 \in \ker(s_{r_2})$. Or $\det(s_{r_2}) \neq 0$ par la remarque 6, donc $\ker(s_{r_2}) = \{0\}$ et ainsi $v_1 = 0$, ce qui est absurde. D'où si l'on pose :

$$\lambda = \frac{v_1^*(s_{r_2}(v_1))}{1 - z_{r_1}}$$

On a bien : $s_{r_2}(v_1) = \lambda v_1$ avec $\lambda \neq 0$. Par ailleurs, on a pour $x \in V$:

$$v_1^* \circ s_{r_2}^{-1}(x) = v_1^*(x + z_{r_2}^{-1} v_2^*(x) v_2) = v_1^*(x) + z_{r_2}^{-1} v_2^*(x) v_1^*(v_2)$$

En développant $s_{r_2}(v_1)$ du λ on obtient bien : $v_1^* \circ s_{r_2}^{-1}(x) = \lambda^{-1} v_1^*$. Ainsi, on a $(i) \implies (ii)$
- Supposons (ii), donc il existe $\lambda \in \mathbb{K}^*$ tel que : $(\lambda v_1, \lambda^{-1} v_1^*) = (s_{r_2}(v_1), v_1^* \circ s_{r_2}^{-1})$
Soit $x \in L_{r_1}$, donc il existe $\mu \in \mathbb{K}$ tel que $x = \mu v_1$. On a d'une part :

$$s_{r_1}(x) = \mu s_{r_1}(v_1) = \mu(v_1 - v_1^*(v_1)v_1) = \mu z_{r_1} v_1$$

Et d'autre part (en se servant de l'hypothèse) :

$$s_{r_2}(x) = \mu s_{r_2}(v_1) = \mu\lambda v_1 = \lambda x$$

Ainsi :

$$s_{r_2} s_{r_1}(x) = \mu z_{r_1} s_{r_2}(v_1) = \mu\lambda z_{r_1} v_1 = \lambda z_{r_1} x$$
$$s_{r_1} s_{r_2}(x) = \lambda s_{r_1}(x) = \lambda\mu z_{r_1} v_1 = \lambda z_{r_1} x$$

D'où : $s_{r_2} s_{r_1}(x) = s_{r_1} s_{r_2}(x)$.
Soit $x \in H_{r_1}$, on a donc $s_{r_1}(x) = x$ et ainsi : $s_{r_2} s_{r_1}(x) = s_{r_2}(x)$. D'autre part : $s_{r_2}(x) = x - v_2^*(x)v_2$ donc :

$$s_{r_1} s_{r_2}(x) = s_{r_1}(x) - v_2^*(x) s_{r_1}(v_2) = x - v_2^*(x)v_2 + v_2^*(x)v_1^*(v_2)v_1$$

De plus, à nouveau par l'hypothèse on sait que :

$$v_1^* \circ s_{r_2}^{-1}(x) = v_1^*(x) + z_{r_2}^{-1} v_2^*(x) v_1^*(v_2) = \lambda^{-1} v_1^*(x)$$

Ainsi on obtient :

$$v_2^*(x) v_1^*(v_2) = z_{r_2}(\lambda^{-1} - 1) v_1^*(x)$$

Et comme $x \in H_{r_1}$ on obtient : $v_2^*(x)v_1^*(v_2) = 0$ et ainsi : $s_{r_1}s_{r_2}(x) = x - v_2^*(x)v_2 + v_2^*(x)v_1^*(v_2)v_1 = x - v_2^*(x)v_2 = s_{r_2}(x) = s_{r_2}s_{r_1}(x)$ et on a ainsi montré que :

$$s_{r_1} s_{r_2} = s_{r_2} s_{r_1}$$

D'où $(ii) \implies (i)$ et l'équivalence annoncée : $(i) \Leftrightarrow (ii)$.
• En échangeant les rôles de r_1 et r_2 l'équivalence précédente montre que $(i) \Leftrightarrow (iii)$.
• Montrons que $(iiii) \Leftrightarrow (ii)$
- Supposons $(iiii)$, donc il existe $\lambda \in \mathbb{K}^*$ avec $\lambda = z_{r_2}$ ou $\lambda = 1$ tel que :

$$(\lambda v_1, \lambda^{-1} v_1^*) = (s_{r_2}(v_1), v_1^* \circ s_{r_2}^{-1})$$

Donc cela signifie que r_1 est une racine propre de s_{r_2} et donc $(iiii) \implies (ii)$.
- Réciproquement supposons (ii), donc il existe $\lambda \in \mathbb{K}^*$ tel que :

$$(\lambda v_1, \lambda^{-1} v_1^*) = (s_{r_2}(v_1), v_1^* \circ s_{r_2}^{-1})$$

En particulier on a $s_{r_2}(v_1) = \lambda v_1$ donc $v_1 - v_2^*(v_1)v_2 = \lambda v_1$ et ainsi $(1-\lambda)v_1 = v_2^*(v_1)v_2$ et en composant l'égalité par v_2^* :

$$(1-\lambda) v_2^*(v_1) = v_2^*(v_1) tr(r_2)$$

et donc :

$$(1 - \lambda - tr(r_2)) v_2^*(v_1) = 0$$

Ainsi, soit $v_2^*(v_1) \neq 0$ et on obtient $\lambda = z_{r_2}$ soit $v_2^*(v_1) = 0$ et comme on a par le premier point nécessairement :

$$\lambda = \frac{v_1^*(s_{r_2}(v_1))}{1 - z_{r_1}} = \frac{v_1^*(v_1 - v_2^*(v_1)v_2)}{tr(r_1)} = \frac{tr(r_1) - v_2^*(v_1)v_1^*(v_2)}{tr(r_1)}$$

Il vient alors $\lambda = 1$. Ce qui conclut la preuve en application des deux lemmes précédents. □

3.2.5 Groupes et décomposition orthogonale

Soit R un ensemble fini de réflexions de V. On notera G_R le sous-groupe de $\mathrm{GL}(V)$ engendré par les réflexions R.

Définition 17. Un groupe de réflexion complexes est un sous-groupe fini de $\mathrm{GL}(V)$ engendré par un ensemble (fini) R de réflexions.

On notera V^{G_R} l'ensemble des points fixes de V sous l'action de G_R. Autrement dit :

$$V^{G_R} := \{x \in V \mid \forall g \in G_R,\ g(x) = x\}$$

Lemme 12. *On a l'égalité*[2]

$$V^{G_R} = \bigcap_{r \in R} H_r$$

2. On devrait plutôt écrire : $V^{G_R} = \bigcap_{\{r \mid s_r \in R\}} H_r$ mais pour faciliter l'écriture, on notera abusivement le prédicat par : $r \in R$. Cela est également légitimé par le lemme 7.

Démonstration. • Soit $x \in V^{G_R}$, alors $\forall g \in G_R,\ g(x) = x$ et en particulier pour $s_r \in R \subseteq G_R$: $s_r(x) = x$ i.e. $x \in H_r$ et donc $x \in \bigcap_{r\in R} H_r$. On a ainsi montré que $V^{G_R} \subseteq \bigcap_{r\in R} H_r$.

• Soit $x \in \bigcap_{r\in R} H_r$ et soit $g \in G_R$, comme R est une partie génératrice du groupe G_R on peut écrire :

$$g = s_{r_1}^{\epsilon_1} \cdots s_{r_m}^{\epsilon_m} \text{ avec } \epsilon_i = \pm 1 \text{ et } s_{r_i} \in R$$

Comme pour tout $i \in [\![1, m]\!]$ on sait que $s_{r_i}(x) = x$ et $s_{r_i}^{-1}(x) = x$, on en déduit que $g(x) = x$ et ainsi $x \in V^{G_R}$. D'où : $\bigcap_{r\in R} H_r \subseteq V^{G_R}$ et cela prouve le lemme. □

Définition 18. On dira que l'ensemble R est complet s'il est stable par la G_R-conjugaison. C'est à dire, si $g \in G_R$ et $s_r \in R$ alors $gs_rg^{-1} \in R$.

On supposera dans la suite, sauf mention contraire, que R est un ensemble complet. Ainsi G_R est un sous-groupe normal du sous-groupe de $\mathrm{GL}(V)$ qui stabilise R. Posons l'espace V_R suivant :

$$V_R := \sum_{r\in R} L_r$$

Rappels sur quelques notions de représentations de groupes :

• Une *représentation linéaire* du groupe G dans le $\mathbb{K}$-espace vectoriel de dimension finie V est une action de G sur V telle que pour tout $g \in G$, l'application $\varphi_g : x \mapsto g \cdot x$ est un automorphisme de V.
Il revient au même de dire que le morphisme de groupe $\varphi : G \to \mathfrak{S}(V)$ (qui à $g \in G$ associe φ_g) associé à l'action de groupe possède son image dans $\mathrm{GL}(V)$.
On identifiera donc une représentation linéaire de G à un morphisme $\varphi : G \to \mathrm{GL}(V)$.
• Un sous-espace vectoriel W de V est dit *stable pour la représentation*[3] si pour tout $g \in G$, W est stable par $\varphi(g)$.
• Si W est stable pour la représentation, on appelle *représentation induite* sur W, l'action de G sur W héritée par restriction de l'action initiale de G sur V.
• La représentation est dite *simple* (ou *irréductible*) si V n'admet pas de sous-espaces stables autres que $\{0\}$ et V.
• La représentation est dite *indécomposable* si l'on ne peut pas écrire V comme somme directe de sous-espaces stables non triviaux (i.e. différents de $\{0\}$ et V).
• La représentation est dite *complètement réductible* si V est somme directe de sous-espaces stables tels que les représentations induites sont simples.

