1. Groupes finis de réflexion

Soit k un sous-corps de $\mathbb{C}$ et soit V un k-espace vectoriel de dimension n. Un élément $s \in \mathrm{End}(V)$ est dit une *pseudo-réflexion* si $\mathrm{rang}(\mathrm{Id}_V - s) = 1$. Si s est d'ordre fini (il possède alors une unique valeur propre $\zeta \neq 1$, une racine de l'unité) nous dirons aussi que s est une réflexion complexe. La "justification" de cette définition est que si nous prenons $k = \mathbb{R}$, une réflexion complexe est une vraie réflexion (d'ordre 2). Par abus, nous dirons souvent simplement "réflexion" pour "réflexion complexe".

Une réflexion complexe est de la forme $s(x) = x - \check{r}(x)r$ où $\check{r} \in V^*$ est une forme linéaire de noyau l'hyperplan $H_s = \mathrm{Ker}(s - \mathrm{Id}_V)$, et r est un vecteur propre associé à la valeur propre $\zeta \neq 1$ de s, ces données vérifiant $\check{r}(r) = 1 - \zeta$. Nous disons que r (resp. $\check{r}$) est une racine (resp. coracine) associée à la réflexion s. Ces données sont uniques à multiplication près de r par un scalaire et de $\check{r}$ par le scalaire inverse.

Soit W un sous-groupe fini de $GL(V)$. Nous noterons $\mathrm{Ref}(W)$ l'ensemble des réflexions complexes de W. On dit que W est un *groupe fini de réflexions complexes* s'il est engendré par $\mathrm{Ref}(W)$. Un tel groupe est associé au système d'hyperplans W-invariant $\mathcal{A}_W = \{H_s\}_{s \in \mathrm{Ref}(W)}$.

Quand $k = \mathbb{R}$, on obtient la notion de groupe fini de réflexions réel, dont nous verrons qu'elle coïncide avec celle de groupe de Coxeter fini (attention ! il existe des groupes engendrés sur $\mathbb{C}$ par des réflexions d'ordre 2 qui ne sont pas réalisables sur $\mathbb{R}$).

Lemme 1.1. *Pour $H \in \mathcal{A}_W$, le groupe $C_W(H)$ est cyclique.*

Démonstration. Le sous-$C_W(H)$-module de V donné par H a un supplémentaire $C_W(H)$-stable[1], qui est une droite. L'action de $C_W(H)$ est donnée par son action sur cette droite, donc elle est cyclique (un sous-groupe fini de $\mathbb{C}^\times$ est cyclique). □

Il résulte de ce lemme que l'on peut choisir une racine commune r_H pour toutes les réflexions de $C_W(H)$, ce que nous ferons par la suite. Notons aussi que $|\mathrm{Ref}(W)| = \sum_{H \in \mathcal{A}_W} (|C_W(H)| - 1)$. Si toutes les réflexions sont d'ordre 2, il y en a autant que d'hyperplans. Le lemme ci-dessus admet une réciproque.

Lemme 1.2. *Deux réflexions ont des racines proportionnelles si et seulement si elles ont même hyperplan.*

Démonstration. Le fait que deux réflexions de même hyperplan ont des racines proportionnelles vient d'être remarqué. Dans l'autre sens, soit D la droite contenant les racines des réflexions s_1 et s_2. Le sous-groupe engendré par s_1 et s_2 préserve un hyperplan H supplémentaire à D ; alors H est nécessairement un hyperplan de réflexion pour s_1 et pour s_2. □

Les deux lemmes ci-dessus utilisent (via le théorème de Mashke) le fait que le groupe soit fini. Nous verrons des contre-exemples aux deux pour des groupes de réflexions réels infinis.

On dit que W est irréductible si V est une représentation irréductible de W. Un groupe de réflexions complexes est un produit direct de groupes irréductibles. Ces derniers ont été classifiés par Shephard et Todd, en une famille infinie a 3 paramètres (qui contient les 4 familles infinies de groupes de Coxeter), et 34 groupes "sporadiques" (qui pour des raisons historiques sont notés G_4 à G_{37}).

[1] rappel : théorème de Mashke

2. Invariants des groupes finis

Soit V un k-espace vectoriel, et soit W un sous-groupe de $\mathrm{GL}(V)$. On appelle invariants polynomiaux les invariants S^W de W dans l'algèbre symétrique[2] S de V. Pour tout choix d'une base $x_1, \ldots, x_n$ de V, l'algèbre S s'identifie à l'algèbre de polynômes $k[x_1, \ldots, x_n]$. Nous allons voir que W est un groupe de réflexions complexes si et seulement si S^W est une algèbre de polynômes.

Le point de vue de la géométrie algébrique. Soit V^* le dual de V, sur lequel W agit par la représentation contragrédiente ($w \in W$ agit par ${}^t w^{-1}$ sur V^*). L'algèbre symétrique S^* de V^* s'identifie au fonctions polynomiales sur V, *i.e.* du point de vue de la géométrie algébrique, on a $V = \operatorname{Spec} S^*$. Alors le quotient V/W existe comme variété algébrique et s'identifie à $\operatorname{Spec}(S^{*W})$ (nous le verrons au niveau des ensembles plus tard) ; et W est un groupe de réflexions complexe si et seulement si $V/W \simeq V$ (en fait, W est déjà un groupe de réflexions complexes dès que la variété V/W est lisse).

Ceci donne une raison de s'intéresser aux invariants dans S^* plutôt que dans S. Toutefois nous étudierons plutôt S, ce qui nous évitera en général de prendre l'action contragrédiente. Quand nous aurons besoin de l'aspect quotient de variétés nous considérerons simplement S comme les fonctions régulières sur V^* muni de l'action contragrédiente de W. Sur V^* les rôles sont inversés et la réflexion s de racine r et coracine $\check{r}$ fixe l'hyperplan $\operatorname{Ker} r \subset V^*$ et a $\check{r}$ comme racine.

Finitude des invariants. Nous allons montrer que S^W est engendré par un nombre fini d'invariants. La preuve due à Hilbert devient très simple en introduisant une définition : un module M sur un anneau commutatif A est dit *Noetherien* si toute chaîne croissante de sous-modules est stationnaire. Cela équivaut à ce que tout sous-module soit de type fini. A lui-même est dit Noetherien s'il l'est comme A-module. Il est clair que tout quotient ou sous-module d'un module Noetherien l'est, ainsi que tout somme directe de modules Noetheriens (on montre plus généralement que si dans une suite exacte $0 \to M' \to M \xrightarrow{f} M'' \to 0$ les modules M' et M'' sont Noetheriens, alors M l'est aussi ; pour cela on utilise que si $E \subset F$ sont deux sous-modules de M tels que $E \cap M' = F \cap M'$ et $f(E) = f(F)$ alors $E = F$). Un A-module sur un anneau Noetherien A est Noetherien si et seulement si il est de rang fini (il est alors Noetherien comme sous-module d'un A^n).

Théorème 2.1. *(base de Hilbert) Si A est Noetherien, $A[x]$ l'est aussi.*

Démonstration. On remarque d'abord qu'un anneau A est Noetherien si et seulement si tout idéal est de type fini. En effet, si A est Noetherien un idéal=sous-module.

Il suffit donc de voir que tout idéal I de $A[x]$ est de type fini. Soit I_0 l'idéal de A formé des coefficients de plus haut degré des éléments de I. Alors I_0 est de type fini comme idéal de A, engendré par disons $a_1, \ldots, a_n$; soient $f_1, \ldots, f_n$ des éléments de I de coefficients de plus haut degré $a_1, \ldots, a_n$, et soit $t = \max(\deg f_i)$ et I' le sous-idéal de I engendré par les f_i. Alors pour tout $a \in I_0$, l'idéal I' contient un polynôme de terme directeur ax^t, donc tout élément de I est congru modulo I' à un polynôme de degré plus petit que t. Le A-module M des polynômes de degré

[2] rappel : produit tensoriel, algèbre tensorielle, symétrique

plus petit que t est isomorphe à $A \oplus \ldots \oplus A$ (t fois) donc est Noetherien, donc $I \cap M$ est de rang fini et $I = (I \cap M) \oplus I'$ est de type fini. □

Il en résulte que toute A-algèbre de type fini est Noetherienne.

Nous montrons maintenant le

Théorème 2.2. *(Hilbert-Noether) S^W est une algèbre de type fini sur k.*

Démonstration. Notons d'abord que S est un S^W-module de rang fini. En effet tout élément $p \in S$ est entier[3] sur S^W, car il est racine du polynôme unitaire à coefficients dans S^W donné par $\prod_{w \in W}(X - wp)$. En particulier les générateurs $x_1, \ldots, x_n$ de S sur k sont entiers sur S^W et chaque extension $S^W[x_1, \ldots x_i][x_{i+1}] \supset S^W[x_1, \ldots, x_i]$ est donc finie.

Le théorème résulte donc de la

Proposition 2.3. *Soit S une k-algèbre de type fini et soit R une sous-algèbre telle que S soit un R-module de rang fini. Alors R est une k-algèbre de type fini.*

Démonstration. S étant de rang fini sur R, les éléments de S sont finis sur R. Notons $P(s)$ le polynôme à coefficients dans R qui exprime l'intégralité de $s \in S$ sur R, et soit R' la sous-algèbre de S engendrée par les coefficients des $P(s)$ quand p décrit un ensemble de générateurs de S sur k. Les générateurs de S étant entiers sur R' par construction, S est déjà de rang fini sur R', et R' est une algèbre de type fini sur k, donc l'anneau R' est Noetherien. Le R'-module S est de rang fini sur R', donc Noetherien. Son R'-sous-module R est donc Noetherien, donc aussi de rang fini sur R', donc de type fini sur k. □

□

L'action de W étant degré par degré, on peut trouver un ensemble de générateurs homogènes $f_1, \ldots, f_r$ de S^W. S étant de rang fini sur S^W, le degré de transcendance[4] de S^W doit être le même que celui de S, à savoir n. On peut donc trouver n générateurs algébriquement indépendants parmi les f_i, *i.e.*, quitte à renuméroter les f_i on peut supposer que $k[f_1, \ldots, f_n]$ est une algèbre de polynômes. On peut montrer (avec de l'algèbre commutative – plus exactement le théorème de normalisation de Noether) que dans cette situation S^W est un module libre sur $k[f_1, \ldots, f_n]$ (un tel anneau qui est libre sur un anneau de polynômes est appelé *anneau de Cohen-Macauley*) mais nous ne l'utiliserons pas.

Invariants des groupes de réflexion complexes. Nous allons démontrer la caractérisation de Shephard-Todd des groupes de réflexion complexes en deux temps. Dans un premier temps nous supposerons que les groupes de réflexions complexes ont des invariants polynomiaux (ce qui avait été vérifié cas par cas par Shephard et Todd), et nous en déduirons la réciproque. Puis nous exposerons une preuve due a Chevalley de la partie directe.

Notre outil dans le premier temps sera uniquement les *séries de Poincaré* : soit M un k-espace vectoriel gradué par $\mathbb{N}$ (tel que chaque M_i soit de dimension finie). On appelle *série de Poincaré* de M la série formelle en t donnée par $P_M = \sum_{n=0}^{\infty} \dim M_i t^i$. On vérifie facilement qu'on a $P_{M \oplus M'} = P_M + P_{M'}$, et $P_{M \otimes M'} = P_M \times P_{M'}$ (si on gradue $M \otimes M'$ par le degré total). Si $f_1, \ldots, f_n$ sont

[3] rappel : éléments entiers

[4] rappel : extensions transcendantes

des polynômes algébriquement indépendants de degrés $d_1, \dots, d_n$ on a $P_{k[f_1,\dots,f_n]} = \prod_{i=1}^{i=n}(1-t^{d_i})^{-1}$. En effet, on a $k[f_1,\dots,f_n] \simeq k[f_1] \otimes \dots \otimes k[f_n]$ et $P_{k[f_i]} = \sum_{j=0}^{\infty} t^{jd_i} = (1-t^{d_i})^{-1}$. En particulier a $P_S = (1-t)^{-n}$.

Une idée de la forme générale que peut prendre une série de Poincaré est donné par le

Théorème 2.4. *(Hilbert-Serre) Soit A une k-algèbre graduée de type fini, engendrée par des éléments homogènes $x_1,\dots,x_r$ de degrés $d_1,\dots,d_r$. Soit M un A-module gradué de type fini. Alors il existe $f \in \mathbb{Z}[t]$ tel que $P_M = \frac{f(t)}{(1-t^{d_1})\dots(1-t^{d_r})}$.*

Démonstration. La preuve se fait par récurrence sur r. Si $r = 0$ alors M est un k-espace vectoriel gradué de dimension finie et le résultat est évident. Sinon, on commence par remarquer que si l'on a une suite exacte de modules gradués $0 \to M_1 \to \dots \to M_n \to 0$ alors $\sum_i (-1)^i P_{M_i} = 0$. Nous considérons maintenant l'application de multiplication par x_r dans M, qui n'est pas graduée mais qui le devient si l'on considère que son origine est $M[-d_r]$, module obtenu en incrémentant la graduation de d_r ; on a $P_{M[-d_r]} = t^{d_r} P_M$. Si M' et M'' sont respectivement le noyau et le conoyau de la multiplication par x, on a : $0 \to M'[-d_r] \to M[-d_r] \xrightarrow{x_r} \to M \to M'' \to 0$ d'où $t^{d_r}P_{M'} - t^{d_r}P_M + P_M - P_{M''} = 0$. Mais M' et M'' sont toujours de type fini sur A, et sont annulés par x_r, donc sont en fait de type fini sur la sous-algèbre A' engendrée par $x_1,\dots,x_{r-1}$. Par récurrence (*i.e.*, en utilisant que $P_{M'}$ et $P_{M''}$ sont de la forme $\frac{f(t)}{(1-t^{d_1})\dots(1-t^{d_{r-1}})}$) le résultat sur P_M s'en déduit immédiatement. □

Lemme 2.5. *(Molien) On a $P_{S^W} = |W|^{-1} \sum_{w\in W} \det(1-wt \mid V)^{-1}$.*

Démonstration. On peut généraliser la notion de série de Poincaré : si $w \in \mathrm{End}(M)$ agit degré par degré, on définit sa *trace graduée* $P_M(w) = \sum_{i=0}^{\infty} \mathrm{Trace}(w \mid M_i)t^i$; on a $P_M(\mathrm{Id}) = P_M$. Pour calculer la trace graduée de $w \in W$ sur S, choisissons une base de V formée de vecteurs propres $x_1,\dots,x_n$ de w et soient $\lambda_1,\dots,\lambda_n$ les valeurs propres associées. On a clairement $P_S(w) = \prod_i P_{k[x_i]}(w)$ et $P_{k[x_i]}(w) = \sum_{j=0}^{\infty}(\lambda_i t)^j = (1-\lambda_i t)^{-1}$ donc $P_S(w) = \det(1-wt \mid V)^{-1}$. Maintenant, $p_W = |W|^{-1}\sum_{w\in W} w$ est un projecteur sur S^W, donc $P_S(p_W) = P_{S^W}$, d'où le lemme. □

Nous avons aussi besoin d'un lemme sous les sous-algèbres de polynômes d'une algèbre de polynômes

Lemme 2.6. *Soient $k[f_1,\dots,f_n] \subset k[f'_1,\dots,f'_n]$ deux sous-algèbres polynomiales de $k[x_1,\dots,x_n]$. Si on suppose que $f_1,\dots,f_i$ sont de degrés $d_1,\dots,d_n$ rangés en ordre croissant, de même que $f'_1,\dots,f'_n$ de degré $d'_1,\dots,d'_n$ rangés en ordre croissant, alors $d'_i \le d_i$.*

Démonstration. Il existe des polynômes $p_1,\dots,p_n$ tels que $f_i = p_i(f'_1,\dots,f'_n)$. Donc si $\deg f_i < \deg f'_i$, alors $f_1,\dots,f_i$ ne feraient intervenir que $f'_1,\dots,f'_{i-1}$ ce qui est absurde puisqu'ils sont algébriquement indépendants. □

Nous prouvons maintenant en admettant (ii)⇒(iii) le théorème

Théorème 2.7. *Soient $f_1,\dots,f_n$ des éléments algébriquement indépendants de S^W de degré $d_1,\dots,d_n$, tels que $d_1\dots d_n$ soit minimal. Alors on a toujours $|W| \le d_1\dots d_n$, et on a équivalence entre :*
(i) $|W| = d_1\dots d_n$.