Comme R est complet, V_R est stable par l'action de G_R.
En effet, si $s_r \in R$ alors on a $L_r = Im(s_r - 1)$ et si $g \in G_R$, on a par la remarque 5 :

$$gs_rg^{-1} = s_{g\cdot r} \in R$$

Théorème 4. ***Théorème de Maschke***
Soit G un groupe fini d'ordre $\#G$ qui n'est pas un multiple de la caractéristique du corps $\mathbb{K}$. Alors, toute représentation $\mathbb{K}$-linéaire de G est complètement réductible.

Démonstration. Montrons d'abord que pour toute représentation de G dans un $\mathbb{K}$-espace vectoriel V, tout sous-espace stable W de V admet un supplémentaire stable.
Soit p un projecteur quelconque sur W. On construit le projecteur $\tilde{p}$ de la manière suivante :

$$\tilde{p} := \frac{1}{\#G} \sum_{g\in G} \varphi(g) \circ p \circ \varphi(g)^{-1}$$

- Vérifions qu'il s'agit effectivement d'un projecteur :
Pour tout $g \in G$ et $x \in V$ on a $p(\varphi(g)^{-1}(x)) \in W$ et comme W est stable, on obtient :

$$(\varphi(g) \circ p \circ \varphi(g)^{-1})(x) \in W$$

3. Par la suite, on commettra l'abus de langage "stable" pour raccourcir l'appellation "stable pour la représentation".

Par structure d'espace vectoriel, on a donc : $\tilde{p}(x) \in W$ et ainsi $Im(\tilde{p}) \subseteq W$. Soit $x \in W$, on sait que $\varphi(g)^{-1}(x) \in W$ par stabilité de W. Ainsi $p(\varphi(g)^{-1}(x)) = \varphi(g)^{-1}$ et on a donc $(\varphi(g) \circ p \circ \varphi(g)^{-1})(x) = x$ et l'on déduit $\tilde{p}(x) = x$. Ceci montre à la fois que $W \subseteq Im(\tilde{p})$ et à la fois que $\tilde{p}$ est un projecteur d'image W.
- Montrons une propriété du projecteur $\tilde{p}$: pour tout $g_0 \in G$ on a $\varphi(g_0) \circ \tilde{p} = \tilde{p} \circ \varphi(g_0)$ ($\tilde{p}$ commute avec l'action φ). En effet, on peut écrire :

$$\varphi(g_0) \circ \tilde{p} \circ \varphi(g_0)^{-1} = \frac{1}{\#G} \sum_{g \in G} \varphi(g_0)\varphi(g) \circ p \circ \varphi(g)^{-1}\varphi(g_0)^{-1}$$

et donc :

$$\varphi(g_0) \circ \tilde{p} \circ \varphi(g_0)^{-1} = \frac{1}{\#G} \sum_{g \in G} \varphi(g_0 g) \circ p \circ \varphi(g_0 g)^{-1}$$

Comme $g \mapsto g_0 g$ est une bijection de G, il s'en suit :

$$\varphi(g_0) \circ \tilde{p} \circ \varphi(g_0)^{-1} = \tilde{p}$$

et l'on déduit la propriété : $\varphi(g_0) \circ \tilde{p} = \tilde{p} \circ \varphi(g_0)$.
- Prouvons maintenant le théorème de Maschke. Comme $\tilde{p}$ est un projecteur d'image W et commute avec l'action de G, on en déduit que $\ker(\tilde{p})$ est un supplémentaire stable de W dans V.
- Le théorème découle ensuite par récurrence forte sur la dimension de $n := V$:
Initialisation : Pour $n = 0, 1$ la représentation de groupe est simple donc complètement réductible.
Hérédité : Supposons le résultat vrai au rang $n \geq 2$. Si la représentation est simple, elle est alors complètement réductible. Si elle n'est pas simple, on peut prendre W un sous-espace stable non trivial. Par ce qui précède, on peut trouver un supplémentaire stable de W dans V en prenant le noyau de $\tilde{p}$. Comme les dimensions de W et du supplémentaire sont strictement inférieures à celle de V, on applique l'hypothèse de récurrence sur chaque sous-espace. Et cela nous montre bien que la représentation est complètement réductible. □

Un corollaire immédiat du théorème de Maschke est que si l'on suppose G fini et $\mathbb{K}$ un corps de caractéristique 0, alors toute représentation $\mathbb{K}$-linéaire de G est complètement réductible. **On supposera dans toute la suite que l'on satisfait cette hypothèse**.

Par les rappels précédents, l'action induit donc dorénavant une représentation complètement réductible de G_R sur V

Lemme 13. *On possède ainsi l'égalité : $V = V_R \bigoplus V^{G_R}$ et la représentation induite sur V_R induit un isomorphisme entre G_R et son image dans* $\mathrm{GL}(V_R)$.

Démonstration. • Montrons tout d'abord l'égalité $V = V_R \bigoplus V^{G_R}$:
On a vu que l'espace V_R est stable par l'action de G_R, donc il existe un supplémentaire V' stable par G_R également (reprendre la première partie de la preuve du théorème de Maschke). Pour $r \in R$, l'espace V_R contient le sous-espace propre non trivial de dimension 1 de s_r donc H_r contient V' par le lemme 8. Il s'en suit que $V' \subseteq \bigcap_{r \in R} H_r = V^{G_R}$. Montrons que $V_R \cap V^{G_R} = 0$.
Comme V^{G_R} est stable par G_R, il existe un supplémentaire V'' de V^{G_R} dans V stable par G_R. Pour $r \in R$, on a nécessairement $L_r \subseteq V''$ (car sinon on aurait $L_r \subseteq H_r$ par le lemme 8 et donc s_r serait triviale et comme $V = V^{G_R} \bigoplus V''$ on obtiendrait une contradiction). D'où $V_R \subseteq V''$ et en particulier on obtient que $V_R \cap V^{G_R} = 0$.
• La représentation induite considérée est la représentation $\varphi : G_R \to \mathrm{GL}(V_R)$. Comme φ est un morphisme de groupes, on peut considérer son noyau $\ker(\varphi) = \{g \in G_R \mid \varphi_g = Id_{V_R}\}$.
Soit $g \in G_R$ tel que $g \neq Id_{G_R}$ donc il existe $x \in V$ tel que $g(x) \neq x$. On a nécessairement $x \in V_R$ car si pour tout $x \in V_R$, $g(x) = x$ alors comme par définition de V^{G_R} on a pour tout $x \in V^{G_R}$: $g(x) = x$ on aurait ainsi $g(x) = x$ pour tout $x \in V$ car $V = V_R \bigoplus V^{G_R}$ et alors $g = Id_{G_R}$ ce qui est exclu. Donc si $g \neq Id_{G_R}$, on a nécessairement $x \in V_R$ tel que $g(x) \neq x$ et ainsi $\varphi_g \neq Id_{V_R}$. D'où :

$$\ker(\varphi) = \{Id_{G_R}\}$$

Ainsi on a bien φ injective et évidemment surjective sur son image, d'où le fait que la représentation induite sur V_R induit un isomorphisme entre G_R et son image dans $\mathrm{GL}(V_R)$. □

On notera $\sim$ la **relation d'équivalence sur l'ensemble des racines** obtenue comme étant la fermeture transitive [4] de la relation $\mathcal{R}$:"r et r' ne sont pas orthogonales".

Lemme 14. *Si $r \sim r'$ et si $g \in G_R$, alors $g \cdot r \sim g \cdot r'$. En particulier les classes d'équivalences pour la relation $\sim$ sont stables par G_R.*

Démonstration. Soit $g \in G_R$ on suppose que $r \sim r'$ donc il existe $r = r_0, r_1, \cdots, r_{m-1}, r_m = r'$ tels que $r_i \mathcal{R} r_{i+1}$. Montrons que si $r_i \mathcal{R} r_{i+1}$ alors $(g \cdot r_i) \mathcal{R} (g \cdot r_{i+1})$. Procédons par l'absurde : Si $g \cdot r_i$ et $g \cdot r_{i+1}$ sont orthogonales alors par le lemme 9, il vient :

$$s_{(g \cdot r_i)} \cdot (g \cdot r_{i+1}) = (g \cdot r_{i+1})$$

Comme on sait par la remarque 5 que : $s_{(g \cdot r_i)} = g s_{r_i} g^{-1}$, on obtient :

$$g \cdot s_{r_i} \cdot r_{i+1} = g \cdot r_{i+1}$$

En multipliant par g^{-1} à gauche de chaque côté de l'égalité, on obtient finalement :

$$s_{r_i} \cdot r_{i+1} = r_{i+1}$$

Et à nouveau par le lemme 9, on en déduit que r_i et r_{i+1} sont orthogonales, donc on ne peut avoir $r_i \mathcal{R} r_{i+1}$ et cela fournit une contradiction. Ainsi nécessairement : $(g \cdot r_i) \mathcal{R} (g \cdot r_{i+1})$ et l'on en déduit :

$$g \cdot r \sim g \cdot r'$$

□

Remarque 8. Le nombre de classes d'équivalence pour $\sim$ (on notera k ce nombre) est majoré par la dimension de V.

En effet, prenons $r_1 = (v_1, v_1^*), \cdots, r_m = (v_m, v_m^*)$ des racines qui sont 2 à 2 dans des classes d'équivalences différentes. On va montrer que $(v_1, \cdots, v_m)$ sont linéairement indépendants. Supposons que :

$$\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$$

En appliquant v_i^* à l'égalité précédente, comme les r_i sont 2 à 2 orthogonales, il vient :

$$\lambda_i v_i^*(v_i) = 0$$

C'est à dire $\lambda_i = 0$ pour tout $i \in [\![1, m]\!]$ et donc le nombre de classes d'équivalences est majoré par la dimension de V.

On notera donc $Rac = Rac_1 \sqcup \cdots \sqcup Rac_k$ la décomposition de l'ensemble des racines en classes d'équivalences pour $\sim$.
On notera également G_i le sous-groupe de G_R engendré par les réflexions s_r pour $r \in Rac_i$.
Enfin nous noterons V_i le sous-espace de V engendré par les espaces L_r lorsque $r \in Rac_i$.

Lemme 15. *On a les trois points suivants :*
- *Le groupe G_i agit trivialement sur $\sum_{j \neq i} V_j$*
- *Pour $1 \leq i \neq j \leq k$, les groupes G_i et G_j commutent.*
- *On a l'égalité : $G_R = G_1 \cdots G_k$ (produit de groupes).*

4. C'est à dire la plus petite relation transitive sur l'ensemble des racines contenant la relation $\mathcal{R}$

Démonstration. • Soit $s_r \in G_i$ telle que $r = (v_1, v_i^*) \in Rac_i$ et soit $r_j = (v_j, v_j^*) \in Rac_j$ avec $i \neq j$.
Comme on a :

$$s_r(v_j) = v_j - v_i^*(v_j)v_i$$

Comme r et r_j sont orthogonales, il vient : $v_i^*(v_j) = 0$ d'où :

$$s_r(v_j) = v_j$$

Ainsi par linéarité des endomorphismes que représentent les réflexions, on peut conclure que G_i agit trivialement sur $\sum_{j \neq i} V_j$.
• Soit $s_i \in G_i$ (associée à la racine $r_i = (v_i, v_i^*)$) et $s_j \in G_j$ (associée à la racine $r_j = (v_j, v_j^*)$) telles que $i \neq j$ on a pour $x \in V$:

$$s_i s_j(x) = s_j(x) - v_i^*(s_j(x))v_i$$

C'est à dire :

$$s_i s_j(x) = x - v_j^*(x)v_j - v_i^*(x - v_j^*(x)v_j)v_i$$

On a par linéarité et en utilisant l'orthogonalité de r_i et r_j :

$$s_i s_j(x) = x - v_j^*(x)v_j - v_i^*(x)v_i$$

De même en échangeant les indices i et j par symétrie de l'expression ci-dessus :

$$s_j s_i(x) = x - v_j^*(x)v_j - v_i^*(x)v_i$$

D'où :

$$s_i s_j = s_j s_i$$

Et on a bien que les groupes G_i et G_j commutent.
• On a un sens évident : $G_i \cdots G_k \subseteq G_R$ par structure de groupes.
Soit $g \in G_R$, comme G_R est engendré par un ensemble fini R de réflexions, on peut écrire :

$$g = s_{r_1}^{\epsilon_1} \cdots s_{r_m}^{\epsilon_m} \text{ avec } \epsilon_i = \pm 1 \text{ et } s_{r_i} \in R$$

De plus, pour tout $i \in [\![1, m]\!]$ il existe $j \in [\![1, k]\!]$ tel que $r_i \in Rac_j$ car $r_i \in Rac = Rac_1 \sqcup \cdots \sqcup Rac_k$. Donc en regroupant les r_i qui sont dans Rac_j et en notant g_j le produit des $s_{r_i}^{\epsilon_i}$ lorsque $r_i \in Rac_j$ on obtient :

$$g = g_1 \cdots g_k$$

avec $g_j \in G_j$ et d'où le résultat : $G_R \subseteq G_i \cdots G_k$. □

Lemme 16. *On suppose toujours que la représentation induite par l'action de G_R sur V est complètement réductible. On a les points suivants :*
• *Pour $1 \leq i \leq k$, la représentation induite par l'action de G_i sur V_i est irréductible.*
• $V_R = \bigoplus_{i=1}^{k} V_i$
• *On a l'égalité : $G_R = G_1 \times \cdots \times G_k$ (produit direct de groupes).*

Démonstration. • Le sous-espace V_i est stable par G et l'action de G sur un sous-espace stable est complètement réductible par hypothèse. De plus l'image de G dans $\mathrm{GL}(V_i)$ est la même que l'image de G_i dans $\mathrm{GL}(V_i)$, donc en déduit que que l'action de G_i sur V_i est complètement réductible.
Supposons que $R = R_i$ (c'est à dire qu'il n'y ait qu'une seule classe d'équivalence). Donc on a :

$$V = V_R \text{ et } G = G_i$$

Montrons que V_i est irréductible pour l'action de G_i. Comme V est complètement réductible pour l'action de G on peut écrire :

$$V = V' \bigoplus V''$$

avec V' et V'' des sous-espaces stables par G, montrons que soit V' soit V'' est égal à V. Définissons :

$$R' := \left\{ s_r \in R \mid L_r \subseteq V' \right\} \text{ et } R'' := \left\{ s_r \in R \mid L_r \subseteq V'' \right\}$$

Par le lemme 8, on remarque que si $r \in R'$ alors $V'' \subseteq H_r$ et lorsque $r \in R''$ on a $V' \subseteq H_r$. Ainsi cela montre que tout élément de R' est orthogonal à tout élément de R''. Donc soit R' soit R'' est égal à R et on en déduit que $V' = V$ ou $V'' = V$.
• Par le lemme précédent, on en déduit que :

$$\sum_{j \neq i} V_j \subseteq V^{G_i}$$

Par le premier point et par le lemme 13, on a :

$$V_i \cap \sum_{j \neq i} V_j = 0$$

• Un élément $g \in G_i$ qui appartient aussi à $\prod_{j \neq i} V_j$ agit trivialement sur V_i. A nouveau par le premier point et par le lemme 13, la représentation de G_i sur V_i est fidèle et on a donc $g = Id$. □

3.2.6 Classification de Shephard-Todd

On supposera dans cette sous-partie que $\mathbb{K} = \mathbb{C}$.

On va construire tout d'abord une famille infinie de groupes, que l'on notera $G(de, e, r)$. Cette famille de groupes dépend donc de 3 paramètres : d, e et r trois entiers strictement positifs.

• Soit $D_r(de)$ l'ensemble des matrices complexes de taille $r \times r$ diagonales, dont les coefficients de la diagonale sont à valeur dans μ_{de} (le groupe des racines complexes de-ièmes de l'unité).

• L'application suivante définit un morphisme de groupes surjectif :

$$(\det)^d : D_r(de) \to \mu_e$$

En effet, le déterminant étant un morphisme de groupes, on en déduit que $(\det)^d$ est également un morphisme de groupes.
Soit $y := \exp(\frac{2ik\pi}{e})$ une racine e-ième de l'unité. On prend la matrice ci-dessous :

$$\left(\begin{array}{c|c} I_{r-1} & 0 \\ \hline 0 & \exp(\frac{2ik\pi}{de}) \end{array} \right)$$

Cette matrice est bien dans $D_r(de)$ et est envoyé sur y par $(\det)^d$, ce qui montre la surjectivité du morphisme.
On note $A(de, e, r)$ le noyau du morphisme $(\det)^d$. En particulier, par le premier théorème d'isomorphisme on en déduit :

$$\#A(de, e, r) = \frac{(de)^r}{e}$$

• En identifiant le groupe symétrique $\mathfrak{S}_r$ avec le groupe des matrices de permutations de tailles $r \times r$, on définit :

$$G(de, e, r) := A(de, e, r) \rtimes \mathfrak{S}_r$$

(Ce qui revient au même que de faire agir $\mathfrak{S}_r$ sur $A(de, e, r)$).
On en déduit le cardinal de $G(de, e, r)$:

$$\#G(de, e, r) = \frac{r!(de)^r}{e}$$

On peut voir le groupe $G(de, e, r)$ comme étant le groupe des matrices monomiales de taille $r \times r$ de coefficients à valeurs dans μ_{de} (c'est à dire les matrices ayant exactement une valeur non nulle sur chaque ligne et chaque colonne - c'est une généralisation des matrices de permutations, où la valeur des coefficients non nuls n'est pas forcément 1) et ici, dont le produit des coefficients non nul est à valeur dans μ_d.

Exemple 3. On a les isomorphismes suivants :

$$G(1, 1, r) \simeq \mathfrak{S}_r$$

$$G(d, 1, 1) \simeq \mathbb{Z}/d\mathbb{Z}$$

Théorème 5. ***Classification de Shephard-Todd (1955)***
Soit G_R un groupe de réflexions complexes irréductible. Alors, au moins une des assertions suivantes est vraie :

- *Il existe trois entiers d, e et r avec $de \geq 2$ et $r \geq 1$ tels que $G_R \simeq G(de, e, r)$*
- *Il existe un entier $r \geq 1$ tel que $G_R \simeq \mathfrak{S}_r$*
- *G_R est isomorphe à l'un des 34 groupes exceptionnels obtenus dans des cas particuliers de la classification (notés $G_4, \cdots, G_{37}$).*

La preuve de ce théorème est très longue et est donc ici admise. Plusieurs outils de la preuve résident néanmoins dans les parties précédentes : décomposition orthogonale, lemmes 15 et 16. On pourra trouver une preuve complète du théorème dans [11] et [12].