(ii) W est engendré par $\mathrm{Ref}(W)$.
(iii) $S^W = k[f_1, \dots, f_n]$.
Et, si ces conditions sont vérifiées alors
(iv) $|\mathrm{Ref}(W)| = \sum_{i=1}^n (d_i - 1)$.

Démonstration. Sur la formule 2.5, on voit que la série P_{S^W} converge pour t réel tel que $0 \leq t < 1$, et que P_{S^W} a un développement en série de Laurent au voisinage de 1 qui commence par $\frac{1}{|W|(1-t)^n} + \frac{|\mathrm{Ref}(W)|}{2|W|(1-t)^{n-1}} + \dots$. En effet, seule l'identité contribue au terme en $(1-t)^{-n}$, et seules les réflexions complexes de W contribuent au terme en $(1-t)^{1-n}$; de plus pour chaque réflexion complexe de valeur propre λ non réelle on a $\frac{1}{1-\lambda} + \frac{1}{1-\lambda^{-1}} = 1$, et pour $\lambda = -1$ on a $\frac{1}{1-(-1)} = 1/2$, d'où le facteur $\frac{1}{2}$.

D'autre part, le développement en série de Laurent de $P_{k[f_1,\dots,f_n]}$ au voisinage de 1 est $\frac{1}{(1-t)^n d_1 \dots d_n} + \frac{\sum_{i=1}^{i=n}(d_i-1)}{(1-t)^{n-1} 2 d_1 \dots d_n} + \dots$ (pour trouver le second terme, on multiplie par $(1-t)^n$, on dérive et on fait $t = 1$).

Comme $k[f_1, \dots, f_n] \subset S^W$, les coefficients de la série $P_{k[f_1,\dots,f_n]}$ sont inférieurs ou égaux à ceux de la série P_{S^W}, donc pour $0 \leq t < 1$ on a $P_{k[f_1,\dots,f_n]}(t) \leq P_{S^W}$. En particulier, le premier coefficient du développement de Laurent de la première série en 1 doit être inférieur au premier coefficient de Laurent de la deuxième série, *i.e.* $|W| \leq d_1 \dots d_n$. On voit aussi que (iii)⇒(i) et (iii)⇒ (iv).

Montrons maintenant (i)⇒ (ii). Puisque $|W| = d_1 \dots d_n$ on peut comparer le deuxième coefficient des développements de Laurent et on obtient $|\mathrm{Ref}(W)| \geq \sum_{i=1}^n (d_i - 1)$. Soit W' le sous-groupe engendré par $\mathrm{Ref}(W)$. Alors, par $(ii) \Rightarrow (iii)$ il existe $f'_1, \dots, f'_n$ algébriquement indépendants tels que $S^{W'} = k[f'_1, \dots, f'_n]$. Soient $d'_1, \dots d'_n$ les degrés des f'_i ; (iii)⇒ (i) appliqué à W' montre que $|W'| = d'_1 \dots d'_n$, et (iii)⇒ (iv) appliqué à W' montre que $|\mathrm{Ref}(W)| = |\mathrm{Ref}(W')| = \sum_{i=1}^n (d'_i - 1)$. Puisque $k[f_1, \dots, f_n] \subset S^W \subset S^{W'}$, si les d_i et d'_i sont rangés en ordre croissant, par 2.6 on a $d_i \geq d'_i$. Nous pouvons maintenant conclure : $\sum_{i=1}^{i=n}(d'_i - 1) = |\mathrm{Ref}(W)| \geq \sum_{i=1}^{i=n}(d_i - 1)$, ce qui impose $d_i = d'_i$ d'où $|W'| = |W|$ donc $W' = W$. □

Notons comment le (i) de ce théorème se généralise a des groupes finis quelconques : en écrivant que S^W est Cohen-Macauley, on a $S^W = \oplus_{i=1}^s k[f_1, \dots, f_n]\alpha_i$ pour certains éléments homogènes α_i de degré e_i et certains éléments homogènes algébriquement indépendants f_i de degré d_i ; la série de Poincaré de S^W est donc $\frac{t^{e_1} + \dots + t^{e_s}}{(1-t^{d_1})\dots(1-t^{d_n})}$ et le développement en série de Laurent au voisinage de 1 comme dans la preuve du théorème donne $|W| = d_1 \dots d_n / s$.

Exercice 2.8. Soit W le groupe d'ordre 2 plongé dans $\mathrm{GL}_2(k)$ en envoyant son élément non trivial sur $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Montrer que la série de Poincaré de ses invariants est $P_{S^W} = \sum_{i=0}^{\infty} (2i+1) t^{2i}$. En déduire que, dans la base de k^2 donnée par $x = (1, 0)$, $y = (0, 1)$, l'algèbre S^W est engendrée par x^2, xy et y^2, *i.e.* on a $S^W = k[x^2, y^2] \oplus k[x^2, y^2]xy$. Montrer que $S^W \simeq k[\alpha.\beta, \gamma]/(\alpha\gamma - \beta^2)$ (où dans l'isomorphisme $\alpha = x^2$, $\beta = xy$ et $\gamma = y^2$). On notera que, conformément au théorème de Hilbert-Serre, on a $P_{S^W} = f(t)/(1-t^2)^3$, où $f(t) = 1 - t^4$.

Exemple 2.9. La famille (triplement) infinie de groupes engendrés par des réflexions complexes est $G(de, e, r) \subset \mathrm{GL}_r(\mathbb{Q}(\zeta_{de}))$ défini comme l'ensemble des matrices monômiales à coefficients dans μ_{de} et dont le produit des coefficients est dans μ_d.

Si D est le sous-groupe des matrices diagonales de $G(de,e,r)$ alors il est clair que $|D| = (de)^r/e$ et $G(de,e,r) = D \rtimes \mathfrak{S}_r$.

Appelons t_i la matrice de la permutation $(i-1,i)$, $s(e)$ la matrice $\begin{pmatrix} 0 & \zeta_e^{-1} & 0 \\ \zeta_e & 0 & 0 \\ 0 & 0 & \mathrm{Id} \end{pmatrix}$, et $t(d)$ la matrice $\mathrm{diag}(\zeta_d, 1, \ldots, 1)$. Toutes ces matrices sont de vraies réflexions sauf la dernière qui n'est qu'une pseudo-réflexion quand $d > 2$. On vérifie aisément que :
• $G(e,e,r)$ est engendré par $s(e), t_2, \ldots, t_r$.
• $G(d,1,r)$ est engendré par $t(d), t_2, \ldots, t_r$.
• Les cas ci-dessus sont les seuls cas où $G(de,e,r)$ est engendré par r réflexions dans les autres cas il en faut $r+1$ (de même, 8 des 34 groupes sporadiques nécessitent $r+1$ réflexions (r pour les autres)). $G(de,e,r)$ est engendré par $t(d), s(ed), t_2, \ldots, t_r$.

Si $v_1, \ldots, v_r$ est la base de V dans laquelle nous avons écrit les matrices ci-dessus, des générateurs algébriquement indépendants de l'anneau des invariants de $G(ed,e,r)$ sont : $f_k = \sum_{j_1<\ldots<j_k} v_{j_1}^{de} \ldots v_{j_k}^{de}$ pour $k = 1, \ldots, r-1$ et $f_r = (v_1 \ldots v_r)^d$. En effet : il est clair que ce sont des invariants, ils sont algébriquement indépendants car $v_1, \ldots, v_r$ sont algébriques sur $f_1, \ldots, f_r$ (les v_i^{de} sont zéros de $x^r - f_1 x^{r-1} + \ldots + (-1)^{r-1} f_{r-1} x + (-1)^r f_r^e$) et le produit de leurs degrés : $de, 2de, \ldots, (r-1)(de), rd$ est l'ordre de $G(de,e,r)$.

Remarque 2.10. Notons que les f_i ne sont pas uniques : par exemple, si on prend $G(2,1,2)$ on vient de voir que $\deg(f_1) = 2$ et $\deg(f_2) = 4$. Alors en remplaçant f_2 par $f_2 + f_1^2$ on a un autre système d'invariants algébriquement indépendants. Par contre, 2.6 montre que les degrés des f_i sont uniques.

3. Groupes de réflexion réels

Avant de démontrer que tout groupe de réflexion réel fini est un groupe de Coxeter, nous allons définir et étudier cette notion.

Groupes de Coxeter. Soit W un groupe engendré par un ensemble S d'involutions. Tout élément de w est produit d'un nombre fini d'éléments de S, donc est l'image dans W d'un mot du monoïde libre S^* engendré par S. On dit que $s_1 \ldots s_k \in S^*$ est une *décomposition réduite* de $w \in W$ si c'est un mot de longueur minimum d'image w, et cette longueur est appelée longueur de w et notée $l(w)$. Si $s, s' \in S$, et que le produit ss' est d'ordre fini m, on note $\Delta_{s,s'}$ le mot $\underbrace{ss'ss'\cdots}_{m \text{ termes}}$. Dans W, on a la relation $\Delta_{s,s'} = \Delta_{s',s}$ dite *relation de tresse* liant s et s' (la raison de cette terminologie apparaîtra plus tard) et les deux membres sont des décompositions réduites du même élément de W. Si l'ordre de ss' est infini, on dit que $\Delta_{s,s'}$ n'existe pas.

Définition 3.1. *On dit que (W,S) comme ci-dessus est un système de Coxeter si*

$$\langle s \in S \mid s^2 = 1, \Delta_{s,s'} = \Delta_{s',s} \text{ quand } \Delta_{s,s'} \text{ existe} \rangle$$

est une présentation[5] *de W.*

Attention ! Une telle présentation ne définit un système de Coxeter que si la longueur du mot $\Delta_{s,s'}$ est l'ordre de ss' ; il se trouve que c'est toujours le cas (cf. 3.19), mais ce n'est pas évident.

[5] rappel : groupe libre, présentation de groupes, de monoïdes

Nous utiliserons la terminologie suivante dans un système de Coxeter : les éléments de S seront appelés les *réflexions élémentaires* de W, les éléments de l'ensemble R des éléments de W conjugués à un élément de S seront appelés les *réflexions* de W.

Si W possède un ensemble S d'involutions telles que (W,S) soit un groupe de Coxeter, on dit que W est un groupe de Coxeter, et que S est un ensemble de générateurs de Coxeter de W.

Théorème 3.2. *Soit S un ensemble d'involutions engendrant un groupe W. Les propriétés suivantes sont équivalentes :*
(i) (W,S) est un système de Coxeter.
(ii) (Condition d'échange) Si $s_1 \dots s_k$ est une décomposition réduite de w et $s \in S$ est tel que $l(ws) \leq l(w)$, alors il existe i tel que $ws = s_1 \dots \hat{s}_i \dots s_k$.

Et sous ces conditions on a :
(iii) (Lemme de Matsumoto) Deux décompositions réduites d'un même mot sont équivalentes par relations de tresses. En d'autres termes, toute application de $f : S \to M$ dans un monoïde (induisant donc une application encore notée $f : S^* \to M$) telle que $f(\Delta_{s,s'}) = f(\Delta_{s',s})$ quand $\Delta_{s,s'}$ existe est constante sur l'ensemble des décompositions réduites d'un élément donné de W.

Démonstration. Nous allons montrer (i)⇒(ii)⇒(iii), et que sous la condition que $l(ws) \neq l(w)$ pour $w \in W, s \in S$ (qui est par exemple impliquée par (ii)), alors (iii)⇒(i).

Lemme 3.3. *Soit (W,S) un système de Coxeter, et soit N l'application de S^* dans l'ensemble des parties de R qui associe à $s_1 \dots s_k$ l'ensemble des éléments de R qui apparaissent un nombre impair de fois dans la suite $\{s_k, {}^{s_k}s_{k-1}, \dots, {}^{s_k s_{k-1} \dots s_2}s_1\}$. Alors $N(s_1 \dots s_k)$ ne dépend que de l'image w de $s_1 \dots s_k$ dans w (nous le noterons $N(w)$) et il a $l(w)$ éléments.*

Démonstration. Pour voir que N ne dépend que de l'image d'un élément dans W, on utilise que W est en bijection avec l'ensemble des classes de S^* pour la relation qui est la clôture transitive des équivalences $assb = ab$ et $a\Delta_{s,s'}b = a\Delta_{s',s}b$ (cela résulte de la définition d'une présentation d'un groupe dans le cas particulier où les générateurs sont des involutions). Pour vérifier que N est compatible avec ces équivalences, on utilise le fait qui est immédiat d'après la définition que $N(xy) = N(y) \dot{+} \overline{y}^{-1} N(x) \overline{y}$ où $\dot{+}$ désigne la différence symétrique (somme modulo 2 des fonctions caractéristiques) et où $\overline{y}$ est l'image de y dans W. En utilisant cette égalité, les relations à démontrer résultent de $N(ss) = \emptyset$ et de $N(\Delta_{s,s'}) = N(\Delta_{s',s})$, égalités qui sont immédiates à vérifier.

La deuxième assertion du lemme vient du fait que si la décomposition $s_1 \dots s_k$ est réduite, les éléments de la suite $\{s_k, {}^{s_k}s_{k-1}, \dots, {}^{s_k s_{k-1} \dots s_2}s_1\}$ sont tous distincts. En effet, s'il existe $i < j$ tels que $s_k \dots s_i \dots s_k = s_k \dots s_j \dots s_k$ alors $s_i s_{i+1} \dots s_j = s_{i+1} s_{i+2} \dots s_{j-1}$ ce qui contredit le fait que la décomposition $s_1 \dots s_k$ soit réduite. □

Montrons maintenant (i)⇒(ii). Si $l(ws) \leq l(w)$, alors $l(ws) < l(w)$. En effet la présentation de W montre que $s \mapsto -1$ se prolonge en un caractère de degré 1 de W donné par $w \mapsto (-1)^{l(w)}$, donc $(-1)^{l(ws)} = -(-1)^{l(w)}$. Si $l(ws) < l(w)$, alors on obtient une décomposition réduite de w en faisant suivre par s une décomposition de ws, donc on en déduit que $s \in N(w)$. Il existe donc i tel que $s = s_k \dots s_i \dots s_k$, ce qui donne $ws = s_1 \dots \hat{s}_i \dots s_k$ c.q.f.d.

Montrons maintenant (ii)⇒(iii). Soit $f : S^* \to M$ une application comme dans l'énoncé et montrons par récurrence sur $l(w)$ que deux décompositions réduites de w ont même image dans M. Raisonnant par l'absurde, soient $s_1 \dots s_k$ et $s'_1 \dots s'_k$ deux décompositions réduites d'image différente par f. Par la condition d'échange, on a $s'_1 s_1 \dots s_k = s_1 \dots \hat{s}_i \dots s_k$, *i.e.* $s_1 \dots s_k = s'_1 s_1 \dots \hat{s}_i \dots s_k$. Par hypothèse de récurrence, leurs premières lettres étant égales, on a $f(s'_1 s_1 \dots \hat{s}_i \dots s_k) = f(s'_1 \dots s'_k)$ et donc on doit avoir $i = k$ sinon toujours par hypothèse de récurrence on aurait $f(s'_1 s_1 \dots \hat{s}_i \dots s_k) = f(s_1 \dots s_k)$. On arrive donc à la conclusion que $s'_1 s_1 \dots s_{k-1}$ est une autre décomposition réduite de w telle que $f(s'_1 s_1 \dots s_{k-1}) \neq f(s_1 \dots s_k)$.

Reprenant le même raisonnement à partir de ces deux dernières décompositions, on trouve que $s_1 s'_1 s_1 \dots s_{k-2}$ est une décomposition réduite de w telle que

$$f(s_1 s'_1 s_1 \dots s_{k-2}) \neq f(s'_1 s_1 \dots s_{k-1});$$

continuant ainsi de proche en proche, on trouve que $w = \Delta_{s_1,s'_1} = \Delta_{s'_1,s_1}$ et $f(\Delta_{s_1,s'_1}) \neq f(\Delta_{s'_1,s_1})$, ce qui contredit l'hypothèse.

Montrons maintenant (iii)⇒ (i) sous la condition que $l(ws) \neq l(w)$ quand $s \in S$. (i) est équivalent au fait que toute application $f : S \to G$ de S dans un groupe G (induisant donc une application encore notée $f : S^* \to G$) telle $f(s^2) = 1$ et $f(\Delta_{s,s'}) = f(\Delta_{s',s})$ induit un homomorphisme $W \to G$. On sait déjà, d'après le lemme de Matsumoto, que f induit une application bien définie $f : W \to G$. Il reste à voir que $f(w)f(w') = f(ww')$ et, puisque S engendre W, il suffit de voir que $f(s)f(w) = f(sw)$. Si $l(sw) > l(w)$ alors puisque f est définie en faisant le produit suivant une décomposition réduite le résultat est clair. Si $l(sw) < l(w)$, alors l'égalité $f(s)^2 = 1$ permet de ré-écrire l'équation à démontrer $f(w) = f(s)f(sw)$ et le même raisonnement s'applique. □

Si (W, S) est un système de Coxeter, pour $I \subset S$, on note W_I le sous-groupe de W engendré par I (par (ii) du théorème précédent il est clair que (W_I, I) est un système de Coxeter). Nous aurons besoin de la notion suivante :

Définition-Théorème 3.4. *$w \in W$ est dit I-réduit s'il vérifie une des conditions équivalentes suivantes :*
(i) Pour tout $v \in W_I$, on a $l(vw) = l(v) + l(w)$.
(ii) Pour tout $s \in I$, on a $l(sw) > l(w)$.
(iii) w est de longueur minimum dans $W_I w$.
Et il y a un seul élément I-réduit dans $W_I w$.

Démonstration. Il est clair que (i)⇒(ii) et (i)⇒(iii), ainsi que (iii)⇒(ii) car (iii) implique que $l(sw) \geq l(w)$. Montrons que non (iii)⇒ non (ii). Si w' n'est pas de longueur minimum dans $W_I w'$, c'est-à-dire que $w' = vw$ avec $v \in W_I$ et $l(w) < l(w')$, en ajoutant un à un les termes d'une décomposition réduite de v à w et en appliquant à chaque fois le lemme d'échange, on trouve une décomposition réduite $\hat{v}\hat{w} (= vw = w')$ où on a noté $\hat{v}$ (resp. $\hat{w}$) le produit d'une suite extraite stricte d'une décomposition réduite de v (resp. w). Comme $l(\hat{w}) \leq l(w) < l(w')$, on a $l(\hat{v}) > 0$, donc il existe une décomposition réduite de w' commençant par un élément de I, donc w' ne vérifie pas (ii). De même non (i)⇒ non (iii) car si $l(vw) < l(v) + l(w)$ alors une décomposition réduite de vw est de la forme $\hat{v}\hat{w}$ où $l(\hat{w}) < l(w)$. Donc $\hat{w} \in W_I w$ et est de longueur inférieure à celle de w.

Enfin un élément vérifiant (i) est clairement unique dans $W_I w$. □

Groupes de réflexion réels. Soit maintenant W un groupe de réflexions fini sur le $\mathbb{R}$-espace vectoriel V. On appelle *chambres* de l'arrangement $\mathcal{A}_W$ les composantes connexes de $V - \bigcup_{H\in\mathcal{A}_W} H$; on appelle murs d'une chambre C les $H \in \mathcal{A}_W$ tels que $H \cap \overline{C}$ soit un fermé de H d'intérieur non vide. Remarquons que par 1.1 et la remarque qui suit, pour tout $H \in \mathcal{A}_W$ il existe une unique réflexion que nous noterons s_H d'hyperplan H.

Nous allons voir que W est un *groupe de Coxeter*.

Proposition 3.5. *Soit W un groupe de réflexion fini dans V espace vectoriel réel de dimension finie. Alors :*
(i) Soit C une chambre, $\mathcal{M}$ l'ensemble de ses murs, et soit $S = \{s_H \mid H \in \mathcal{M}\}$. Alors (W, S) est un système de Coxeter, et on a $m_{s_H,s_{H'}} = |\{H'' \in \mathcal{A}_W \mid H'' \supset H \cap H'\}|$.
(ii) Le fixateur dans W de $x \in V$ est engendré par les réflexions qui fixent x.

Démonstration. Notons W' le sous-groupe de W engendré par S. Montrons d'abord que pour tout $x \in V$, il existe $w \in W'$ tel que $w(x) \in \overline{C}$.

Lemme 3.6. *Si $W \subset \mathrm{GL}(V)$ est un sous-groupe fini, alors il existe une forme B bilinéaire symétrique définie positive (un produit scalaire) invariante par W.*

Démonstration. Choisissons une forme $B(x, y)$ arbitraire définie positive ; alors $\sum_{w\in W} B(wx, wy)$ l'est aussi et est invariante par W. □

Grâce à ce lemme, nous pouvons supposer que V est muni d'un produit scalaire tel que les réflexions de W soient orthogonales. Choisissons $a \in C$ et soit y un point de l'orbite de x sous W' à distance minimale de a. Alors on doit nécessairement avoir $y \in \overline{C}$. En effet, si a et y sont de part et d'autre du mur H de C, alors $s_H(y)$ est plus près de a que y.

On en déduit que pour toute chambre C' il existe $w \in W'$ tel que $w(C') = C$. En effet, par ce qui précède on peut trouver w tel que $w(C') \cap \overline{C} \neq \emptyset$, et ceci implique $w(C') = C$. On en déduit aussi que toute réflexion s_H de W est dans W'. En effet, soit C' une chambre dont H est un mur. Soit $w \in W'$ tel que $w(C') = C$. Alors $w(H)$ est un mur de C, donc $ws_Hw^{-1} \in S$. Donc $W' = W$.

Pour démontrer (i), nous utiliserons le lemme suivant :

Lemme 3.7. *Soit W un groupe engendré par un ensemble d'involutions S et soit $\{D_s\}_{s\in S}$ un ensemble de parties de W contenant 1, telles que $D_s \cap sD_s = \emptyset$ pour tout $s \in S$, et telles que pour $s, s' \in S$ on ait $w \in D_s, ws' \notin D_s \Rightarrow ws' = sw$. Alors (W, S) est un système de Coxeter, et on a $D_s = \{w \in W \mid l(sw) > l(w)\}$.*

Démonstration. Soit $s_1 \dots s_k$ une décomposition réduite de $w \notin D_s$ et soit i minimal tel que $s_1 \dots s_i \notin D_s$ ($i > 0$ puisque $1 \in D_s$). Alors de $s_1 \dots s_{i-1} \in D_s$ et $s_1 \dots s_i \notin D_s$ on tire $ss_1 \dots s_{i-1} = s_1 \dots s_i$, d'où $sw = s_1 \dots \hat{s}_i \dots s_k$ (et $l(sw) < l(w)$). Si $w \in D_s$ alors $sw \notin D_s$ et appliquant le même raisonnement à sw on a $l(w) < l(sw)$. Au total on a donc vérifié la condition d'échange, d'où le résultat. □

Nous appliquons le lemme en prenant pour H mur de C l'ensemble D_{s_H} égal à l'ensemble des w tels que $w(C)$ soit du même coté de H que C. La seule chose non triviale à vérifier est que si $w \in D_{s_H}$ et si H' est un mur de C tel que $ws_{H'} \notin D_{s_H}$, alors $ws_{H'} = s_Hw$. Par hypothèse $ws_{H'}(C)$ et $w(C)$ sont de part et d'autre de H, donc $s_{H'}(C)$ et C sont de part et d'autre de $w^{-1}(H)$. Ceci n'est possible que si $H' = w^{-1}(H)$, *i.e.* $s_{H'} = w^{-1}s_Hw$, d'où le résultat.

La valeur annoncée pour $m_{s_H,s_{H'}}$ se voit en se ramenant au rang 2, spécifiquement en considérant le groupe engendré par les $s_{H''}$ dans l'espace $V/(H \cap H')$.

On utilise 3.6 pour réaliser s_H et $s_{H'}$ comme des réflexions orthogonales. Alors $s_H s_{H'}$ est une rotation d'angle 2θ, si θ est l'angle entre H et H'. Cet angle doit être un multiple rationnel de π pour que le groupe engendré soit fini, et on trouve $m_{s_H,s_{H'}} = \pi/\theta$. Le groupe engendré par s_H et $s_{H'}$ est un groupe diédral.

Montrons (ii). Soit C une chambre telle que $x \in \overline{C}$. Nous allons montrer par récurrence sur $l(w)$ que si $w(x) = x$ alors w appartient au sous-groupe de W engendré par les s_H où H est un mur de C contenant x. Si $w \neq 1$, il existe un mur H de C tel que $l(s_H w) < l(w)$ (où ici nous mesurons la longueur par rapport au système S des s_H où H est un mur de C). On a $x \in \overline{C} \cap w(\overline{C})$ puisque w fixe x ; d'autre part, puisque $w \notin D_{s_H}$ (cf. notations du lemme), $w(C)$ et C sont de part et d'autre de H, d'où $\overline{w(C)} \cap \overline{C} \subset H$ et d'où $x \in H$, ce qui permet de conclure par récurrence. □

Remarque 3.8. La preuve ci-dessus peut s'étendre au cas où V est un espace affine et où W est fini modulo les translations qu'il contient (on obtient un *groupe de Weyl affine*).

Remarque 3.9. Nous pourrons étendre le (ii) de 3.5 aux groupes de réflexions complexes (résultat dû à Steinberg), mais la preuve sera plus difficile.

Exercice 3.10. Montrer que $(\mathfrak{S}_n, \{(i, i+1)\}_{i=1\ldots n-1})$ est un système de Coxeter, et qu'on a $l(w) = |\{i < j \mid w(i) > w(j)\}|$ (on utilisera 3.7 avec $D_{(i,i+1)} = \{w \mid w^{-1}(i) < w^{-1}(i+1)\}$ puis on montrera que $N(w) = \{(i,j) \mid i < j \text{ et } w(i) > w(j)\}$).

Exercice 3.11. Montrer que $(1,2) \mapsto (1,2)(3,4)(5,6), (1,2,3,4,5,6) \mapsto (2,3)(4,5,6)$ donne un automorphisme de $\mathfrak{S}_6$. Montrer que pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ doit préserver les transpositions, et en déduire qu'il est intérieur.

Exercice 3.12. Montrer que dans la situation de 3.5 il existe un élément $w_0 \in W$ qui est l'unique élément ayant une des deux propriétés suivantes :
- w_0 est de longueur maximum parmi les éléments de W.
- $w_0(C) = -C$.

(On utilisera que $-C$ est la seule chambre séparée de C par tous les hyperplans de $\mathcal{M}$).

Exercice 3.13. Soit $(W, \{s, s'\})$ un système de Coxeter avec $m = m_{s,s'} < \infty$. Montrer que
- Les degrés de réflexion de W sont 2 et m.
- $\sum_{w \in W} t^{l(w)} = \frac{(t^2-1)(t^m-1)}{(t-1)^2}$
- Si m est le double d'un entier impair, alors $(W, \{s, w_0 s', w_0\})$ est aussi un système de Coxeter.

Pour les quelques énoncés suivants nous prenons à nouveau pour k un sous-corps de $\mathbb{C}$ arbitraire.

Proposition 3.14. *(Double commutant) Soit A une k-algèbre semi-simple et soit V un A-module de dimension finie. Soit $Im_V(A)$ l'image de A dans $\mathrm{End}_k(V)$. Alors si $D = \mathrm{End}_A(V)$, on a $\mathrm{End}_D(V) = Im_V(A)$.*

Démonstration. Soit $n = \dim V$.Un élément de $\mathrm{Im}_{V^n}(A)$ s'identifie à $\mathrm{diag}(a)$ pour $a \in \mathrm{Im}_V(A)$, une matrice diagonale par bloc avec le même élément $a \in \mathrm{Im}_A(V)$ répété sur la diagonale, donc $\mathrm{End}_A(V^n)$ s'identifie à $M_n(D)$, les matrices $n \times n$ à coefficients dans D. Si $f \in \mathrm{End}_D(V)$, alors $\mathrm{diag}(f) \in \mathrm{End}_{M_n(D)}(V^n)$. Soit $\{x_1, \dots, x_n\}$ une k-base de de V. Alors, A étant semi-simple, il existe un sous-module supplémentaire de $A.(x_1, \dots, x_n)$ dans V^n, *i.e.* le projecteur π sur $A.(x_1, \dots, x_n)$ appartient à $M_n(D) = \mathrm{End}_A(V^n)$. Donc si $f \in \mathrm{End}_D(V)$, alors $\mathrm{diag}(f)$ commute à π, donc $(f(x_1), \dots, f(x_n))$ est dans l'image de π, *i.e.* il existe $a \in \mathrm{Im}_A(V)$ tel que $(f(x_1), \dots, f(x_n)) = a(x_1, \dots, x_n)$. Comme $\{x_1, \dots, x_n\}$ est une base on en déduit $f = a$. On a donc $\mathrm{End}_D(V) \subset \mathrm{Im}_A(V)$. L'inclusion dans l'autre sens est évidente. □

Définition-Théorème 3.15. *Soit A une k-algèbre semi-simple et soit V un A-module irréductible de dimension finie. On dit que V est absolument irréductible si $V \otimes \mathbb{C}$ est encore un $A \otimes \mathbb{C}$-module irréductible. On a équivalence entre :*
(i) V est absolument irréductible.
(ii) $\mathrm{End}_A(V) = k\,\mathrm{Id}$.
(iii) $Im_V(A) = \mathrm{End}_k(V)$.

Démonstration. Montrons (i)⇒(ii). Puisque V est simple, si $f \in \mathrm{End}_A(V)$ et $f \neq 0$ alors f est un isomorphisme, sinon $\mathrm{Ker}\, f$ serait un sous-A-module propre de V (donc $\mathrm{End}_A(V)$ est un *corps gauche*). Si $f \neq 0$ alors l'extension $f_{\mathbb{C}}$ de f à $V \otimes \mathbb{C}$ possède au moins une valeur propre λ ; on a $f - \lambda I \in \mathrm{End}_{A\otimes\mathbb{C}}(V \otimes \mathbb{C})$ donc puisque $f - \lambda I$ n'est pas un isomorphisme on a $f = \lambda I$.

La proposition 3.14 implique que (ii)⇒(iii).

Enfin (iii)⇒(i) est clair : si $\mathrm{Im}_V(A) = \mathrm{End}_k(V)$ alors on a aussi $\mathrm{Im}_{V\otimes\mathbb{C}} A \otimes \mathbb{C} = \mathrm{End}_{\mathbb{C}}(V \otimes \mathbb{C})$; ce ne serait pas le cas si $V \otimes \mathbb{C}$ n'était pas irréductible. □

Remarque 3.16. On a vu que $\mathrm{End}_A(V)$ est un corps gauche D. Le degré d'un corps gauche D sur son centre K est un carré m^2. L'entier m est appelé *l'indice de Schur* de V. La décomposition en modules simples de $V \otimes \mathbb{C}$ est de la forme $m.(\sum_{\sigma\in\mathrm{Gal}(K/k)} {}^{\sigma}\rho)$, où K est la plus petite extension de k sur laquelle le caractère de ρ est défini, mais où la représentation ρ n'est définie que sur une extension de degré m de K (alors que $m\rho$ est définie sur K).

Lemme 3.17. *Soit $W \subset \mathrm{GL}(V)$ un sous-groupe fini.*
(i) Si V est irréductible et $\mathrm{Ref}(W) \neq \emptyset$ alors V est absolument irréductible.
(ii) Si V est absolument irréductible alors deux formes bilinéaires invariantes par W sont proportionnelles.

Démonstration. Pour (i) il suffit de voir que tout $u \in \mathrm{End}_k(V)$ qui est W-invariant est un scalaire. Soit s une réflexion de G ; alors u stabilise le noyau de $1 - s$, qui est une droite ; soit α sa valeur propre sur cette droite. Alors $u - \alpha\,\mathrm{Id}$ est encore W-invariant et a un noyau non trivial ; comme W est irréductible cet élément doit être nul donc u est scalaire.