On peut toutefois montrer une partie du théorème : les groupes $G(de, e, r)$ sont des groupes de réflexions complexes.

Lemme 17. *Les groupes $G(d, 1, r)$ sont des groupes de réflexions complexes.*

Démonstration. • On rappelle que $G(d, 1, r)$ est le groupe des matrices carrées de taille r à coefficients dans μ_d avec un unique coefficient non nul par ligne et par colonne.
• On peut voir $\mathfrak{S}_r$ comme un groupe de réflexions réel (voir Exemple 1 - partie groupes de réflexions réels) et donc on peut considérer les matrices de permutations comme des réflexions.
• Si z est une racine primitive d-ième de l'unité alors $G(d, 1, r)$ est engendré par la matrice :

$$M := \left(\begin{array}{c|c} z & 0 \\ \hline 0 & I_{r-1} \end{array}\right)$$

et par les matrices de permutations associées aux $(i\ i+1)$. La matrice M est clairement une réflexion complexe et par le deuxième point tous les générateurs sont des réflexions.
Donc les groupes $G(d, 1, r)$ sont des groupes de réflexions complexes. □

Théorème 6. ***/ Lemme pour la classification***
Les groupes $G(de, e, r)$ sont des groupes de réflexions complexes.

Démonstration. On a l'égalité :

$$G(de, e, r) = G(d, 1, 1)G(de, de, r)$$

Comme $G(d, 1, 1)$ est un groupe de réflexions complexes par le lemme précédent, il suffit de prouver que $G(de, de, r)$ est un groupe de réflexions complexes. Il suffira en effet de voir $G(d, 1, 1)$ comme un sous-groupe de $\mathrm{GL}(V)$ où V est l'espace vectoriel dont on prend le sous-groupe $G(de, de, r)$ de $\mathrm{GL}(V)$.
Remarquons que $G(de, de, r)$ est engendré par les matrices de permutations associées aux $(i\ i+1)$ et par la matrice :

$$Q := \left(\begin{array}{c|c} C & 0 \\ \hline 0 & I_{r-2} \end{array}\right) \text{ où } C := \begin{pmatrix} 0 & z \\ z^{-1} & 0 \end{pmatrix}$$

avec z une racine primitive de-ième de l'unité. La matrice Q est bien une réflexion complexe car si on note $(e_1, \cdots, e_r)$ la base canonique de $\mathbb{C}^r$, l'endomorphisme associé fixe tous les éléments de l'hyperplan engendré par $ze_1 + e_2$ et par les $e_3, \cdots, e_r$.
Donc $G(de, de, r)$ est engendré par des réflexions complexes, ce qui en fait donc un groupe de réflexions complexes. □

4 Liens entre groupes de tresses et groupes de réflexions

Nous allons voir tout d'abord que l'on peut représenter les groupes de tresses et les groupes de réflexions complexes d'une même manière à l'aide des diagrammes de Coxeter et Artin. Puis nous verrons comment on peut voir un groupe de tresse comme étant un groupe engendré par des éléments appelés *réflexions de tresses*.

4.1 Diagrammes de Coxeter - Artin

On construit les diagrammes de Coxeter - Artin (on dit aussi "diagrammes à la Coxeter") de la manière suivante :

• Les nœuds correspondent aux générateurs du groupe, ils sont schématisés par des boules contenant ou non un nombre à l'intérieur. La présence d'un nombre à l'intérieur de la boule signifie l'ordre du générateur dans la présentation. L'absence de nombres dans les boules d'un diagramme a lieu en présence de groupe de tresses.

• Deux nœuds distincts qui sont associés à des générateurs qui commutent n'ont pas de lien direct dans le diagramme.

• Le diagramme :

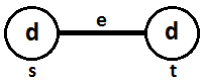

FIGURE 12 – Exemple de diagramme

correspond à la présentation suivante :

$$\langle s, t \mid s^d = t^d = 1 \text{ et } \underbrace{ststst\cdots}_{e \text{ facteurs}} = \underbrace{tstst\cdots}_{e \text{ facteurs}} \rangle$$

• Lorsque $e = 2$ on ne fera donc pas figurer de "lien" entre les générateurs, et lorsque $e = 3$ on omettra de mentionner "3" sur la barre du lien. Lorsque $e = 4$ on utilisera 2 barres de la manière suivante :

FIGURE 13 – Exemple de diagramme avec double lien

qui correspond à la présentation :

$$\langle s, t \mid s^5 = t^4 = 1 \text{ et } ststst = tstst \rangle$$

Exemple 4. Diagramme des groupes $G(d, 1, r)$
qui a pour générateurs : $M, s_1, \cdots, s_{r-1}$ (où M est la matrice du lemme 17 et les s_i les matrices de permutations associées aux $(i\ i+1)$) et pour relations :

• $M^d = s_i^2 = 1$ et $Ms_1Ms_1 = s_1Ms_1M$ et pour $i \in [\![1, r-2]\!]$: $s_is_{i+1}s_i = s_{i+1}s_is_{i+1}$, $Ms_{i+1} = s_{i+1}M$

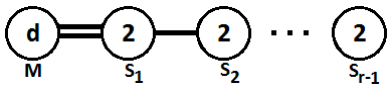

FIGURE 14 – Diagramme de $G(d,1,r)$

• Et en rajoutant la relation : $s_i s_j = s_j s_i$ si $|i-j|>1$.

Pour montrer cela, on montre tout d'abord qu'un groupe $G(d,1,r)$ vérifie les relations ci-dessus. Pour montrer que les relations sont "nécessaires" pour décrire la présentation de $G(d,1,r)$ il s'agit de remarquer que l'on ne peut pas déduire une relation d'une autre (ce qui est assez clair dans notre cas) en raisonnant par l'absurde.

De même, pour obtenir une présentation de $G(de,e,r)$ il suffit de considérer les générateurs :

$$\left\{M^e, M^{-1}s_1M, s_1, \cdots, s_{r-1}\right\}$$

soumis aux relations ci-dessus auxquelles on a retiré : $Ms_1Ms_1 = s_1Ms_1M$ et auxquelles on a rajouté :

$$M^eM's_1 = M's_1M^e$$
$$M's_1s_2M's_1s_2 = s_2M's_1s_2M's_1$$
$$\underbrace{s_1M^eM's_1M's_1\cdots}_{e+1} = \underbrace{M^eM's_1M's_1\cdots}_{e+1}$$
$$(M^e)^d = 1 \text{ et } (M')^e = s_i^2 = 1$$

où $M' = M^{-1}s_1M$.

• Les diagrammes de Coxeter-Artin utilisent également la forme suivante :

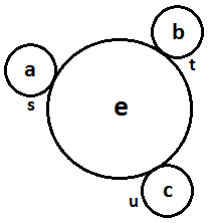

FIGURE 15 – Exemple de diagramme circulant

correspondant à la présentation :

$$\langle s,t,u \mid s^a = t^b = u^c = 1 \text{ et } \underbrace{stustu\cdots}_{e \text{ facteurs}} = \underbrace{tustus\cdots}_{e \text{ facteurs}} = \underbrace{ustust\cdots}_{e \text{ facteurs}}\rangle$$

On pourra consulter [13] pour d'autres exemples de diagrammes ou pour des formes un peu plus exotiques. Cependant on peut déjà remarquer que cette présentation sous forme de diagrammes est particulièrement adaptée aux groupes ayant une présentation dite de Coxeter :

Définition 19. • Un groupe est dit de Coxeter s'il admet une présentation de la forme :

$$\langle s_1, \cdots, s_n \mid (s_is_j)^{m_{i,j}}\rangle$$

avec :

$$\begin{cases} m_{i,j} = m_{j,i} \in (\mathbb{N}\setminus\{0,1\}) \cup \{\infty\} \text{ si } i \neq j \\ m_{i,i} = 1 \text{ sinon} \\ (s_is_j)^\infty \text{ signifie qu'il n'y a pas de relation entre } s_i \text{ et } s_j \end{cases}$$

• Soit $S := \{s_1, \cdots, s_n\}$ un ensemble de générateurs, on définit la matrice de Coxeter associée à S par :

$$M_S := (m_{i,j})_{s_i,s_j \in S}$$

Théorème 7. *Tout groupe fini de Coxeter est un groupe de réflexions (réel).*

Démonstration. On ne fait figurer ici qu'une démonstration-résumée. Une preuve complète se trouve dans [14] et [15].
Soit G un groupe de Coxeter, on munit $V = \mathbb{R}^{\#S}$ d'une forme bilinéaire symétrique définie par :

$$\begin{aligned} B : \quad & \mathbb{R}^{\#S} \times \mathbb{R}^{\#S} \longrightarrow \mathbb{R} \\ & (e_i, e_j) \longmapsto -\cos(\tfrac{\pi}{m_{i,j}}) \end{aligned}$$

On construit ensuite l'application :

$$\varphi : S \to \mathrm{GL}_n(\mathbb{R})$$

de la manière suivante : pour tout $i, j \in [\![1, n]\!]$

$$\varphi(s_i)(e_j) = e_j - 2B(e_i, e_j)e_i$$

On montre que les $\varphi(s_i)\varphi(s_j)$ sont d'ordre $m_{i,j}$ et par propriété universelle qu'on a bien un morphisme étendu à G :

$$\varphi : G \to \mathrm{GL}_n(\mathbb{R})$$

On obtient ainsi une représentation linéaire du groupe G, on montre enfin qu'elle est fidèle (donc injective) et ainsi on obtient que φ réalise un isomorphisme de G sur $\varphi(G)$ qui est un groupe de réflexions réel.