Pour (ii), soit B et B' deux formes bilinéaires invariantes par W. Alors on voit d'abord que si $B \neq 0$, elle est non dégénérée : sinon l'orthogonal de V pour B serait un sous-espace propre non trivial W-invariant. Donc B, ainsi que B', réalise un isomorphisme de V sur V^*. Il en résulte qu'il existe $u \in \mathrm{GL}(V)$ tel que $B'(x, y) = B(u(x), y)$. De $B(u(x), y) = B(u(wx), wy) = B(wu(x), wy)$ pour $w \in W$ et de la

non-dégénérescence de B on tire que u est W-invariant. Comme W est absolument irréductible u est un scalaire d'où le résultat. □

Nous supposons à nouveau pour le reste de la section que $k = \mathbb{R}$. Notons qu'une conséquence de 3.17(i) et 3.15(ii) est que si W comme en 3.5 possède un élément non trivial dans son centre, c'est le scalaire -1. Et par 3.12, c'est w_0.

Proposition 3.18. *Soit W comme dans 3.5, supposé irréductible. Soit B un produit scalaire comme dans 3.6, et pour $H \in \mathcal{M}$ soit e_H le vecteur unitaire orthogonal à H situé du même côté de H que C. Alors*
(i) Les e_H sont linéairement indépendants.
(ii) La forme B est donnée par $B(e_H, e_{H'}) = -\cos(\pi/m_{s_H,s_{H'}})$.

Démonstration. Le (ii) est clair en se plaçant dans le sous-espace de dimension 2 donné par l'orthogonal de $H \cap H'$.

Pour voir le (i), notons qu'il résulte du (ii) que si $H \neq H'$ alors $B(e_H, e_{H'}) \leq 0$. Soit q la forme quadratique associée à B et soit $\sum_{H\in\mathcal{M}} c_H e_H = 0$ une relation de dépendance linéaire. Alors $B(e_H, e_{H'}) \leq 0$ implique que $q(\sum_{H\in\mathcal{M}} |c_H| e_H) \leq q(\sum_{H\in\mathcal{M}} c_H e_H)$, donc $\sum_{H\in\mathcal{M}} |c_H| e_H = 0$. Notons maintenant que si $t \in C$, le choix de e_H implique que $B(t, e_H) > 0$. Alors $\sum_{H\in\mathcal{M}} |c_H| B(t, e_H) = 0$ implique $|c_H| = 0$ cqfd. □

Remarquons qu'une conséquence de la proposition ci-dessus est que si V est irréductible alors $|S| = \dim V$.

Représentation géométrique des groupes de Coxeter. À un système de Coxeter on associe une *matrice de Coxeter*, matrice symétrique dont le coefficient $m_{s,s'}$ est la longueur de $\Delta_{s,s'}$ quand cet élément existe (et on pose $m_{s,s} = 1$), sinon ∞.

Proposition 3.19. *Pour toute matrice symétrique $\{m_{s,s'}\}_{s,s'\in S}$ à coefficients entiers ≥ 2 ou $+\infty$ et à coefficients diagonaux 1 il existe un groupe de Coxeter W qui admet cette matrice comme matrice de Coxeter ; de plus W peut être réalisé comme groupe de réflexions dans un espace vectoriel réel de dimension $|S|$.*

Démonstration. La construction est suggérée par 3.18. On munit $V = \mathbb{R}^{|S|}$, de base $\{e_s\}_{s\in S}$, de la forme bilinéaire donnée par $\langle e_s, e_{s'} \rangle = -\cos(\pi/m_{s,s'})$ (où on pose $\pi/m_{s,s'} = 0$ si $m_{s,s'} = \infty$). On a donc $\langle e_s, e_s \rangle = 1$ et $\langle e_s, e_{s'} \rangle = -1$ si $m_{s,s'} = \infty$. On fait agir sur V le groupe W défini par la présentation $\langle s \in S \mid (ss)^{m_{s,s'}} = 1\rangle$ en faisant agir s par $s(x) = x - 2\langle x, e_s \rangle e_s$. Alors s est une réflexion, qui préserve $\langle\ ,\ \rangle$.

Pour vérifier qu'on a une représentation de W, il faut calculer l'ordre de ss'. Posons $\lambda = \langle e_s, e_{s'} \rangle$. On obtient $ss'(e_s) = (4\lambda^2 - 1)e_s - 2\lambda e_{s'}$ et $ss'(e_{s'}) = 2\lambda e_s - e_{s'}$. Si $\lambda = -1$, on a $ss'(e_s + e_{s'}) = e_s + e_{s'}$, d'où, en itérant la première formule qui s'écrit dans ce cas $ss'(e_s) = 2(e_s + e_{s'}) + e_s$, on obtient $(ss')^m(e_s) = 2m(e_s + e_{s'}) + e_s$ et ss' est d'ordre infini. Sinon, identifions le plan engendré par e_s et $e_{s'}$ au plan complexe en identifiant e_s à 1 et $e_{s'}$ à $-e^{-i\theta}$ où $\theta = \pi/m_{s,s'}$. Alors sur ce plan $\langle\ ,\ \rangle$ s'identifie au produit scalaire usuel et on trouve $ss'(e_s) = (4\cos^2\theta - 1) - 2\cos\theta e^{-i\theta} = e^{2i\theta}$ et $ss'(e_{s'}) = -2\cos\theta + e^{-i\theta} = -e^{i\theta}$, donc ss' agit sur ce plan comme une rotation d'angle $2\pi/m_{s,s'}$. Agissant trivialement sur l'orthogonal du plan pour $\langle\ ,\ \rangle$, ss' est donc d'ordre $m_{s,s'}$.

Nous avons donc déjà vu que W possède une représentation où ss' est d'ordre $m_{s,s'}$, donc toute matrice de Coxeter correspond à un groupe de Coxeter.

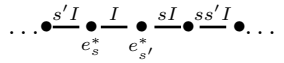
En fait la représentation de réflexion que nous venons de construire est injective, et fait donc de W un groupe de réflexion. Pour démontrer cela, nous considérons la représentation contragrédiente de W sur V^* . Pour $I \subset S$ nous posons $C_I = \{x^* \in V^* \mid x^*(e_s) > 0 \forall s \in I\}$, et on pose $C = C_S$ (c'est une chambre pour le système dual d'hyperplans). La fidélité de la représentation résulte alors du

Lemme 3.20. *(Tits) Si $w \neq 1$, alors $w(C) \cap C = \emptyset$.*

Démonstration. Pour $I \subset S$, soit $\alpha_I(w)$ l'élément de W_I de longueur maximum tel que $l(\alpha_I(w)) + l(\alpha_I(w)^{-1}w) = l(w)$ (cf. 3.4). Nous allons montrer par récurrence sur $l(w)$ que $w(C) \subset \alpha_I(w)C_I$ pour tout $I \subset S, |I| \leq 2$. Le lemme en résultera car si $w \neq 1$, il existe $s \in S$ tel que $\alpha_{\{s\}}(w) = s$, d'où $w(C) \subset sC_{\{s\}} = -C_{\{s\}} \not\supset C$.

Supposons donc l'assertion vraie pour les éléments de longueur inférieure à w, et commençons par la démontrer quand $I = \{s\}$. Si $\alpha_I(w) = s$ alors $w = sw'$ où $l(w') < l(w)$ et $\alpha_I(w') = 1$ d'où $w(C) = sw'(C) \subset sC_{\{s\}}$ q.e.d. Si $\alpha_I(w) = 1$ choisissons s' tel que $\alpha_{\{s'\}}(w) = s'$ et écrivons $w = \alpha_{\{s,s'\}}(w)w'$. Puisque $l(w') < l(w)$ on a par récurrence $w(C) = \alpha_{\{s,s'\}}(w)w'(C) \subset \alpha_{\{s,s'\}}(w)(C_{\{s,s'\}})$. En prenant le sous-espace de V engendré par e_s et $e_{s'}$, ce qui revient à prendre le quotient correspondant de V^*, on est donc ramené à la même question pour le groupe diédral $W_{s,s'}$, *i.e.* de montrer que si $w' = \alpha_{\{s,s'\}}(w)$ vérifie $\alpha_{\{s\}}(w') = 1$ alors $w'C' \subset C'_{\{s\}}$ où on a noté C' l'analogue de C pour $W_{s,s'}$ (l'image de C dans le quotient, qui coïncide avec celle de $C_{\{s,s'\}}$).

Si $m_{s,s'} = \infty$, soit $\{e_s^*\}_{s\in S}$ la base duale de $\{e_s\}_{s\in S}$; en utilisant la définition $(se_s^*)(x) = e_s^*(sx)$, on trouve pour l'action contragrédiente que s agit par $s(e_s^*) = e_s^* + 2(e_{s'}^* - e_s^*)$ et $s(e_{s'}^*) = e_{s'}^*$ (et l'on a la formule symétrique pour l'action de s'). L'élément s (resp. s') préserve la droite affine passant par e_s^* et $e_{s'}^*$ et sur cette droite agit comme la réflexion par rapport à $e_{s'}^*$ (resp e_s^*). L'intersection I de C' avec cette droite est le segment délimité par e_s^* et $e_{s'}^*$, et les images par s (resp s') sont translatées ; on voit que si w' a une décomposition réduite commençant par s', l'image de I par w' est du même côté de $e_{s'}^*$ que e_s^* cqfd.



On notera que dans le cas $m_{s,s'} = \infty$, dans la représentation sur V les hyperplans de réflexion de s et s' intersectent tous deux le plan $\langle e_s, e_{s'}\rangle$ en le vecteur $e_s + e_{s'}$, donc la chambre fondamentale est stable par ss'. C'est ce qui nécessite le passage au dual.

Si $m_{s,s'} < \infty$ alors $\langle\ ,\ \rangle$ est définie positive donc on peut identifier V à V^* au moyen de cette forme pour faire le dessin, qui ressemble à une version circulaire du précédent (s et s' préservent le cercle unité, et l'intersection de I de C' avec ce cercle est l'arc de cercle délimité par e_s^* et $e_{s'}^*$; les transformés sI,$s'I$,etc... sont des arcs disposés comme dans le dessin précédent, avec $\Delta_{s,s'}I$ diamétralement opposé à I).

Enfin montrons l'assertion pour $I = \{s, s'\}$. Si $\alpha_{\{s,s'\}}(w) = 1$ alors $\alpha_{\{s\}}(w) = \alpha_{\{s'\}}(w) = 1$ et $w(C) \subset C_{\{s\}} \cap C_{\{s'\}} = C_{\{s,s'\}}$ q.e.d. Sinon $w = \alpha_{\{s,s'\}}(w)w'$ où $w'(C_{\{s,s'\}}) = C_{\{s,s'\}}$ d'où le résultat. □

□

Classification des groupes de Coxeter finis. Un groupe de Coxeter est encodé par son *graphe de Coxeter*. Ce graphe décrit la matrice de Coxeter, et est construit

comme suit : les sommets sont en bijection avec l'ensemble S, et il y a une arête entre s et s' quand $m_{s,s'} \geq 3$. Cette arête est décorée par $m_{s,s'}$. Les conventions pour les graphes on été particulièrement adaptées aux groupes dits "de Weyl" ou "cristallographiques", qui sont les groupes de Coxeter finis définis sur $\mathbb{Q}$: on verra que 3.19 définit un groupe sur $\mathbb{Q}$ si $m_{s,s'} \in \{2, 3, 4, 6\}$. Par suite, on convient qu'une arête telle que $m_{s,s'} = 3$ (resp. 4, 6) est tracée simple (resp. double, triple).

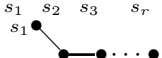
Proposition 3.21. *Soit Γ un graphe de Coxeter, W le groupe de Coxeter correspondant, soit V la représentation géométrique de W (c.f. 3.19) et $B(\Gamma)$ la forme bilinéaire correspondante. Alors*
(i) V est irréductible si et seulement si Γ est connexe.
(ii) W est fini si et seulement si $B(\Gamma)$ est définie positive.

Démonstration. Pour (i), il est clair que V se décompose en sous-représentations suivant les composantes connexes de Γ. Réciproquement soit U un sous-espace W-stable de V. Notons que pour tout $s \in S$, on a $e_s \in U$ ou $e_s \perp U$. En effet tout sous-espace stable par s et qui n'est pas dans H_s contient $< e_s >$ (puisque si $x \notin H_s$, alors $s(x) - x$ est un multiple non nul de e_s). Donc U implique une partition $S = S_1 \coprod S_2$ où $S_1 = \{s \mid e_s \in U\}$ et $S_2 = \{s \mid e_s \perp U\}$ telle que si $s \in S_1$ et $S' \in S_2$ alors $\langle e_s, e_{s'} \rangle = 0$, *i.e.* une partition de Γ en deux composantes connexes.

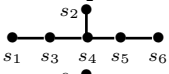
Pour (ii), on peut supposer V irréductible car $B(\Gamma)$ est définie positive (resp. $W(\Gamma)$ est fini) si et seulement si il en est ainsi pour chaque composante connexe de Γ. Si W est fini alors $B(\Gamma)$ est définie positive par 3.6 et 3.17(ii). Réciproquement, si $B(\Gamma)$ est définie positive son groupe orthogonal O est compact et un sous-groupe discret d'un groupe compact est fini. En effet, W est discret car si $x \in C$, l'ensemble $\{g \in \mathrm{GL}(V^*) \mid g(x) \in C\}$ est un voisinage ouvert de l'origine qui rencontre un seul élément de W. Si W était infini, il contiendrait au moins une suite $\{w_n\}_n$ convergente dans O. Alors $w_n^{-1} w_{n+1}$ convergerait vers l'origine ce qui est absurde puisqu'il existe un voisinage de l'origine contenant un seul élément de W. □

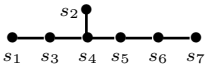
Théorème 3.22. *Les seuls graphes de Coxeter connexes donnant lieu à des groupes finis sont les suivants :*

- *Type* $A_n = G(1, 1, n+1)$

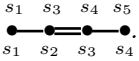
- *Type* $B_n = G(2, 1, n)$ 

- *Type* $D_n = G(2, 2, n)$

- *Type* $E_6 = G_{35}$ 

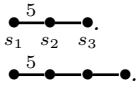
- *Type* $E_7 = G_{36}$ 

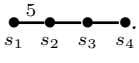
- *Type* $E_8 = G_{37}$ 

- *Type* $F_4 = G_{28}$ 

- *Type* $G_2 = G_{6,6,2}$ 

- *Type* $I_2(e) = G_{e,e,2}$ 

- *Type* $H_3 = G_{23}$ 

- *Type* $H_4 = G_{30}$ 

Démonstration. Nous ne détaillerons pas la preuve que les formes définies par ces graphes sont définies positives ; la preuve usuelle utilise les systèmes de racines. La preuve que nous suggérons au lecteur est de vérifier que les déterminants des $B(\Gamma)$ sont positifs — cela le montrera aussi pour les mineurs principaux car ils correspondent à des $B(\Gamma')$ pour des sous-graphes ; et une matrice dont tous les mineurs principaux sont positifs définit une forme bilinéaire définie positive. Il pourra être plus commode de multiplier par 2 la matrice de $B(\Gamma)$ pour calculer le déterminant ; par exemple, pour le type A_n on trouvera par récurrence sur n que le déterminant de $2B(\Gamma)$ est $n+1$, et pour D_n on trouvera 4 (ces nombres sont *l'indice de connexion* du système de racines correspondant).

Excluons maintenant les graphes autres que ceux de l'énoncé. Disons qu'un graphe Γ est sphérique si $B(\Gamma)$ est définie positive. Nous allons utiliser constamment les valeurs de $-\cos\pi/m_{i,j}$ et de son carré pour les petites valeurs de $m_{i,j}$ qui sont :

$m_{i,j}$	2	3	4	5	6
$-\cos\pi/m_{i,j}$	0	$-1/2$	$-1/\sqrt{2}$	$-(1+\sqrt{5})/4$	$-\sqrt{3}/2$
$(\cos\pi/m_{i,j})^2$	0	$1/4$	$1/2$	$(3+\sqrt{5})/8$	$3/4$

Nous considérons un graphe Γ sphérique connexe et faisons les observations suivantes :

(i) Tout sous-graphe de Γ est sphérique (en effet un sous-graphe définit un sous-groupe).

(ii) Γ est un arbre. En effet, si $s_1,\dots,s_r$ est un circuit de Γ, et si on pose $v=e_{s_1}+\dots+e_{s_r}$, on a $\langle v,v\rangle = r+2\sum_{i=1}^{r-1}\langle e_{s_i},e_{s_{i+1}}\rangle + 2\langle e_{s_r},e_{s_1}\rangle \le 0$.

(iii) Si $\{j \mid j\in J\}$ sont les sommets adjacents à $s\in S$, alors $\sum_{j\in J}\langle e_s,e_j\rangle^2 < 1$. En effet cette inégalité est simplement l'écriture du fait que e_s est plus long que sa projection sur le sous-espace engendré par les e_j (dont les e_j forment une base orthonormée par (ii)).

Une conséquence immédiate de (iii) est de limiter les possibilités pour l'étoile d'un point à : une seule arête, deux arêtes l'une d'ordre 3 et l'autre d'ordre ≤ 5, ou 3 arêtes d'ordre 3.

(iv) Le graphe Γ' obtenu en retirant à Γ une arête d'ordre 3 est sphérique. En effet posons $B'=B(\Gamma')$; si (s,s') est l'arête ôtée, et e est le vecteur correspondant à $s=s'$ dans le graphe Γ', on trouve si v est combinaison linéaire de $e_{s''}$ avec $s''\neq s, s''\neq s'$ que $B'(v+\lambda e, v+\lambda e) = B'(v,v) + 2B'(v,\lambda e)+\lambda^2 = B(v,v)+2\lambda B(v,e_s+e_{s'})+\lambda^2 = B(v+\lambda(e_s+e_{s'}),v+\lambda(e_s+e_{s'}))-\lambda^2(1+2<e_s,e_{s'}>) = B(v+\lambda(e_s+e_{s'}),v+\lambda(e_s+e_{s'}))$.

Parmi les conséquences de (iv) on a que Γ a au plus une arête d'ordre >3 (sinon, en rapprochant les arêtes d'ordre >3 on a une configuration interdite par (iii)), et de même, Γ a au plus une étoile d'ordre 3 ; et si Γ a une arête d'ordre >3 c'est une chaîne.

(v) Si Γ est une chaîne $s_1,\dots,s_i,s'_j,s'_{j-1},\dots s'_1$ où toutes les arêtes sont d'ordre 3 sauf celle entre s_i et s'_j qui est d'ordre m, on pose $v=e_{s_1}+2e_{s_2}\dots+ie_{s_i}$ et $w=je_{s'_j}+\dots+e_{s'_1}$. Alors on trouve $\langle v,v\rangle = i(i+1)/2$, $\langle w,w\rangle = j(j+1)/2$ et $\langle v,w\rangle = -ij\cos\pi/m$. L'inégalité $\langle v,w\rangle^2 < \langle v,v\rangle\langle w,w\rangle$ donne alors $(i+1)(j+1) > 4ij\cos^2\pi/m$. En remplaçant $4ij\cos^2\pi/m$ par sa minoration $2ij$, on trouve $(i-1)(j-1)<2$ ce qui limite les possibilités où $i\le j$ à $(1,j)$,

$(2,2)$ et $(2,3)$. En reportant dans l'inégalité $(i+1)(j+1) > 4ij\cos^2\pi/m$, on tombe exactement sur les chaînes de l'énoncé.

(vi) Il reste le cas où Γ n'a que des arêtes simples et où il existe $s \in \Gamma$ tel que $\Gamma - \{s\}$ soit union de 3 chaînes de longueur p, q, r. Si u, v, w sont des vecteurs comme en (v) (de poids croissant quand on va vers le sommet commun s) et qu'on pose $e = e_s$, alors u, v, w sont orthogonaux ; en écrivant que e est plus long que sa projection sur le sous-espace engendré par u, v, w on obtient $1 > \langle e,u\rangle^2/\langle u,u\rangle + \langle e,v\rangle^2/\langle v,v\rangle + \langle e,w\rangle^2/\langle w,w\rangle$, ce qui, en tenant compte de $\langle e,u\rangle = -p/2$, $\langle e,v\rangle = -q/2$, $\langle e,w\rangle = -r/2$ et de $\langle u,u\rangle = p(p+1)/2$, etc... s'écrit $1/(p+1) + 1/(q+1) + 1/(r+1) > 1$, ce qui ne laisse subsister que les tri-chaînes de l'énoncé.

□

Exercice 3.23. Soit V la représentation géométrique d'un groupe de Coxeter W. On suppose que V est définie sur $\mathbb{Z}$, c'est-à-dire que V possède un réseau invariant par W. Montrer alors que tous les $m_{s,s'}$ appartiennent à $\{2,3,4,6,\infty\}$ (on calculera la trace de ss' sur V). On suppose maintenant que tous les $m_{s,s'}$ sont dans $\{2,3,4,6\}$ et qu'on peut trouver des réels $\lambda_s \neq 0$ tels que $\lambda_s/\lambda_{s'}$ soit égal à 1 (resp. $\sqrt{2}$ ou $1/\sqrt{2}$, $\sqrt{3}$ ou $1/\sqrt{3}$) si $m_{s,s'} = 3$ (resp. 4, 6). Montrer alors que le réseau engendré par les $\lambda_s e_s$ est invariant par W. En déduire que si le graphe de Coxeter est un arbre et que tous les $m_{s,s'}$ sont dans $\{2,3,4,6\}$, alors il existe un réseau invariant par W (il en résulte que les 8 premiers types de groupes du théorème précédent sont définis sur $\mathbb{Z}$; les autres ne sont pas rationnels).

4. Compléments sur les groupes de réflexion complexes

Maintenant à nouveau V est un espace vectoriel sur un sous-corps k de $\mathbb{C}$.

Proposition 4.1. *Si W est un groupe de réflexions complexes sur V irréductible qui possède un degré $d_i = 2$ alors il est réel. Réciproquement si W est un groupe de réflexion réel irréductible non trivial, alors il possède un unique degré d_i minimal, égal à 2.*

Démonstration. Un invariant homogène de degré 2 est une forme bilinéaire symétrique W-invariante non nulle sur V^*.

Si W est réel irréductible une telle forme existe et est unique à scalaire près par 3.6 et 3.17(ii), d'où la réciproque.

Si V^* admet une forme bilinéaire invariante non nulle alors elle définit un isomorphisme entre les représentations V et V^* de W, donc le caractère de réflexion χ de W est réel. Le théorème de Frobenius-Schur dit que si de plus la forme est symétrique alors la représentation est réelle. En effet soit B une telle forme. En utilisant l'analogue en complexe de 3.6, on peut par ailleurs choisir un produit scalaire $\langle\,,\,\rangle$ invariant par W. On définit ϕ par $B(x,y) = \overline{\langle\,\phi(x),y\,\rangle}\forall y$. Alors ϕ est une bijection, et $\overline{\langle\,\phi(\lambda x),y\,\rangle} = B(\lambda x,y) = \lambda B(x,y) = \lambda\overline{\langle\,\phi(x),y\,\rangle} = \overline{\langle\,\overline{\lambda}\phi(x),y\,\rangle}$ montre que ϕ est anti-linéaire ; puis $\overline{\langle\,\phi(wx),y\,\rangle} = B(wx,y) = B(x,w^{-1}y) = \overline{\langle\,\phi(x),w^{-1}y\,\rangle} = \overline{\langle\,w\phi(x),y\,\rangle}$ montre que ϕ commute à W. Enfin $\langle\,\phi^2(x),y\,\rangle = \overline{B(\phi(x),y)} = \overline{B(y,\phi(x))} = \langle\,\phi(x),\phi(y)\,\rangle$, d'où $\langle\,\phi^2(x),y\,\rangle = \langle\,x,\phi^2(y)\,\rangle$, ce qui est la définition d'un opérateur Hermitien. Tout opérateur Hermitien ρ est diagonalisable (on vérifie que l'orthogonal d'un vecteur propre de ρ est stable par ρ) et ses valeurs propres sont réelles (car si $\rho(x) = \lambda x$ alors $\overline{\lambda}\langle\,x,x\,\rangle = \langle\,x,\lambda x\,\rangle = \langle\,x,\rho(x)\,\rangle =$

$\langle \rho(x), x \rangle = \langle \lambda(x), x \rangle = \lambda \langle x, x \rangle$). Comme $\langle \phi^2(x), x \rangle = \langle \phi(x), \phi(x) \rangle$ on voit que les valeurs propres $\{\lambda_i\}_i$ de ϕ^2 sont positives. Soit P un polynôme à coefficients réels tel que $P(\lambda_i) = \sqrt{\lambda_i}$ pour tout i. Alors $\sigma = P(\phi^2)$ est toujours Hermitien (car P est à coefficients réels) et commute toujours à W, et commute à ϕ. Enfin $\sigma^2 = \phi$ (ce sont deux opérateurs diagonaux dans la même base avec mêmes valeurs propres). Finalement $\varphi = \sigma^{-1}\phi$ est une involution anti-linéaire commutant à W. Soient V_+ et V_- les espaces propres de φ pour 1 et -1. Alors l'anti-linéarité de φ montre que $iV_+ = V_-$. Et le fait que φ commute à W montre que V_+ et V_- sont W-stables. Donc (V_+, iV_+) est une structure réelle W-stable sur V cqfd. □

Remarque 4.2. En général, si W est un groupe de réflexion complexe et χ son caractère de réflexion, alors on peut démontrer que la représentation V de W est réalisable sur $\mathbb{Q}(\chi)$. (*c.f.* Benson 7.1.1).

On a un critère commode pour savoir le statut d'une représentation par rapport aux réels :

Proposition 4.3. *(Indicateur de Frobenius-Schur) Soit ρ une représentation irréductible complexe du groupe fini W. Soit χ son caractère. Alors $|W|^{-1}\sum_{w\in W}\chi(w^2)$ vaut respectivement $1, -1, 0$ si respectivement ρ est réelle, χ est réelle mais ρ ne l'est pas, χ n'est pas réel.*

Démonstration. Soit V l'espace de la représentation ρ ; on a[6] $V \otimes V = S^2V \oplus \Lambda^2 V$. En regardant les valeurs propres de $\rho(w)^2$, on trouve que $\chi(w^2) = \mathrm{Trace}(w \mid S^2V) - \mathrm{Trace}(w \mid \Lambda^2 V)$. L'indicateur de Frobenius-Schur vaut donc $\langle S^2V, \mathrm{Id} \rangle_W - \langle \Lambda^2 V, \mathrm{Id} \rangle_W$. Comme $\langle \chi, \overline{\chi} \rangle_W = \langle \chi^2, \mathrm{Id} \rangle_W$ on voit que si χ n'est pas réel alors Id n'intervient pas dans $V \otimes V$ et l'indicateur vaut 0 ; sinon Id intervient une fois, dans S^2V ou dans $\Lambda^2 V$, et l'indicateur vaut ± 1. Il vaut 1 si et seulement si il existe un vecteur non nul de S^2V stable par W, *i.e.* il existe une forme bilinéaire symétrique invariante par W ; on a vu que cela équivaut à ce que ρ soit réelle. □

Exercice 4.4. Soit $Q = \langle I, J \mid I^2 = J^2, I^4 = 1, J = IJI \rangle$ le "groupe des quaternions". Montrer que $I \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J \mapsto \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$ est une représentation irréductible ρ de Q sur $\mathbb{C}$ qui n'est pas définie sur $\mathbb{R}$, mais telle que 2ρ soit définie sur $\mathbb{R}$ (on utilisera la représentation de $\mathbb{C}$ dans $\mathrm{End}(\mathbb{R}^2)$).

La classification des groupes de réflexion complexes de rang 2. Nous ne donnons qu'un bref aperçu de cette classification. Il est facile de déterminer les groupes imprimitifs, donc nous expliquons comment trouver les groupes primitifs. On commence par utiliser une méthode générale pour passer des sous-groupes finis de $\mathrm{GL}_2(\mathbb{C})$ à ceux de $\mathrm{SL}_2(\mathbb{C})$: si G est un tel sous-groupe fini, on définit n, d, H et K par : $\mu_{nd} = G\,\mathrm{SL}_2(\mathbb{C}) \cap \mathbb{C}$, $\mu_d = G \cap \mathbb{C}$, $H = G\mathbb{C} \cap \mathrm{SL}_2$ et $K = G \cap \mathrm{SL}_2$ où $\mathbb{C}$ représente les scalaires de GL_2 et μ_a représente les racines a-ièmes de l'unité. On associe ainsi à G un sous-groupe H de $\mathrm{SL}_2(\mathbb{C})$ et un sous-groupe normal K de H tel que le quotient soit isomorphe à μ_n, et un entier d. Réciproquement, toutes les fois qu'on se donne un tel triplet H, K, d on construit un groupe $G \subset \mathrm{GL}_2(\mathbb{C})$ comme image des couples $(x, y) \in \mu_{nd} \times H$ tels que x et y ont même image dans $\mu_n \simeq H/K$ par l'application produit $(x, y) \mapsto xy$.

[6] rappel : algèbre extérieure

Pour trouver les sous-groupes finis primitifs de $SL_2(\mathbb{C})$ on utilise d'abord qu'un tel sous-groupe est conjugué à un sous-groupe de $\mathrm{SU}_2(\mathbb{C})$ (puisqu'il admet un produit scalaire invariant). Ensuite on utilise le revêtement $\mathrm{SU}_2(\mathbb{C}) \to \mathrm{SO}_3(\mathbb{R})$ qui est d'ordre 2 (qu'on obtient par exemple en identifiant les quaternions de norme 1 à la sphère dans $\mathbb{R}^3$). On trouve les sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$ en classifiant les polyèdres réguliers : il y a un groupe associé au tétraèdre (le groupe $\mathfrak{S}_4$), un associé au cube et octaèdre (le même car ces polyèdres sont duaux) et un associé au dodécaèdre et à l'icosaèdre. En relevant on obtient 3 sous-groupes finis primitifs de $\mathrm{SL}_2(\mathbb{C})$, qui sont appelés groupe binaire tétraédral, groupe binaire octaédral et groupe binaire icosaédral. Pour trouver lesquels donnent des groupes de réflexions complexes dans $\mathrm{GL}_2(\mathbb{C})$, on calcule les invariants de ces groupes et on trouve par quels scalaires il faut les étendre pour trouver un groupe de réflexion complexes. Le groupe binaire tétraédral donne lieu à G_4–G_7, le groupe binaire octaédral donne lieu à G_8–G_{15}, et le groupe binaire icosaédral à G_{16}–G_{22}.

Le théorème de Chevalley. Soit comme précédemment un sous-groupe fini $W \in \mathrm{GL}(V)$, et soit S l'algèbre symétrique de V.

Définition 4.5. *Soit I l'idéal de S engendré par les éléments de S^W de degré strictement positif. Nous appelons algèbre des co-invariants et notons S_W l'algèbre S/I.*

Notons que comme I est gradué, S_W hérite d'une graduation. Notons aussi que par le théorème de Mashke, I admet un supplémentaire W-stable H dans S, qui est isomorphe comme W-module à S_W.

Avant de montrer le théorème de Chevalley, nous montrons maintenant

Théorème 4.6. *Si W est engendré par $\mathrm{Ref}(W)$, alors l'application naturelle $H \otimes S^W \to S$ donnée par la multiplication définit un isomorphisme gradué W-invariant : $S \simeq S_W \otimes_k S^W$. De plus la représentation de W sur S_W est une version graduée de la représentation régulière de W.*

Démonstration. Montrons d'abord pourquoi le fait que $H \otimes_k S^W \to S$ soit un isomorphisme implique que la représentation de W sur S_W est la représentation régulière. L'isomorphisme dit que toute k-base de H est une S^W-base de S, donc une base de $\mathrm{Frac}(S)$ sur $\mathrm{Frac}(S^W)$. Or $\mathrm{Frac}(S^W) = \mathrm{Frac}(S)^W$ (si $x/y \in \mathrm{Frac}(S)^W$ on obtient un élément de $\mathrm{Frac}(S^W)$ en multipliant numérateur et dénominateur par les W-transformés de y). Mais $\mathrm{Frac}(S)/\mathrm{Frac}(S)^W$ est une extension Galoisienne de groupe W (car $W \to \mathrm{Aut}(\mathrm{Frac}(S))$ est injective). Par le théorème de la base normale, l'extension $S_W \otimes_k \mathrm{Frac}(S^W)$ est donc la représentation régulière, donc S_W est déjà la représentation régulière (car par exemple elle a même caractère).