□

Remarque 9. La réciproque du théorème précédent est vraie, mais la preuve est assez longue. Elle utilise entre autres un théorème de Matsumoto et l'ordre de Bruhat-Chevalley. On en trouvera une preuve dans [2].

Ainsi on connait une classification des groupes de Coxeter à l'aide la classification de Shephard-Todd.

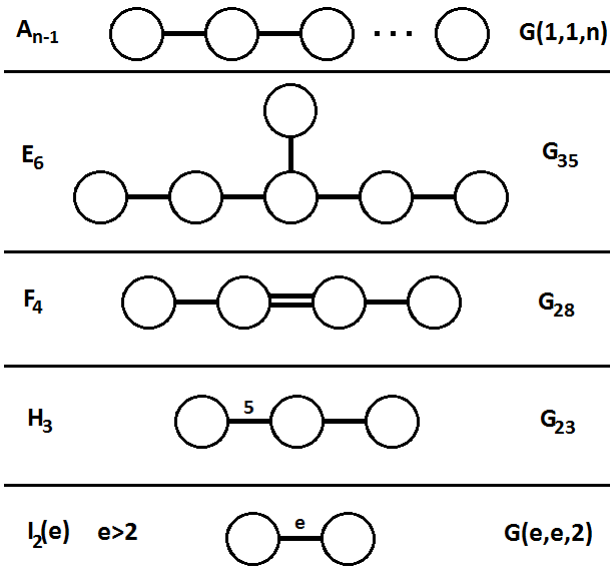

FIGURE 16 – Quelques diagrammes de groupes de la classification de Shephard-Todd

On a fait figurer les correspondances dans la classification de Dynkin (à gauche des diagrammes). Les groupes de type A_{n-1}, E_6, F_4 sont des groupes de réflexions sur le corps $\mathbb{Q}$ (on les appellent groupes de Weyl). Le groupe de type H_3 est un groupe de réflexion sur le corps $\mathbb{Q}(\sqrt{5})$ et celui de type $I_2(e)$ un groupe de réflexion sur le corps $\mathbb{Q}(\zeta_e + \zeta_e^{-1})$ où $\zeta_e = \exp(\frac{2i\pi}{e})$.

On peut remarquer aussi, par la définition 12 que les groupes de tresses vérifient à peu de choses près une présentation de Coxeter. En effet, il faut rajouter à une présentation de Coxeter les relations de type "tresse" (correspondant au premier type - voir figure 9) pour obtenir une présentation d'un groupe de tresses.
C'est pour cette raison que l'on peut aussi représenter les groupes de tresses par des diagrammes de Coxeter-Artin en omettant notamment les nombres dans les boules définissants les générateurs.

4.2 Réflexions de tresses

Soit $\mathbb{K}$ un corps commutatif de caractéristique 0. Soit V un $\mathbb{K}$-espace vectoriel de dimension n et $G \subseteq \mathrm{GL}(V)$ un sous-groupe fini engendré par un ensemble de réflexions R.

On se donne un système d'hyperplans invariants par l'action de G :

$$A := (H_r)_{s_r \in R}$$

On définit l'ensemble suivant :

$$V^{\mathrm{reg}} := V - \bigcup_{H \in A} H$$

On note p la surjection canonique $p : V^{\mathrm{reg}} \to V^{\mathrm{reg}}/G$

Définition 20. Soit $x_0 \in V^{\mathrm{reg}}$
• On appelle groupe de tresses pures en x_0 associé à G le groupe :

$$P := \pi_1(V^{\mathrm{reg}}, x_0)$$

• On appelle groupe de tresses en x_0 associé à G le groupe :

$$T := \pi_1(V^{\mathrm{reg}}/G, p(x_0))$$

Théorème 8. ***Théorème de Steinberg***
Soit G un groupe fini de réflexions de V Soit X un sous-ensemble de V. Alors le fixateur $G(X)$ de X est un groupe de réflexions engendré par des réflexions dans G dont l'hyperplan de réflexion contient X.

Démonstration. Théorème admis, une preuve se trouve dans [1] (partie 4). □

Soit $H \in A$, on note e_H le cardinal du groupe $G(H)$ (fixateur de H). On pose :

$$z_H := \exp\left(\frac{2i\pi}{e_H}\right)$$

On note s_H et on appelle *réflexion distinguée* la réflexion dans G d'hyperplan de réflexion H et de déterminant z_H. On pose :

$$L_H := Im(s_H - Id_V)$$

Pour $x \in V$, on écrit : $x = pr_H(x) + pr_H^{\perp}(x)$ avec :

$$pr_H(x) \in H \text{ et } pr_H^{\perp}(x) \in L_H$$

Soit $t \in \mathbb{R}$, on définit :

$$z_H^t := \exp\left(\frac{2it\pi}{e_H}\right) \quad \text{et} \quad s_H^t(x) := pr_H(x) + z_H^t pr_H^{\perp}(x)$$

On remarque que s_H^t est un élément de $\mathrm{GL}(V)$ et que si $t \neq 0$ on obtient une réflexion complexe, le cas $t = 0$ correspondant au cas réel. On remarque également que si l'on compose e_H fois l'endomorphisme s_H^t par lui-même, on obtient :

$$s_H^{te_H}(x) := pr_H(x) + \exp(2i\pi t) pr_H^{\perp}(x)$$

Pour $x \in V$, on note $\sigma_{H,x}$ le chemin dans V qui part de x et arrive en $s_H(x)$ défini par :

$$\begin{array}{rl} \sigma_{H,x} : & [0,1] \longrightarrow V \\ & t \longmapsto s_H^t(x) \end{array}$$

Et on définit par $\pi_{H,x}$ la boucle dans V de point initial x :

$$\begin{array}{rl} \pi_{H,x} : & [0,1] \longrightarrow V \\ & t \longmapsto s_H^{te_H}(x) \end{array}$$

Soit γ un chemin dans V^{reg} de point initial x_0 et de point final x_H.
On définit le chemin $s_H(\gamma^{-1})$ par :

$$\begin{array}{rl} s_H(\gamma^{-1}) : & [0,1] \longrightarrow V^{\text{reg}} \\ & t \longmapsto s_H(\gamma^{-1}(t)) \end{array}$$

Ce chemin commence au point $s_H(x_H)$ et arrive au point $s_H(x_0)$. On définit le chemin $\sigma_{H,\gamma}$ par :

$$\sigma_{H,\gamma} := s_H(\gamma^{-1}) \cdot \sigma_{H,x_H} \cdot \gamma$$

où ici $\cdot$ désigne la concaténation des chemins.

Remarque 10. Pourvu que x_H soit choisi "proche de H" et loin de l'autre hyperplan (sous entendu l'hyperplan de A le plus proche de H dans V) alors le chemin $\sigma_{H,\gamma}$ est dans V^{reg} et sa classe d'homotopie ne dépend pas du choix de x_H.

Remarque 11. La remarque 10 n'est plus vraie si l'on considère uniquement le cas $\mathbb{K} = \mathbb{R}$.

On définit la boucle $\pi_{H,\gamma}$ par :

$$\pi_{H,\gamma} := \gamma^{-1} \cdot \pi_{H,x_H} \cdot \gamma$$

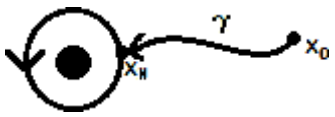

FIGURE 17 – Boucle $\pi_{H,\gamma}$

Définition 21. On appelle réflexions de tresse les éléments $s_{H,\gamma} \in T$ définis par les chemins $\sigma_{H,\gamma}$.
Si l'image de $s_{H,\gamma}$ dans G est s_H on dit que $s_{H,\gamma}$ est une s_H-réflexion de tresse.
On notera encore $\pi_{H,\gamma}$ l'élément de P défini par la boucle $\pi_{H,\gamma}$.

Lemme 18. • *Si γ' est un chemin dans V^{reg} avec pour point initial x_0 et pour point final x_H. Si l'on note τ la boucle dans V^{reg} définie par : $\tau := \gamma'^{-1} \cdot \gamma$ alors on a :*

$$\sigma_{H,\gamma'} = \tau \cdot \sigma_{H,\gamma} \tau^{-1}$$

• *Dans le groupe T on l'égalité :*

$$s_{H,\gamma}^{e_H} = \pi_{H,\gamma}$$

Démonstration. • Par définition on a :

$$\sigma_{H,\gamma'} := s_H(\gamma'^{-1}) \cdot \sigma_{H,x_H} \cdot \gamma'$$

Et par ailleurs :

$$\tau \cdot \sigma_{H,\gamma} \cdot \tau^{-1} = \gamma'^{-1} \cdot \gamma \cdot s_H(\gamma^{-1}) \cdot \sigma_{H,x_H} \cdot \gamma \cdot \gamma^{-1} \cdot \gamma'$$

De plus on a :

$$\gamma'^{-1} \cdot \gamma \cdot s_H(\gamma^{-1}) = s_H(\gamma'^{-1})$$

Car on a d'une part :

$$\tau \cdot \gamma^{-1} := \gamma'^{-1}$$

et :

$$s_H(\tau \cdot \gamma^{-1}) = s_H(\tau) \cdot s_H(\gamma^{-1})$$

De plus, par homotopie :

$$s_H(\tau) = \tau$$

D'où :

$$\tau \cdot \sigma_{H,\gamma} \cdot \tau^{-1} = s_H(\gamma'^{-1}) \cdot \sigma_{H,x_H} \cdot \gamma' = \sigma_{H,\gamma'}$$

• Pour le deuxième point, il suffit de remarquer que l'on a pour tout $t \in [0,1]$ et $x \in V$:

$$\sigma_{H,x}^{e_H} = \pi_{H,x}$$

□

Par le lemme précédent, on peut énoncer le théorème suivant :

Théorème 9. • *Le groupe de tresses T est engendré par les réflexions de tresses $s_{H,\gamma}$ (pour tout hyperplan H et chemin γ).*
• *Le groupe de tresses pures P est engendré par les éléments $s_{H,\gamma}^{e_H} = \pi_{H,\gamma}$.*

Démonstration. La preuve découle du fait que la variété V (resp. V/G) est simplement connexe (tout lacet peut être réduit homotopiquement à un point). Les hyperplans (resp. les images des hyperplans de réflexions dans V/G) sont irréductibles, fermés et de codimension 1. Et les réflexions de tresses définies précédemment sont des générateurs de monodromie. □

5 Automorphismes d'un groupe de réflexions complexes

Dans cette section, nous montrons quelques résultats sur le groupe des automorphismes d'un groupe de réflexions complexes. Ces résultats ont été obtenus très récemment (2010) et l'étude de propriétés sur les automorphismes de ces groupes est encore l'objet de nombreuses recherches.

Définition 22. Soit G un groupe fini. On note $Z(G)$ le centre de G. Un automorphisme f de G est dit **central** si et seulement si il induit l'identité sur $G/Z(G)$ ou de manière équivalente s'il vérifie :

$$\forall g \in G,\ g^{-1} f(g) \in Z(G)$$

Lemme 19. *Le groupe $D := A(de, e, r)$ est des matrices diagonales dans $G := G(de, e, r)$ est un sous-groupe caractéristique de G si et seulement si G n'est pas un des groupes suivants :*

$$G(2,2,2),\ G(2,1,2),\ G(4,2,2),\ G(3,3,3),\ G(2,2,4)$$

On rappelle qu'un sous-groupe H de G est dit caractéristique s'il est stable par tout automorphisme de G.

Démonstration. On montre tout d'abord que pour $r \geq 5$, le groupe D est l'unique sous-groupe maximal distingué abélien de G.
Soit E un autre sous-groupe distingué abélien de G. On a par définition $G = D \rtimes \mathfrak{S}_r$, on en déduit que l'image $E/(E \cap D)$ de E dans $\mathfrak{S}_r$ est un sous-groupe distingué abélien de $\mathfrak{S}_r$. Or on sait par l'étude des sous-groupes distingués de $\mathfrak{S}_r$ qu'un tel sous-groupe est nécessairement trivial si $r \geq 5$. On en déduit que :

$$E/(E \cap D) = 1$$

et donc :

$$E \subseteq D$$

Ce qui permet de dire que le groupe D est l'unique sous-groupe maximal distingué abélien de G.
On suppose maintenant que $r \leq 4$.
Si $d = e = 1$ alors $G = \mathfrak{S}_r$ et $D = 1$ est donc caractéristique. On supposera donc désormais $de > 1$. On va montrer que D est l'unique sous-groupe distingué abélien d'ordre maximal, excepté pour quelques cas particuliers.
On peut exclure tout d'abord $G = G(2,2,2)$ car $Out(G) = \mathrm{GL}_2(\mathbb{F}_2)$ et donc ne préserve pas $D \simeq \mathbb{Z}/2\mathbb{Z}$.
Remarquons pour la suite que l'ordre du centre $Z(G)$ est le *pgcd* des degrés des réflexions de G égal à $d \cdot pgcd(e,r)$. Par ailleurs, on rappelle le résultat vu dans la partie 3 : $\#D = d^r e^{r-1}$.
Pour $r = 1$ on a $G = D$ et donc il n'y a rien à prouver. Soit E un sous-groupe distingué abélien de G dont l'image dans $\mathfrak{S}_r$ est non triviale. Pour $r = 2, 3, 4$ le seul sous-groupe distingué abélien non trivial K de $\mathfrak{S}_r$ est transitif et a pour ordre r. Il s'en suit que l'image de E dans $\mathfrak{S}_r$ est K et a fortiori transitif. Soit $x \in E \cap D$ une matrice disagonale dans E avec pour diagonale :

$$Diag(\alpha_1, \cdots, \alpha_r)$$

Pour $g \in E$ qui a pour image $w \in K \subset \mathfrak{S}_r$, on a $x = gxg^{-1}$ qui est une matrice diagonale avec pour diagonale :

$$Diag(\alpha_{w(1)}, \cdots, \alpha_{w(r)})$$

Comme K est transitif, on obtient :

$$\alpha_1 = \cdots = \alpha_r$$

Donc $x \in Z(G)$ et $E \cap D \subset Z(G)$. Il s'ensuit que E est une extension de K par un sous-groupe de $Z(G)$. En particulier il vient :

$$\#E \leq \#Z(G)\#K = r \cdot d \cdot pgcd(e,r)$$

Comme $\#D = d^r e^{r-1}$, on en déduit que :

$$\#E < \#D$$

sauf pour les cas : $G = G(4,4,2), G(2,1,2), G(4,2,2), G(3,3,3), G(2,2,4)$. A part pour ces exceptions, D est préservé par tout automorphisme de G par unicité du sous-groupe distingué abélien D qui est maximal.
On peut vérifier les cas correspondants aux exceptions "à la main" en construisant à chaque fois un contre-exemple. Et on remarquera que $G(2,1,2)$ possède des automorphismes extérieurs qui ne préservent pas D mais que tout automorphisme de $G(4,4,2)$ préserve D. On peut aussi vérifier ces cas particuliers à l'aide d'un logiciel comme GAP. □

Théorème 10. *Tout automorphisme du groupe $G(de,e,r)$ est composé d'un automorphisme qui préserve les réflexions et d'un automorphisme central, excepté pour les cas $G(1,1,6) = \mathfrak{S}_6$ et $G(2,2,2) = \mathfrak{S}_2 \times \mathfrak{S}_2$.*

Démonstration. Prouvons le théorème pour $G = G(de,e,r)$ avec G différent de :

$$G(2,1,2),\ G(4,2,2),\ G(3,3,3),\ G(2,2,4)$$

On ne traitera pas cas particuliers qui peuvent être prouvés à la main (ce qui est long et on pourra en voir une preuve dans [16]).
On supposera donc G différent de ces exceptions (et celles du lemme précédent) et de plus on supposera $r \neq 6$.
Soit M la matrice définie dans la preuve du lemme 17 et soit s_i (pour $i \in [\![1, r-1]\!]$) les

matrices de permutations associées aux $(i\ i+1)$. On a vu que ces matrices sont des réflexions complexes. On peut remarquer que $G(de,e,r)$ est engendré par :

$$\left\{M^e, M^{-1}s_1M, s_1, \cdots, s_{r-1}\right\}$$

(si $d=1$ on retire M^e et si $e=1$ on retire $M^{-1}s_1M$) on peut reprendre le lemme 17 pour s'en apercevoir.
Soit ϕ un automorphisme de G. Comme G n'est pas une des exceptions du lemme précédent, on peut l'appliquer et voir que ϕ préserve D et induit ainsi un automorphisme $\overline{\phi}$ de $\mathfrak{S}_r$.
Comme $r \neq 6$, on sait par l'étude des automorphismes de $\mathfrak{S}_r$ que $\overline{\phi}$ est nécessairement intérieur.
On notera $g \mapsto Ad(g)$ l'application qui à $g \in G$ associe l'automorphisme intérieur :

$$Ad(g) : x \mapsto gxg^{-1}$$

On remarque donc que $\overline{\phi}$ est de la forme $Ad(\sigma)$ avec $\sigma \in \mathfrak{S}_r$ et relève σ en une matrice de permutation dans G. Ainsi, modulo la composition par un automorphisme intérieur on peut supposer que ϕ induit l'identité sur $\mathfrak{S}_r$ et donc préserve la forme des matrices monomiales dans G.
On notera M_σ la matrice de permutation associée à $\sigma \in \mathfrak{S}_r$.
Ainsi, $\phi(s_1)$ est de la forme :

$$Diag(x_1, \cdots, x_r)M_{(1\ 2)}$$

Comme $\phi(s_1)$ est une involution, on obtient que $x_1 = x_2^{-1}$ et que $x_3, \cdots, x_r$ sont des ± 1.
Le fait que $\phi(s_1)$ commute avec $\phi(s_3), \cdots, \phi(s_{r-1})$ implique que :

$$x_3 = x_4 = \cdots = x_r$$

Ainsi, $\phi(s_1)$ est de la forme :

$$Diag(\alpha_1^{-1}, \alpha_1, \epsilon, \cdots, \epsilon)M_{(1\ 2)}$$

avec $\epsilon = \pm 1$ et $\alpha_1 \in \mu_{de}$. De même, $\phi(s_i)$ est de la forme :

$$Diag(\epsilon, \cdots, \alpha_i^{-1}, \alpha_i, \cdots, \epsilon)M_{(i\ i+1)}$$

où α_i est en i-ème position (le signe ϵ est le même qu'avant car s_1 et s_i sont conjuguées).
De plus, $\phi(M^{-1}s_1M)$ est de la forme :

$$Diag(\alpha'^{-1}, \alpha', \epsilon', \cdots, \epsilon')M_{(1\ 2)}$$

Avec $\epsilon' = \epsilon$ lorsque $r > 2$ et dans ce cas on obtient :

$$M^{-1}s_1M = (s_2s_1M^{-1}s_1Ms_2)^{-1}(s_1)(s_2s_1M^{-1}s_1Ms_2)$$

et donc $M^{-1}s_1M$ est conjugué à s_1.
Soit :

$$s := Diag(1, \epsilon\alpha_1^{-1}, \epsilon^2(\alpha_1\alpha_2)^{-1}, \cdots, \epsilon^r(\alpha_1\cdots\alpha_r)^{-1}) \in G(de,1,r)$$