Pour démontrer que $S \simeq S_W \otimes_k S^W$, nous allons montrer que toute base homogène $\{z_i\}_i$ de H est une S^W-base de S.

Montrons d'abord que z_i engendre S comme S^W-module, *i.e.* que $S = S^W H$. Sinon, soit f un élément homogène de degré minimum de S qui n'est pas dans $S^W H$. Choisissons une écriture homogène de $f \in I + H$ de sorte que $f = g + \sum_i \lambda_i z_i$ où $\lambda_i \in k$ et $g \in I$ et z_i sont de même degré que f. Écrivons $g = \sum_j x_j y_j$ où $x_j \in S^W$ sont de degré strictement positif et $y_j \in S$. Alors $\deg y_j < \deg f$, d'où $y_j \in S^W H$, d'où $g \in S^W H$, une contradiction.

Nous allons maintenant montrer que les z_i sont indépendants sur S^W. Nous introduisons d'abord un opérateur S^W-linéaire Δ_s sur S, attaché à une réflexion

s qui baisse de 1 le degré des éléments. Si $r, \check{r}$ sont une racine et une coracine associées à s, on a $sv - v = -\check{r}(v)r$ pour $v \in V$, et comme V engendre S on en déduit que s opère trivialement sur S/Sr ; donc pour tout $x \in S$, il existe $\Delta_s(x)$ tel que $sx - x = \Delta_s(x)r$. On vérifie en multipliant par r la formule $\Delta_s(xy) = x\Delta_s(y) + y\Delta_s(x) + r\Delta_s(x)\Delta_s(y)$. Comme on a $\Delta_s(x) = 0$ si $x \in S^W$, on en déduit que Δ_s est S^W-linéaire. On a le

Lemme 4.7. *Si $x \in S_i$ pour $i > 0$ et si $\forall s \in \mathrm{Ref}(W), \Delta_s(x) \in I$, alors $x \in I$.*

Démonstration. En effet, $\Delta_s(x) \in I \Rightarrow x \equiv sx \pmod I$, d'où, puisque W est engendré par ses réflexions, $x \equiv wx \pmod I$ pour tout $w \in W$, d'où enfin $x \equiv p_W(x) \pmod I$ où p_W est le projecteur $p_W : S \to S^W$ donné par $x \mapsto |W|^{-1} \sum_{w \in W} w(x)$. Mais comme x est homogène de degré non nul on a $p_W(x) \in I$, d'où $x \in I$. □

Pour voir que les z_i sont S^W-linéairement indépendants, nous allons démontrer par récurrence sur m que tout ensemble de m éléments de S d'images dans S_W linéairement indépendantes sont S^W-linéairement indépendants. Supposons la propriété pour $m-1$ et soit $x_1z_1 + \ldots + x_mz_m = 0$ où $x_i \in S^W$ une relation de dépendance entre m tels éléments. On peut supposer z_1 de degré j minimal parmi les z_i. Il existe une suite $s_1, \ldots, s_j$ telle que $\Delta_{s_1} \ldots \Delta_{s_j} z_1 \neq 0$ (sinon $\Delta_{s_1} \ldots \Delta_{s_j} z_1 = 0 \in I$ et par récurrence décroissante sur i par 4.7 on a $\Delta_{s_i} \ldots \Delta_{s_j} z_1 \in I$; en particulier $z_1 \in I$, une contradiction). Comme les Δ_s sont S^W-linéaires, on a $x_1\Delta_{s_1} \ldots \Delta_{s_j} z_1 + \ldots + x_m\Delta_{s_1} \ldots \Delta_{s_j} z_m = 0$. En posant $y_i = -p_W(\frac{\Delta_{s_1} \ldots \Delta_{s_j} z_i}{\Delta_{s_1} \ldots \Delta_{s_j} z_1}) \in S^W$, on a $x_1 = x_2y_2 + \ldots + x_my_m$, d'où $x_2(z_2 + z_1y_2) + \ldots + x_m(z_m + z_1y_m) = 0$, une contradiction car c'est une relation de dépendance linéaire entre $m-1$ éléments $z_i + z_1y_i$ (homogènes car $\deg z_1y_i = \deg z_i$) d'images linéairement indépendantes dans S_W.

□

En vue de 4.6 l'implication promise (ii)⇒(iii) dans 2.7 est une conséquence immédiate de la proposition suivante :

Proposition 4.8. *(Chevalley) Soit S une k-algèbre de polynômes, et soit R une sous-algèbre graduée (i.e., engendrée par ses éléments homogènes) telle que le R-module S admette une base finie formée d'éléments homogènes. Alors R est une k-algèbre de polynômes.*

Démonstration. Commençons par remarquer qu'on est sous les hypothèses de 2.3, donc R est Noetherien. L'idéal R^+ de R engendré par les éléments homogènes de degré positif est donc engendré par un nombre fini d'éléments, qu'on peut supposer homogènes. Soit $\alpha_1, \ldots, \alpha_s$ un ensemble de générateurs homogènes en nombre minimal. Nous allons prouver que $R = k[\alpha_1, \ldots, \alpha_s]$.

Il est clair que les α_i engendrent R comme algèbre : en procédant par récurrence sur le degré, si $x = \sum_i r_i\alpha_i$ une écriture homogène d'un élément homogène de R^+, alors les r_i sont dans R et de degré inférieur à x, donc par récurrence ils sont engendrés par les α_i, d'où le résultat.

Montrons maintenant que les α_i sont algébriquement indépendants. Sinon, soit $H(X_1, \ldots, X_s)$ une relation de dépendance algébrique de degré minimal ; on peut supposer H homogène pour la graduation où l'algèbre de polynômes $k[X_1, \ldots, X_s]$ a été munie du degré $\deg X_i = \deg \alpha_i$. Posons $\beta_i := \frac{\partial H}{\partial X_i}(\alpha_1, \ldots, \alpha_s)$; ce sont encore

des éléments homogènes de R et on a pour tout k :

$$\sum_{i=1}^{s} \beta_i \frac{\partial \alpha_i}{\partial x_k} = \frac{\partial H}{\partial x_k}(\alpha_1, \ldots, \alpha_s) = 0.$$

Soit J l'idéal de R engendré par les β_i, et soit I une partie minimale de $\{1, \ldots, s\}$ telle que J soit engendré par les $\{\beta_i\}_{i \in I}$; soient donc γ_{ij} des éléments de R tels que pour $j \notin I$ on aie $\beta_j = \sum_{i \in I} \gamma_{ji} \beta_i$. En reportant dans l'égalité ci-dessus, on obtient

$$\sum_{i \in I} \beta_i \left(\frac{\partial \alpha_i}{\partial x_k} + \sum_{j \notin I} \gamma_{ji} \frac{\partial \alpha_j}{\partial x_k}\right) = 0 \tag{1}$$

Notons u_{ik} le facteur de β_i dans (1). Nous allons montrer maintenant que $u_{ik} \in R^+S$. Soit $\{z_\lambda\}_{\lambda \in \Lambda}$ une base de S sur R et écrivons les u_{ik} sur cette base : $u_{ik} = \sum_{\lambda \in \Lambda} \epsilon_{ik\lambda} z_\lambda$. À cause de l'indépendance linéaire des z_λ, (1) entraîne que pour tout λ on a $\sum_{i \in I} \beta_i \epsilon_{ik\lambda} = 0$. Si l'un des $\epsilon_{ik\lambda} \notin R^+$, alors, prenant les termes homogènes de degré $\deg \beta_i$ d'une telle relation, on trouve une écriture d'un $\beta_i (i \in I)$ comme combinaison R-linéaire des autres $\beta_{i'} (i' \in I)$, ce qui est absurde, d'où le résultat sur les u_{ik}.

En utilisant que l'on a $\alpha_i = \sum_k \frac{x_k}{\deg \alpha_i} \frac{\partial \alpha_i}{\partial x_k}$, on trouve en remplaçant les u_{ik} par leur valeur que $\sum_k \frac{x_k}{\deg \alpha_i} u_{ik} = \alpha_i + \sum_{j \notin I} \frac{\deg \alpha_j}{\deg \alpha_i} \gamma_{ji} \alpha_j \in R^+S^+$; en d'autres termes on a $\alpha_i + \sum_{j \notin I} \frac{\deg \alpha_j}{\deg \alpha_i} \gamma_{ji} \alpha_j = \sum_k y_k \alpha_k$ où les $y_k \in S$ sont homogènes de degré positif. En prenant la composante homogène de degré $\deg \alpha_i$ de cette égalité, on voit que α_i est combinaison S-linéaire des autres α_j. Mais S étant R-libre, cela implique que α_i est combinaison R-linéaire des autres (on écrit les coefficients dans la base z_λ et on regarde le coefficient d'un z_λ fixé dans l'égalité résultante), une absurdité. □

5. Invariants tordus ; le théorème de Steinberg

Soit χ un caractère irréductible de W. On pose f_χ et appelle *degré fantôme* de χ la multiplicité graduée de χ dans S_W. Si l'on pose $p_\chi = \chi(1)|W|^{-1} \sum_{w \in W} \overline{\chi}(w) w$ alors p_χ est le projecteur sur la partie χ-isotypique dans toute représentation de W (pour le voir on utilise la formule d'orthogonalité des coefficients pour calculer l'image de p_χ dans cette représentation). Par 4.6 on a $P_{S_W} = P_S / P_{S^W}$ et $\chi(1) f_\chi = P_S(p_\chi)/P_{S^W}$ où et $P_S(p_\chi)$ est la trace graduée de p_χ sur S. La formule pour $P_S(w)$ obtenue dans la preuve de 2.5 donne donc :

$$f_\chi = \frac{\prod_i (1 - t^{d_i})}{|W|} \sum_{w \in W} \frac{\overline{\chi(w)}}{\det(1 - wt \mid V)}. \tag{5.1}$$

Le fait que S_W soit une version graduée de la représentation régulière implique que $f_\chi(1) = \chi(1)$. On étend le degré fantôme à tous les caractères par linéarité. Si M est un W-module, alors le degré fantôme de son caractère est aussi le polynôme de Poincaré de $(S_W \otimes M^*)^W$.

Si $f_\chi(t) = \sum_i t^{n_i}$ on pose $N(\chi) = \sum_i n_i$. En particulier si χ est un caractère linéaire, on a $f_\chi = t^{N(\chi)}$ où $N(\chi)$ est l'unique degré de S_W où χ intervient.

Exercice 5.2. (Gutkin) Nous voulons démontrer la formule

$$N(\chi) = \sum_{H \in \mathcal{A}_W} N(\mathrm{Res}^W_{C_W(H)} \chi). \tag{5.3}$$

(i) Montrer que $N(\chi) = \frac{\partial f_\chi}{\partial t} \mid_{t=1}$.

(ii) En utilisant 5.1, montrer que $N(\chi) = \chi(1)|\operatorname{Ref}(W)|/2 + \sum_{s\in\operatorname{Ref}(W)} \frac{\chi(s^{-1})}{\det(s)-1}$.

(iii) Déduire 5.3 de (ii).

(iv) Déduire de 5.3 que $N(\operatorname{Trace} V) = N(\det V) = |\mathcal{A}_W|$ et que $N(\operatorname{Trace} V^*) = N(\det V^*) = |\operatorname{Ref}(W)|$ (où où on a noté $\operatorname{Trace} V$ le caractère de la représentation V).

(v) En considérant le cas de W cyclique d'ordre d, démontrer à partir de (ii) que si $\zeta = e^{2i\pi/d}$ on a $\frac{d-1}{2} + \sum_{i=1}^{d-1} \frac{\zeta^{-ij}}{\zeta^i - 1} = j$ pour $j = 0, \dots, d-1$.

Si χ est un caractère linéaire, par 4.6 il existe un polynôme homogène j_χ de degré $N(\chi)$ tel que les χ-invariants de S soient $j_\chi S^W$.

Pour chaque W-orbite $\mathcal{O}$ d'hyperplans, soit $c_\mathcal{O}$ l'entier tel que pour tout $H \in \mathcal{O}$ on ait $|C_W(H)| = c_\mathcal{O}$. Étant donné le caractère linéaire χ, pour tout $H \in \mathcal{O}$, il existe un entier $0 \leq c_{\chi,\mathcal{O}} \leq c_\mathcal{O} - 1$ tel que pour $s \in C_W(H)$ on ait $\chi(s) = \det(s)^{c_{\chi,\mathcal{O}}}$ (puisque $C_W(H)$ est cyclique — *c.f.* 1.1).

Proposition 5.4. *Pour toute collection d'entiers $0 \leq c_{\chi,\mathcal{O}} \leq c_\mathcal{O} - 1$ il existe un (unique) caractère linéaire tel que si $s \in \operatorname{Ref}(W)$ est tel que $H_s \in \mathcal{O}$ on ait $\chi(s) = \det(s)^{c_{\chi,\mathcal{O}}}$. On a $j_\chi = \prod_\mathcal{O} \prod_{H\in\mathcal{O}} r_H^{c_{\chi,\mathcal{O}}}$.*

Démonstration. Pour démontrer l'existence de χ, il suffit de calculer l'effet de chaque réflexion s sur l'élément j_χ donné ci-dessus. Si $j_\mathcal{O} = \prod_{H\in\mathcal{O}} r_H$, de sorte que $j_\chi = \prod_\mathcal{O} j_\mathcal{O}^{c_{\chi,\mathcal{O}}}$, il suffit de montrer que pour $s \in \operatorname{Ref}(W)$ on a $s(j_\mathcal{O}) = \det(s) j_\mathcal{O}$ si $H_s \in \mathcal{O}$ et $s(j_\mathcal{O}) = j_\mathcal{O}$ sinon. Soit s une réflexion d'hyperplan H. À un scalaire près on a $j_\mathcal{O} = \prod_\mathcal{V} r_\mathcal{V} s(r_\mathcal{V}) \dots s^{|\mathcal{V}|-1}(r_\mathcal{V})$ où $\mathcal{V}$ parcourt les orbites sous s d'hyperplans de $\mathcal{O}$ et où $r_\mathcal{V}$ est une racine pour un des hyperplans de $\mathcal{V}$. Si $\mathcal{V}$ ne contient pas H, alors soit $r_\mathcal{V}$ est stable par s, soit $|\mathcal{V}|$ est égal à l'ordre de s par 1.2 (car alors $r_\mathcal{V}$ n'est pas dans H ni proportionnel à la racine de s, donc ses transformés par s sont tous distincts et deux à deux non proportionnels). Dans les deux cas on a alors que $\prod_\mathcal{V} r_\mathcal{V} s(r_\mathcal{V}) \dots s^{|\mathcal{V}|-1}(r_\mathcal{V})$ est invariant par s. Sinon, si $H \in \mathcal{O}$, il arrive une fois que $\mathcal{V} = \{H\}$ et $\prod_\mathcal{V} r_\mathcal{V} s(r_\mathcal{V}) \dots s^{|\mathcal{V}|-1}(r_\mathcal{V}) = r_H$; l'action de s le multiplie par $\det s$.