Il vient que $Ad(s)$ induit un automorphisme de G qui préserve les réflexions et l'automorphisme composé : $\phi' = Ad(s) \circ \phi$ satisfait :

$$\phi'(s_1) = \epsilon s_1, \cdots, \phi'(s_r) = \epsilon s_r$$

On peut vérifier que l'élément $\phi'(M^{-1}s_1M)$ est de la forme :

$$Diag(\alpha''^{-1}, \alpha'', \epsilon, \cdots, \epsilon)M_{(1\ 2)}$$

pour $\alpha'' \in \mu_{de}$.
On peut remarquer que $s_1M^{-1}s_1M$ est d'ordre de. Cela implique que $\epsilon\alpha''$ est une racine primitive de-ième de l'unité. Ainsi il existe $\gamma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{de})/\mathbb{Q})$ tel que $\gamma(\epsilon\alpha'') = \zeta_{de}$. (**Petit**

rappel : $\mathrm{Gal}(L/K)$ est appelé groupe de Galois de l'extension de corps L sur K , c'est le groupe des automorphismes de corps de L laissant K invariant, on notera également : $\zeta_n = \exp(\frac{2i\pi}{n})$).
En appliquant γ aux matrices de G on obtient un automorphisme qui préserve les réflexions, et si l'on compose cet automorphisme avec ϕ' on obtient un automorphisme ϕ'' tel que :

$$\phi''(s_i) = \epsilon s_i \text{ et } \phi''(M^{-1}s_1M) = \epsilon M^{-1}s_1M$$

- Si $d = 1$ c'est fini car ϕ'' est l'automorphisme central donné par : $s \mapsto \epsilon s$ pour toute réflexion.
- Supposons maintenant que $d > 1$. Alors on peut vérifier que $\phi''(M^e)$ est une matrice diagonale qui commute avec $s_2, \cdots, s_{r-1}$ et est donc de la forme :

$$zDiag(\zeta, 1, \cdots, 1)$$

avec $z \in Z(G)$ et $\zeta \in \mu_{de}$. Comme le produit ci-dessus est d'ordre d, z est nécessairement d'ordre d et ζ une racine primitive d-ième de l'unité.
Supposons tout d'abord que $e = 1$, donc comme déjà mentionné plus haut, on retire $M^{-1}s_1M$ des générateurs. Si l'on compose ϕ'' avec l'automorphisme induit par un élément bien choisi de $\mathrm{Gal}(\mathbb{Q}(\zeta_{de})/\mathbb{Q})$ on peut obtenir ϕ''' un automorphisme tel que :

$$\phi'''(s_i) = \epsilon s_i \text{ et } \phi'''(M) = z'M$$

pour $z' \in Z(G)$. Ainsi on remarque que ϕ''' est un automorphisme central de G.
- On supposera maintenant que e et d sont différents de 1. On rappelle une relation de la présentation du groupe $G(de, e, r)$ donnée dans l'exemple 4 :

$$\underbrace{s_1M^eM's_1M's_1\cdots}_{e+1} = \underbrace{M^eM's_1M's_1\cdots}_{e+1}$$

Cette relation implique que $\zeta = \zeta_d$ et ainsi que ϕ est l'automorphisme central qui vérifie :

$$s_i \mapsto \epsilon s_i \text{ et } M^e \mapsto zM^e$$

En reprenant la méthode ci-dessus, on peut montrer le résultat dans le cas $r = 6$ et $de > 1$ lorsqu'on peut exclure la possibilité pour $\overline{\phi}$ d'être un automorphisme non intérieur de $\mathfrak{S}_6$. Modulo la conjugaison par une matrice de permutation, on peut supposer que $\overline{\phi}$ envoie (1 2) sur (1 2)(3 4)(5 6). Soit $p = M_{(1\ 2)(3\ 4)(5\ 6)}$. On a en notant $C_G(x)$ le centralisateur d'un élément $x \in G$:

$$\phi(C_G(s_1) \cap D) = C_G(\phi(s_1)) \cap D = C_G(p) \cap D$$

La première égalité provient du fait que D est un sous-groupe caractéristique par le lemme précédent. La deuxième égalité provient du fait que $G = D \rtimes \mathfrak{S}_6$ et que D est abélien.
Il s'en suit que $C_G(s_1) \cap D$ et $C_G(p) \cap D$ ont le même cardinal. On peut dénombrer le nombre de matrices dans D qui commutent avec s_1 on obtient :

$$\#(C_G(s_1) \cap D) = (de)^4 d$$

Par ailleurs, une matrice dans $C_G(p) \cap D$ est uniquement déterminée par les coefficients de sa diagonale :

$$(a, b, c) \in \mu_{de}^3 \text{ tels que } c^2 \in a^{-2}b^{-2}\mu_d$$

Comme un élément dans μ_{de} a au plus deux racines carrées, il s'en suit que :

$$\#(C_G(p) \cap D) \leq 2d(de)^2$$

Mais on sait aussi que $de \geq 2$, ce qui implique que :

$$2d(de)^2 < (de)^4 d$$

et donc une contradiction car on a montré que $\#(C_G(p) \cap D) = (de)^4 d$.

Les cas particuliers d'automorphismes de groupes de réflexions complexes peuvent se traiter au "cas par cas" suivant la structure des groupes. On pourra trouver le traitement de ces cas dans [16]. □

6 Quelques utilisations des groupes de tresses et des groupes de réflexions

6.1 Théorème de Shephard-Todd/Chevalley-Serre

Les groupes de réflexions complexes ont de nombreuses applications dans des démonstrations mathématiques. Cependant, une des plus importantes est celle du théorème de Shephard-Todd/Chevalley-Serre. D'abord prouvé en utilisant la classification de Shephard-Todd et en vérifiant le théorème dans chacun des cas particulier de cette dernière, il fut aussi prouvé de manière "globale" sans traiter de "cas par cas" par Chevalley et Serre.

Théorème 11. *Soit G un groupe fini qui agit sur $\mathbb{A} := \mathbb{K}[X_1, \cdots, X_n]$ alors on a l'équivalence :*

$$\mathbb{A}^G \simeq \mathbb{A} \;\Leftrightarrow\; G \text{ est engendré par des réflexions}$$

où $\mathbb{A}^G := \{p \in \mathbb{A} \mid \forall g \in G,\ g(p) = p\}$

Démonstration. Une preuve complète se trouve dans [1], nous ne l'explicitons pas ici par soucis d'espace. □

On peut trouver une version légèrement complémentaire de la précédente :

Théorème 12. *Soit G un sous-groupe fini de $\mathrm{GL}(V)$ (où V est un $\mathbb{K}$-espace vectoriel de dimension n avec $\mathbb{K}$ de caractéristique 0). Soit $S(V)$ l'algèbre symétrique de V isomorphe à l'anneau de polynômes $K[X_1, \cdots, X_n]$. Il y a équivalence entre :*
• *G est engendré par des réflexions*
• *L'anneau $S(V)^G$ des polynômes fixés par G est un anneau de polynôme : $K[f_1, \cdots, f_n]$ où les f_i sont des polynômes homogènes algébriquement indépendants de degrés d_i.*

De plus, si cette équivalence est réalisée, alors si l'on note R l'ensemble des réflexions qui engendre G, on a :

$$\#R = \sum_{i=1}^{n} (d_i - 1)$$

$$\#G = \prod_{i=1}^{n} d_i$$

Exemple 5. Pour $G = \mathfrak{S}_n$ avec l'action de $\mathfrak{S}_n$ sur $V = \mathbb{C}^n$ canonique qui consiste à permuter une base de vecteurs $(e_1, \cdots, e_n)$ en $(e_{\sigma(1)}, \cdots, e_{\sigma(n)})$. On aurait :
$f_1 = X_1 + \cdots + X_n$, $f_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n$, $\cdots$, $f_n = X_1X_2 \cdots X_n$ avec $d_i = i$ $\forall i \in [\![1, n]\!]$.