Il reste à voir que tout χ-invariant est divisible par j_χ. Soit P un χ-invariant et $H \in \mathcal{O}$. Il suffit de démontrer que P est divisible par $r_H^{c_{\chi,\mathcal{O}}}$. Prenons une base de V de la forme $r_H, x_2, \dots, x_n$ où $x_2, \dots, x_n$ est une base de H. Soit s un générateur de $C_W(H)$. On trouve $s(P) = P(s(r_H), s(x_2), \dots, s(x_n)) = P(\det(s) r_H, x_2, \dots, x_n) = \det(s)^{c_{\chi,\mathcal{O}}} P(r_H, x_2, \dots, x_n)$ la dernière égalité car P est un χ-invariant. Cette dernière égalité a lieu pour chaque monôme de P, ce qui implique que le degré en r_H d'un tel monôme est congru à $c_{\chi,\mathcal{O}}$ modulo l'ordre de s, d'où le résultat puisque $c_{\chi,\mathcal{O}}$ est inférieur à l'ordre de s. □

Le Jacobien. On notera qu'on a $j_{\det V^*} = \prod_\mathcal{O} j_\mathcal{O}^{c_\mathcal{O}-1}$ d'où $N(\det V^*) = \sum_H |C_W(H)| - 1 = |\operatorname{Ref}(W)|$.

Soit $x_1, \dots, x_n$ une base de V de telle sorte que $S = k[x_1, \dots, x_n]$.

Proposition 5.5. *Le Jacobien $J = \frac{\partial(f_1,\dots,f_n)}{\partial(x_1,\dots,x_n)} = \det\{\frac{\partial f_i}{\partial x_j}\}_{i,j}$ est un multiple scalaire non nul de $j_{\det V^*}$.*

Démonstration. Commençons par démontrer que $J \neq 0$. Cela résulte du

Lemme 5.6. *Soit $f_1, \dots, f_n \in k[x_1, \dots, x_n]$. Alors les f_i sont algébriquement indépendants si et seulement si $\frac{\partial(f_1,\dots,f_n)}{\partial(x_1,\dots,x_n)}$ est non nul.*

Démonstration. Soit $P(X_1, \dots, X_n)$ un polynôme non nul tel que $P(f_1, \dots, f_n) = 0$. Alors en dérivant $P(f_1, \dots, f_n)$ par rapport à x_j on trouve $\sum_i \frac{\partial P}{\partial X_i}(f_1, \dots, f_n)\frac{\partial f_i}{\partial x_j} = 0$, *i.e.* le vecteur non nul $\{\frac{\partial P}{\partial X_i}(f_1, \dots, f_n)\}_i$ est vecteur propre de la matrice Jacobienne pour la valeur propre 0.

Réciproquement, si les f_i sont algébriquement indépendants, on peut pour chaque i trouver un polynôme non nul $P_i(X_0, X_1, \dots, X_n)$ qui lie $x_i, f_1, \dots, f_n$. Nous prenons de tels polynômes de degré minimal en X_0. On trouve

$$0 = \frac{\partial P_i}{\partial x_j}(x_i, f_1, \dots, f_n) = \frac{\partial P_i}{\partial X_0}(x_i, f_1, \dots, f_n)\delta_{i,j} + \sum_k \frac{\partial P_i}{\partial X_k}(x_i, f_1, \dots, f_n)\frac{\partial f_k}{\partial x_j},$$

ce qui dit que la matrice $\{\frac{\partial P_i}{\partial X_k}(x_i, f_1, \dots, f_k)\}_{i,k}$ multipliée par la matrice Jacobienne est une matrice diagonale, de déterminant non nul d'après le choix des P_i. □

Il suffit ensuite de voir que J est multiple de $j_{\det V^*}$ et que son degré est $N(\det V^*) = |\operatorname{Ref}(W)|$. Le degré de J est $\sum_i (d_i - 1)$, ce qui est $|\operatorname{Ref}(W)|$ d'après 2.7. Il suffit donc de voir que J est un $\det V^*$-invariant. Soit s une réflexion d'hyperplan H. Le Jacobien ne dépend pas de la base x_i choisie à un scalaire près, donc on peut prendre pour base $r_H, x_2, \dots, x_n$ tels que $x_2, \dots, x_n$ soit une base de H. Alors on a $sf_i(r_H, x_2, \dots, x_n) = f_i(r_H, x_2, \dots, x_n) = f_i(\det(s)r_H, x_2, \dots, x_n)$. On en déduit que les monômes de f_i sont de degré en r_H congru à 0 modulo l'ordre de s, donc ceux de $\frac{\partial f_i}{\partial r_H}$ sont de degré congru à -1 modulo l'ordre de s ce qui implique $s\frac{\partial f_i}{\partial r_H}(r_H, x_2, \dots, x_n) = \frac{\partial f_i}{\partial r_H}(\det(s)r_H, x_2, \dots, x_n) = \frac{1}{\det(s)}\frac{\partial f_i}{\partial r_H}(r_H, x_2, \dots, x_n)$, et d'autre part s stabilise $\frac{\partial f_i}{\partial x_j}(r_H, x_2, \dots, x_n)$, d'où le résultat. □

Notons que du point de vue de la géométrie algébrique, 5.6 dit que l'application quotient $V^* \to V^*/W$ donnée par $(f_1, \dots, f_n)$ est lisse en tous les points de V^* où J ne s'annule pas, *i.e.* hors des hyperplans de V^*.

Exercice 5.7. (Macdonald) Soit R un sous-groupe de W engendré par ses réflexions. Soit J_R le Jacobien de R (qui est élément de S_n où $n = |\operatorname{Ref}(R)|$). Soit V_R le sous-W-module de S_n engendré par J_R. Nous voulons démontrer que V_R est irréductible.

(i) Montrer que le caractère linéaire $\det V^*$ de R apparaît avec multiplicité 1 dans S_n et n'apparaît pas dans S_m pour $m < n$ (on utilisera l'isomorphisme $S \simeq S_R \otimes S^R$).

(ii) Montrer que si $V_R = V_1 \oplus V_2$ est une décomposition en deux sous-W-modules, et $J_R = J_1 + J_2$ la décomposition correspondante, alors J_1 et J_2 sont tous deux $\det V^*$-invariants pour R.

(iii) Déduire de (i) et (ii) que V_R est irréductible.

Pour $W = \mathfrak{S}_n$, on obtient une fois chaque représentation irréductible par le procédé ci-dessus en prenant $R = \mathfrak{S}_{n_1} \times \dots \times \mathfrak{S}_{n_r}$ où $n_1 + \dots + n_r = n$.

Le théorème de Steinberg. Nous allons donner une preuve due à Lehrer du théorème de Steinberg.

Lemme 5.8. *Soit $w \in \mathrm{GL}(V)$ d'ordre fini qui normalise W. Alors on peut choisir $f_1, \dots, f_n$ vecteur propres de w. Si ϵ_i sont les valeurs propres correspondantes, alors les couples (d_i, ϵ_i) ne dépendent que de wW. On a $w \in W$ si et seulement si pour tout i on a $\epsilon_i = 1$.*

Démonstration. Soit f un invariant homogène de degré d et soit $P(X_1, \dots, X_n)$ un polynôme tel que $P(f_1, \dots, f_n) = f$. Alors il résulte de l'indépendance algébrique des f_i que tout monôme de P est de la forme $X_1^{e_1} \dots X_n^{e_n}$ avec $d_1e_1 + \dots + d_ne_n = d$. Montrons par récurrence sur d que nous pouvons choisir les f_i de degré d vecteurs propres de w. Puisque W est normalisé par w, cet élément préserve S_d^W. Par récurrence, il préserve le sous-espace engendré par les monômes en les f_i de degré $< d$. L'élément w étant d'ordre fini nous pouvons choisir un supplémentaire w-stable S'_d de ce sous-espace. Toute base de S'_d est un ensemble d'invariants fondamentaux de degré d. Nous prenons une telle base formée de vecteurs propres de w.

On voit de plus dans la construction ci-dessus que les couples nouveaux (d, ϵ_i) qui apparaissent sont uniquement déterminés, car l'espace S'_d est uniquement déterminé.

Enfin, si $\epsilon_i = 1$ pour tout i, soit $\tilde{W} = \langle W, w \rangle$. Alors les f_i sont des éléments algébriquement indépendants de $S^{\tilde{W}}$, donc $|\tilde{W}| \leq d_1 \dots d_n = |W|$ donc $\tilde{W} = W$. □

Une conséquence de lemme ci-dessus est que si V est irréductible, le centre ZW est formé des racines de l'unité d'ordre $\mathrm{pgcd}(d_1, \dots, d_n)$. En effet, le centre est alors formé des scalaires qui sont dans w. Par le lemme ci-dessus, un scalaire est dans w dès qu'il fixe tous les f_i (car ses ϵ_i sont alors égaux à 1). Or ζ agit sur f_i par ζ^{d_i}, d'où le résultat.

Théorème 5.9. *(Steinberg). Soit $V' \subset V$ un sous-espace vectoriel. Alors $C_W(V')$ est engendré par les réflexions qu'il contient.*

Démonstration. En itérant sur une base de V', on voit qu'il suffit de prouver le théorème quand V' est engendré par un unique vecteur v. En fait il nous sera plus commode de démontrer le théorème pour l'action contragrédiente, *i.e.* pour $v \in V^*$. On notera que s de racine r fixe $v \in V^*$ si et seulement si $v(r) = 0$. Soit $R = C_W(v)$ et soit R' le sous-groupe engendré par $\mathrm{Ref}(R)$. Il faut voir que $R' = R$. Notons que R est un sous-groupe normal de R. Il résulte donc de 5.8 que si $w \in R$, on peut choisir des invariants fondamentaux $g_1, \dots, g_n$ pour R' tels qu'il existe ϵ_i tels que $w(g_i) = \epsilon_i g_i$. Et par 5.8, il suffit de montrer que $\epsilon_i = 1$ pour montrer que $w \in R'$. Soient P_i des polynômes tels que $f_i = P_i(g_1, \dots, g_n)$. Par la règle de différentiation des applications composées on a l'égalité de polynômes en $x_1, \dots, x_n$: $\frac{\partial(f_1,\dots,f_n)}{\partial(x_1,\dots,x_n)} = \frac{\partial(P_1,\dots,P_n)}{\partial(g_1,\dots,g_n)} \frac{\partial(g_1,\dots,g_n)}{\partial(x_1,\dots,x_n)}$; par 5.5 appliqué à R' on a $\frac{\partial(g_1,\dots,g_n)}{\partial(x_1,\dots,x_n)} = \prod_{\{H|v(r_H)=0\}} r_H^{|C_{R'}(H)|-1}$; vu que $C_{R'}(H) = C_W(H)$ si $v(r_H) = 0$, on en déduit que $\frac{\partial(P_1,\dots,P_n)}{\partial(g_1,\dots,g_n)} = \prod_{\{H|v(r_H)\neq 0\}} r_H^{|C_W(H)|-1}$; en particulier $v(\frac{\partial(P_1,\dots,P_n)}{\partial(g_1,\dots,g_n)}) \neq 0$. Maintenant notons que si $g_1^{e_1} \dots g_n^{e_n}$ est un monôme de P_i, puisque f_i est w-invariant on a $\epsilon_1^{e_1} \dots \epsilon_n^{e_n} = 1$. On en déduit que $w(\frac{\partial P_i}{\partial g_j}) = \epsilon_j^{-1} \frac{\partial P_i}{\partial g_j}$. Or pour tout polynôme $Q \in k[x_1, \dots, x_n]$ on a $v(w(Q)) = ({}^t w^{-1} v)(Q) = v(Q)$. En particulier $v(w(\frac{\partial P_i}{\partial g_j})) = v(\frac{\partial P_i}{\partial g_j})$ donc si $\epsilon_j \neq 1$ on a pour tout i que $v(\frac{\partial P_i}{\partial g_j}) = 0$. Ceci contredit $v(\frac{\partial(P_1,\dots,P_n)}{\partial(g_1,\dots,g_n)}) \neq 0$. □

6. Les formules de Solomon et Pianzola-Weiss

Nous allons décrire les invariants dans $S \otimes \Lambda V$. Pour cela, nous commençons par définir une dérivation sur $S \otimes \Lambda V$ en posant $d(x \otimes 1) = 1 \otimes x$ et $d(1 \otimes x) = 0$ pour $x \in V$ ce qui suffit à définir d avec la propriété définissante des dérivations $d(fg) = fdg + dfg$. Pour lever l'ambiguïté dans l'écriture des éléments de $S \otimes \Lambda V$, nous noterons $x_1, \ldots, x_n$ une base de $S^1 \simeq V$ et nous utiliserons $dx_1, \ldots, dx_n$ comme base de ΛV. La dérivation d envoie $S^i \otimes \Lambda^j V$ sur $S^{i-1} \otimes \Lambda^{j+1} V$; elle commute aux applications linéaires, en particulier elle est W-équivariante, *i.e.* pour $w \in W$ on a $d(w(f)) = w(df)$. Notons aussi que pour $f \in S$ on a la formule

$$df = \sum_i \frac{\partial f}{\partial x_i} dx_i. \tag{6.1}$$

Pour calculer d et démontrer ces propriétés on peut procéder par récurrence sur le nombre de variables intervenant dans f en écrivant $f = x_1 f' + f''(x_2, \ldots, x_n)$.

Proposition 6.2. *(Solomon) On a* $(S \otimes \Lambda V)^W \simeq k[f_1, \ldots, f_n] \otimes \Lambda[df_1, \ldots, df_n]$.

Démonstration. Pour $I = \{i_1, \ldots, i_j\} \subset [1..n]$ posons $\omega_I = df_{i_1} \ldots df_{i_j}$. Comme d commute à l'action de W, les df_i sont W-invariants ; et par 6.1 on voit que les df_i anticommutent (ce qui justifie le fait d'avoir écrit la sous-algèbre qu'ils engendrent comme extérieure dans l'énoncé du théorème), donc ω_I ne dépend que par un signe de l'ordre du produit ; en particulier $\omega_I \omega_{I'} = 0$ si $I \cap I' \neq \emptyset$ et $\omega_I \omega_{I'} = \pm \omega_{I \cup I'}$ sinon. En utilisant 6.1 et les règles de calcul dans l'algèbre extérieure, on voit que $\omega_{[1..n]} = J dx_1 \ldots dx_n$ (notons que cette formule redémontre que J est $\det V^*$-invariant puisque $\omega_{[1..n]}$ est invariant et puisque par définition $dx_1 \ldots dx_n$ est $\det V$-invariant).

On en déduit que les ω_I sont S-linéairement indépendants. En effet, si l'on a une relation de dépendance $\sum_I c_I \omega_I = 0$ avec $c_I \in S$, on peut d'abord supposer que tous les I dans la somme ont même cardinal en se limitant à un degré donné dans l'algèbre extérieure. Si alors $\overline{I}_0$ est le complémentaire d'un I_0 intervenant dans la somme, en multipliant par $\omega_{\overline{I}_0}$ on obtient $c_{I_0} \omega_{[1..n]} = c_{I_0} J dx_1 \ldots dx_n$ et du fait que $J \neq 0$ et que S est intègre on en déduit $c_{I_0} = 0$.

On en déduit qu'en étendant les scalaires à $K = \mathrm{Frac}(S)$, les ω_I deviennent une base de $K \otimes \Lambda V$ (car ils sont K-linéairement indépendants et leur nombre 2^n est la dimension de ΛV). Or $(K \otimes \Lambda V)^W = K^W \otimes \Lambda[df_1, \ldots, df_n]$; en effet, le membre de droite est clairement inclus dans celui de gauche ; et si $f = \sum_I c_I \omega_I \in K \otimes \Lambda V$ où $c_I \in K$, alors si f est W-invariant on trouve $f = |W|^{-1} \sum_{w \in W} w(f) = \sum_I (|W|^{-1} \sum_{w \in W} w(c_I)) \omega_I$ donc f est dans le membre de droite. De plus si $f \in S \otimes \Lambda V$ alors $f \omega_{\overline{I}} \in S \otimes \Lambda V$ ce qui donne $c_I J dx_1 \ldots dx_n \in S \otimes \Lambda V$ d'où $c_I J \in S$. Si f est W-invariant ceci implique $c_I \in S^W$ car $c_I J$ est alors $\det V^*$-invariant et les $\det_V^*$-invariants de S sont JS^W. □

Corollaire 6.3. *(Solomon)*
(i) Soit $\phi \in \mathrm{GL}(V)$ qui normalise W. On a l'identité suivant de polynômes en deux variables :

$$|W|^{-1} \sum_{w \in W} \frac{\det(1 - yw\phi)}{\det(1 - xw\phi)} = \frac{\prod_i (1 - \epsilon_i y x^{d_i - 1})}{\prod_i (1 - \epsilon_i x^{d_i})}$$

où les ϵ_i sont comme en 5.8.
(ii) Le degré fantôme de $\Lambda^i V^*$ est $\sum_{\{I \subset [1..n] \mid |I| = i\}} \prod_{j \in I} x^{d_j - 1}$.