6.2 Applications en informatique et en physique

• **En informatique**, le groupe de tresses a encore actuellement plusieurs problèmes non résolus. Ces problèmes permettent des applications en cryptographie dont notamment avec le problème du mot ou encore celui de la conjugaison.
Le problème du mot consiste à savoir si étant donné deux mots (suites de lettres codées par les $\sigma_i^{\pm 1}$ voir partie groupe de tresses) codent la même tresse.

L'autre problème consiste, étant donnés x et y deux éléments d'un groupe de tresses, à vérifier que x et y sont conjugués (c'est à dire à vérifier qu'il existe g dans le groupe tel que $x = gyg^{-1}$). Une version plus difficile de ce problème est celle de la recherche du conjuguant, visant à déterminer explicitement g qui permet la conjugaison. Ces problèmes sont résolus aujourd'hui mais pas en temps polynômial, ce qui est donc encore l'objet de nombreuses recherches.

Entre autres, une grosse application en cryptographie de ce dernier problème peut se résumer à l'échange de clé suivant :

Alice et Bob doivent se mettre d'accord sur une clé privé s permettant de sécuriser leurs échanges (de manière à ne pouvoir être connu par d'autres interlocuteurs). On note $\mathcal{T}_{n,2n}$ le groupe de tresses engendré par les générateurs $\sigma_{n+1} \cdots \sigma_{2n-1}$

- On choisit p publique dans $\mathcal{T}_{2n}$
- Alice choisit $a \in \mathcal{T}_n$ et envoie $p_A = apa^{-1}$ à Bob
- Bob choisit $b \in \mathcal{T}_{n,2n}$ et envoie $p_B = bpb^{-1}$ à Alice
- La clé s est obtenue par Alice en calculant ap_Ba^{-1} et par Bob en calculant bp_Ab^{-1}

Les tresses a et b commutent car $a \in \mathcal{T}_n$ et $b \in \mathcal{T}_{n,2n}$ donc $ab = ba$ et ainsi :

$$ap_Ba^{-1} = abpb^{-1}a^{-1} = bapa^{-1}b^{-1} = bp_Ab^{-1}$$

Donc Alice et Bob obtiennent à la fin la même tresse. Le caractère sécurisé de ce protocole est réalisé par la difficulté à trouver a sachant (p, p_A) et à trouver b sachant (p, p_B).

• **En physique**, la température de la couronne solaire s'explique par l'émission d'ondes dites d'Alfven depuis la photosphère vers la couronne. Ce sont des ondes magnéto-acoustiques créées par le champ magnétique intense de l'étoile. Elles transportent une très grande quantité d'énergie et constituent le mécanisme principal en période de faible activité solaire. En période de forte activité, les physiciens ont observé des "nanoéruptions" semblables aux éruptions solaires mais à des énergies beaucoup plus faibles et donc difficiles à observer.
En 2012, une équipe de physiciens de la NASA a réussi grâce à une nouvelle technologie d'observer ces phénomènes. De plus, ils sont parvenus à décrire le mécanisme : les lignes de champ magnétiques suivent des "tressages" particuliers. Et la manière dont est tressé un champ magnétique provenant de ces phénomènes détermine quasiment entièrement le niveau d'énergie libéré. On pourra consulter [17] pour plus d'informations sur le tressage de ces champs magnétiques.

Les groupes de tresses sont aussi utiles pour décrire le comportement des anyons. Ce sont des particules qui peuvent exister dans un espace à deux dimensions. Des "systèmes d'anyons" sont aujourd'hui considérés pour le développement de l'ordinateur quantique. Les anyons ont la propriété de pouvoir être "fusionnés" entre eux selon des règles de concaténation que suivent les diagrammes de tresses explicitées dans la partie 2.

7 Conclusion

L'introduction des groupes de tresses et des groupes de réflexions dans les premières parties de ce rapport, nous a permis de comprendre les liens qui résident entre ces deux types de groupes, notamment à travers leurs *présentations* voisines ou encore la possibilité de voir un groupe de tresse comme étant engendré par des *réflexions de tresses*. Cette dernière caractéristique a été observée grâce à la manipulation de *groupes fondamentaux* faisant intervenir les lacets d'un espace topologique.

Nous avons pu comprendre également, en partie, la longue classification de Shephard-Todd des groupes de réflexions complexes. Celle-ci nécessitant l'introduction d'outils comme les *racines* d'une réflexion ou encore les liens qui existent entre racines : *l'orthogonalité ou le parallélisme*. Pour étudier ces liens, nous avons tout d'abord étudié des propriétés de stabilité des réflexions par passage au conjugué ou à la transposée par exemple. De plus, nous avons montré que l'on pouvait indicer un ensemble de réflexions de différentes manières. Ces différentes manières d'indicer se sont montrées, par la suite, particulièrement utiles dans la définition de sous-espaces vectoriels. Ces derniers ont joué un grand rôle dans la décomposition de notre espace vectoriel de travail V en sous-espaces stables par l'action d'un groupe de réflexion. Cette décomposition est d'ailleurs dans le coeur de la preuve de la classification de Shephard-Todd.

Nous avons aussi introduit les diagrammes *"à la Coxeter"* qui permettent de simplifier la présentation par générateurs et relations des groupes de tresses ou des groupes de réflexions. Ces diagrammes montrent encore l'étroitesse qui existe entre les groupes de tresses et ceux de réflexions car il suffit de retirer les ordres des générateurs dans les diagrammes de réflexions pour basculer à un diagramme de tresses.

Enfin, nous nous sommes attachés à comprendre la structure du groupe des automorphismes d'un groupe de réflexion complexes. Cette structure n'a été mise en lumière que très récemment dans les années (2009-2010) et l'étude des propriétés sur ce groupe d'automorphismes est encore d'actualité.
On a donc pu voir que principalement, tout automorphisme d'un groupe de réflexions complexes est composé d'un automorphisme qui préserve les réflexions et d'un *automorphisme central*.

L'étude de la structure des automorphismes des groupes de tresses est un peu plus ancienne (1981), on pourra consulter [18] pour son étude. Toutefois, celle concernant les automorphismes du groupe de tresses pures est très récente (2017) et on pourra consulter [19] pour en prendre connaissance.

Enfin, nous avons exploré les diverses applications que ces groupes peuvent avoir. Nous avons principalement étudié celles concernant le théorème de Shephard-Todd/Chevalley-Serre en algèbre en suivant sa preuve (non présentée dans ce rapport - on pourra consulter [1]). Puis, nous avons donné quelques utilisations dans les domaines de la cryptographie (problème du mot, du conjuguant) et de la physique (champ magnétiques de la couronne solaire, comportement des anyons).

Table des figures

Figures réalisées sous Geogebra et Paint

Références

[1] **M. Broué**, *Introduction to Complex Reflection Groups and Their Braid Groups*, Lecture Notes in Mathematics, Springer, 1988.

[2] **J. Michel**, *Groupes de tresses, groupes réductifs et algèbres de Hecke*, Notes de cours 3ème cycle, 1998.

[3] **E. Artin**, *Theory of Braids*, Annals of Mathematics, Second Series, Vol. 48, No. 1 (Jan., 1947), pp. 101-126.

[4] **A. Debreil**, *Groupes finis et treillis de leurs sous-groupes*, Calvage & Mounet, 2016.

[5] **H. S. M. Coxeter et W. O. J. Moser**, *Generators and Relations for Discrete Groups*, Springer, 1972 (réimpr. 2013), 3e éd.

[6] **R. A. Wilson**, *The Finite Simple Groups*, Springer, 2009.

[7] **A. Hatcher**, *Algebraic Topology*, Cambridge University Press, 2002, pp. 21-40.

[8] **J. Calais**, *Éléments de théorie des groupes*, Puf, 2016, 2e tirage pp.390-391.

[9] **A. Jon Berrick et al.**, *Braids : Introductory Lectures on Braids, Configurations and Their Applications*, Lecture Notes Series, Institute for Mathematical Sciences University of Singapore, vol-19.

[10] **J.S. Birman**, *Braids, links and mapping class groups*, Princeton University Press and University of Tokyo Press, Annals of mathematics studies, 1974.

[11] **G. C. Shephard et J. A. Todd**, *Finite unitary reflection groups*, Canad , J. Math. 6, 1954, pp. 274-304.

[12] **A. M. Cohen**, *Finite complex reflection groups*, Ann. Sci. Ecole Norm. Sup. (4) 9, 1976, pp. 379–436.

[13] **J. Michel**, *PDF web - Table de diagrammes de Coxeter-Artin*, https ://webusers.imj-prg.fr/ jean.michel/papiers/table.pdf

[14] **N. Bourbaki**, *Groupes et Algèbres de Lie*, Chap. 4-5-6 Éléments de Mathématiques. Hermann, (§68 chapitre 5).

[15] **C. Curtis et I. Reiner**, *Methods of Representation Theory*, Vol.1 Wiley. New York, 1990 (Théorème 64.28)

[16] **I. Marin et J. Michel**, *Automorphisms of Complex Reflections Groups*, 2010, arXiv :math/0701266v3

[17] **J. W. Cirtain et al.**, *Energy release in the solar corona from spatially resolved magnetic braids*, Vol.493, Nature, 2013, pp. 501-503.

[18] **J. L. Dyer et E. K. Grossman**, *The Automorphism Groups of the Braid Groups*, Vol. 103 No. 6, American Journal of Mathematics, 1981, pp. 1151-1169.

[19] **V. G. Bardakov, M. V. Neshchadim, M. Singh**, *Automorphisms of pure braid Groups*, 2017, arXiv :1704.07045