Démonstration. Nous construisons une série de Poincaré en deux variables pour $S \otimes \Lambda V$ en attachant au terme $S^i \otimes \Lambda^j V$ le monôme $x^i(-y)^j$. Nous avons alors un analogue de la formule de Molien dans notre situation : pour $w \in W$ la trace graduée $P_{S\otimes\Lambda V}(w\phi) = P_S(w\phi)P_{\Lambda V}(w\phi)$ et on a vu en 2.5 que $P_S(w\phi) = 1/\det(1 - w\phi x)$; et il est bien connu que $\sum_i (-y)^i \operatorname{Trace}(w\phi \mid \Lambda^i V) = \det(1 - w\phi y)$. Le membre de gauche de la formule de Solomon est donc bien la trace graduée sur $S \otimes \Lambda V$ de ϕ fois le projecteur sur les invariants $|W|^{-1}\sum_{w\in W} w$. Le membre de droite s'obtient en calculant la trace graduée de ϕ sur $k[f_1, \dots, f_n] \otimes \Lambda[df_1, \dots, df_n]$. Comme d commute aux applications linéaires on a $\phi(df_i) = d\phi f_i = \epsilon_i df_i$ et le monôme associé à ω_I est $\prod_{j\in I}(-y\epsilon_i x^{d_j-1})$ et la somme sur I de ces monômes est bien $\prod_i(1 - \epsilon_i y x^{d_i-1})$. On voit aussi au passage que le polynôme de Poincaré de $(S \otimes \Lambda^i V)^W$ est $P_{S^W}(\sum_{\{I\subset[1..n]||I|=i\}} \prod_{j\in I}(-yx^{d^j-1}))\ |_{x=t,y=-1}$ d'où (ii) car $(S\otimes\Lambda^i V)^W = (S^W \otimes S_W \otimes \Lambda^i V)^W = S^W \otimes (S_W \otimes \Lambda^i V)^W$ et nous avons remarqué que le polynôme de Poincaré de $(S_W \otimes \Lambda^i V)^W$ est le degré fantôme de $\Lambda^i V^*$. □

Remarque 6.4. On peut montrer (Steinberg) que si V est irréductible alors $\Lambda^i V^*$ l'est aussi.

Remarque 6.5. En particulier le degré fantôme de V^* est $\sum_i t^{d_i-1}$. On définit les *codegrés* d_i^* de W par le fait que le degré fantôme de V est $\sum_i t^{d_i^*+1}$.

Corollaire 6.6. *(Pianzola-Weiss) Soit ζ une racine de l'unité et notons $V_\zeta(w\phi)$ le ζ-espace propre de $w\phi \in W\phi$. Alors on a l'identité polynomiale :*

$$\sum_{w\in W} T^{\dim(V_\zeta(w\phi))} = \prod_{\{i|\zeta^{d_i}=\epsilon_i\}} (T + d_i - 1) \prod_{\{i|\zeta^{d_i}\neq\epsilon_i\}} d_i$$

Démonstration. Si l'on note $\lambda_1(w\phi), \dots, \lambda_n(w\phi)$ les valeurs propres de $w\phi$, le terme $\frac{\det(1-yw\phi)}{\det(1-xw\phi)} = \prod_i \frac{1-y\lambda_i(w\phi)}{1-x\lambda_i(w\phi)}$ du membre de gauche de 6.3(i) a un pôle d'ordre $\dim V_\zeta(w\phi)$ en $x = \zeta^{-1}$. Nous introduisons par conséquent le changement de variables $y = \zeta^{-1}(1 - T(1 - x\zeta))$, d'où $1 - y\zeta = T(1 - x\zeta)$, ce qui fait disparaître ce pôle. Évaluant le membre de gauche de 6.3(i) en $x = \zeta^{-1}$ on obtient $|W|^{-1}\sum_{w\in W}\prod_{\{i|\lambda_i(w\phi)=\zeta\}} T = |W|^{-1}\sum_{w\in W} T^{\dim V_\zeta(w\phi)}$. Du côté droit, on trouve par dérivation par rapport à x que si $\zeta_i^d = \epsilon_i$ alors la limite de $(1 - \epsilon_i y x^{d_i-1})/(1 - \epsilon_i x^{d_i})$ en $x \mapsto \zeta^{-1}$ est $(T + d_i - 1)/d_i$, sinon la limite est 1. On trouve donc comme limite du membre de droite $\prod_{\{i|\zeta^{d_i}=\epsilon_i\}}(T + d_i - 1)/d_i$, d'où la formule annoncée en utilisant que $|W| = d_1 \dots d_n$. □

Corollaire 6.7. *La dimension maximale d'un ζ-espace propre d'un $w\phi \in W\phi$ est $|\{i \mid \zeta^{d_i} = \epsilon_i\}|$. L'exposant de W est* $\operatorname{ppcm}(d_1, \dots, d_n)$.

Démonstration. La première assertion est une conséquence triviale de 6.6. La deuxième aussi, car on voit que toute valeur propre d'un élément de W est d'ordre un diviseur d'un d_i, donc tout élément de W est d'un ordre qui divise $\operatorname{ppcm}(d_1, \dots, d_n)$. Et réciproquement, pour tout diviseur d d'un des d_i, il existe un élément de W d'ordre multiple de d. □

7. Espaces propres

7.1. **Rappels de géométrie algébrique.** Nous prenons k algébriquement clos (donc $k = \mathbb{C}$) et $V = k^n$. Un sous-variété algébrique affine de V^* est l'ensemble des zéros communs à une famille finie $(p_1, \dots, p_n) \in S$ de polynômes. C'est donc aussi

l'ensemble des zéros communs à l'idéal engendré $I = (p_1, \ldots, p_n)$. Comme S est Noetherien, tout idéal I de S est de type fini donc donne lieu à la variété $V(I)$ de ses zéros. Réciproquement, si $X \subset V^*$, nous notons $I(X)$ l'idéal des polynômes de S qui s'annulent sur X. L'ensemble X est une sous-variété algébrique si $X = V(I(X))$. Dans l'autre sens, nous avons le

Théorème 7.1. *(NulstellenSatz de Hilbert)*

(i) *Une k-algèbre de type fini qui est un corps commutatif est égale à k.*

(ii) *Les idéaux maximaux de S sont les polynômes qui s'annulent en un point.*

(iii) *$I(V(I)) = \sqrt{I}$ où $\sqrt{I}$, appelé la racine de I, est formé de tous les polynômes dont une puissance tombe dans I .*

Démonstration. Nous référons à la littérature et prouvons juste (i)⇒(ii) à titre d'exemple. Les polynômes qui s'annulent en un point sont l'idéal $(x_1 - a_1, \ldots, x_n - a_n)$ où $x_1, \ldots, x_n$ est une base de V et $a_i \in k$; en effet, modulo $x_i - a_i$, tout polynôme est congru à une constante donc le quotient par cet idéal est k et cet idéal est maximal. Réciproquement, si m est un idéal maximal de S, par (i) on a $S/m \simeq k$ et le morphisme quotient restreint à k est un isomorphisme, *i.e.* il existe a_i tels que $x_i - a_i \in m$. Donc $m \supset (x_1 - a_1, \ldots, x_n - a_n)$. □

On a $V(0) = V^*, V(S) = \emptyset, V(\sum_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$ pour toute famille α, et $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$; donc les $V(I)$ vérifient les axiomes des fermés d'une topologie, qui est la *topologie de Zariski*. Les sous-variétés de la variété X correspondent aux idéaux qui contiennent $I(X)$.

Si X est une sous-variété algébrique affine de V^*, le noyau de l'application naturelle de S vers les fonctions polynomiales sur X est $I(X)$. On peut donc identifier $k[X] := S/I(X)$ aux fonctions polynomiales sur X. C'est une k-algèbre de type fini, sans éléments nilpotents (puisque $I(X) = \sqrt{I(X)}$).

Réciproquement toute k-algèbre A de type fini et sans éléments nilpotents définit une variété affine : si $a_1, \ldots, a_n$ sont des générateurs de A, et si $x_1, \ldots, x_n$ est une base de V, alors le noyau de l'application $S \to A$ donnée par $x_i \mapsto a_i$ est un idéal I tel que $A \simeq S/I$. Cette variété n'est pas unique à notre sens (son plongement dans un k^n dépend du choix des a_i) ; mais elle est unique à isomorphisme près : on peut retrouver toute la structure de X (en particulier sa topologie de Zariski) à partir de $k[X]$; les fermés de $A = S/I$ correspondent aux idéaux de S contenant I, qui sont en bijection avec les idéaux de A (et les points de X correspondent aux idéaux maximaux de A). On dit que $X = \mathrm{Spec}(A)$.

Un morphisme de variétés $\mathrm{Spec}\, A \to \mathrm{Spec}\, B$ correspond à un morphisme d'anneaux $B \to A$ (l'image réciproque d'un idéal (resp. idéal premier, idéal maximal) est un idéal (resp. idéal premier, idéal maximal)).

Un sous-ensemble d'un espace topologique est *irréductible* s'il n'est pas l'union de deux fermés propres. La variété X est irréductible si et seulement si $I(X)$ est un idéal premier (en effet si $f_1 f_2 \in I(X)$, alors $X \subset V(f_1) \cup V(f_2)$ donc si X est irréductible on a $(f_1) \subset I(X)$ ou $(f_2) \subset I(X)$. Réciproquement si $I(X) = I_1 \cap I_2$ est premier, on ne peut pas trouver $i_1 \in I_1 - I(X)$ et $i_2 \in I_2 - I(X)$ car $i_1 i_2 \in I_1 \cap I_2$ contredirait la primalité de $I(X)$, donc on a $I(X) = I_1$ ou $I(X) = I_2$). Donc $k[X]$ est intègre si et seulement si X est irréductible.

Pour démontrer les résultats de Springer et Lehrer sur les espaces propres des éléments de W nous utiliserons que $(f_1, \ldots, f_n)$ réalise le quotient ensembliste V^*/W.

Lemme 7.2. *Deux sous-variétés irréductibles $X, X' \subset V^*$ sont dans la même W-orbite si et seulement si pour tout i on a $f_i(X) = f_i(X')$.*

Démonstration. Les sous-variétés irréductibles de V^* sont en bijection avec les idéaux premiers de S. L'application définie par $(f_1, \dots, f_n)$ envoie V^* sur $\mathrm{Spec}(S^W)$. L'énoncé revient a voir que si p et p' sont deux idéaux premiers de S qui ont même intersection avec S^W, alors il existe $w \in W$ tel que $p' = wp$. Supposons que $p' \neq wp$ pour tout $w \in W$. Alors on ne peut avoir $p' \in \bigcup_w wp$ (car un espace vectoriel sur k ne peut être une union finie de sous-espaces propres), donc il existe $x \in p'$ tel que pour tout $w \in W$ on a $wx \notin p$. Alors, comme p est premier, on a $\prod_{w\in W} wx \notin p$ mais cet élément est dans S^W, ce qui contredit $p \cap S^W = p' \cap S^W$. □

Dimension. Comme S est Noetherien, toute suite décroissante de fermés stationne.

Lemme 7.3. *Une variété X est union de ses sous-variétés irréductibles maximales, qui sont dites composantes irréductibles de X et sont en nombre fini ; et toute décomposition en fermés irréductibles sans inclusions mutuelles est la décomposition en composantes irréductibles.*

Démonstration. Montrons par l'absurde que X est union finie de sous-variétés irréductibles. Sinon, l'ensemble des fermés de X qui ne sont pas union finie de sous-variétés irréductibles est non vide, et toute suite décroissante de fermés stationnant, cet ensemble a au moins un élément minimal Y. Cet Y n'est pas irréductible, donc $Y = Y_1 \cup Y_2$ où Y_1 et Y_2 sont fermés ; par minimalité ils sont union finie de fermés irréductibles, donc Y aussi, une contradiction.

Donc $X = \bigcup_i Y_i$ une union de fermés irréductibles. Quitte à retirer certains éléments de cette union, on peut supposer qu'il n'y a pas d'inclusions mutuelles. Soit Y un fermé irréductible maximal de X. Alors $Y = \bigcup_i (Y \cap Y_i)$ montre que Y doit être un des Y_i. On en déduit les assertions de l'énoncé. □

Un ouvert non vide d'un espace irréductible est irréductible et dense. On définit la *dimension* d'une variété comme la longueur maximale d'une chaîne décroissante de fermés irréductibles.

Proposition 7.4. *La dimension d'une variété irréductible X est le degré de transcendance de* $\mathrm{Frac}(k[X])$.

Démonstration. Soit $p \subset k[X]$ correspondant à la sous-variété irréductible Y, si bien que $k[Y] = k[X]/p$; choisissons $x_1, \dots x_k$ des générateurs de $k[X]$ et soient $y_1, \dots, y_k$ leurs images dans $k[Y]$. Si e est le degré de transcendance de $k[Y]$, on peut supposer que $y_1, \dots, y_e$ sont algébriquement indépendants ; alors $x_1, \dots, x_e$ le sont aussi. Montrons que e est strictement plus petit que le degré de transcendance de $k[X]$. Sinon, tout élément de $k[X]$ est algébrique sur $x_1, \dots, x_e$, en particulier étant donné $f \in p - 0$ on peut trouver un polynôme $P(X_0, X_1, \dots, X_e)$ tel que $P(f, x_1, \dots, x_e) = 0$; et on peut supposer P non divisible par X_0 ; alors l'image de $P(f, x_1, \dots, x_e)$ dans $k[Y]$ lie algébriquement les y_i, une contradiction.

On en déduit que le degré de transcendance de $k[X]$ est au moins $\dim X$. Mais, réciproquement, si $x_1, \dots, x_e$ sont algébriquement indépendants alors les idéaux $(x_1, \dots, x_i)$ sont premiers (on vérifie que le quotient est toujours intègre). □

On déduit de cette proposition que toutes les chaînes croissantes maximales de fermés irréductibles sont de même longueur. Donc, si pour $Y \subset X$ fermé irréductible

on définit la codimension de Y comme la longueur d'un chaîne croissante maximale de fermés irréductibles partant de Y, on a $\operatorname{codim} Y + \dim Y = \dim X$.

Théorème 7.5. *(Springer-Lehrer) Soit ζ une racine de l'unité et soit $\phi \in \mathrm{GL}(V)$ qui normalise W. Posons $A = \{i \mid \zeta^{d_i}\epsilon_i = 1\}$.*
(i) Les $V_\zeta^*(w\phi)$ maximaux sont de dimension $|A|$ et sont tous W-conjugués.
(ii) Si U est un $V_\zeta^*(w\phi)$ maximal, alors $N_W(U)/C_W(U)$ est un groupe de réflexion complexe dans son action sur U, avec comme degrés les $\{d_i \mid i \in A\}$.
(iii) Dans la situation de (ii), les hyperplans de $N_W(U)/C_W(U)$ sont les traces des hyperplans de W sur U.

Démonstration. Si $H_i = V(f_i)$ (*i.e.* l'hypersurface des zéros de f_i), on déduit de 7.2 que $\bigcup_{w\in W} V_\zeta^*(w\phi) = \bigcap_{i\notin A} H_i$. En effet v appartient à quelque $V_\zeta^*(w\phi)$ si et seulement si ζv et $\phi(v)$ sont dans la même W-orbite, *i.e.* si pour tout i on a $\zeta^{d_i} f_i(v) = f_i(\zeta v) = f_i(\phi v) = \epsilon_i^{-1} f(v)$, ce qui équivaut à ce que pour tout $i \notin A$ on ait $f_i(v) = 0$. On a aussi que $0 = \bigcap_i H_i$ car cette intersection est formée des $v \in V$ dans la même orbite que 0.

Posons $a = |A|$. Les $V_\zeta^*(w\phi)$ maximaux sont les composantes irréductibles de $\bigcap_{i\notin A} H_i$ (car ce sont des variétés irréductibles sans inclusions mutuelles dont cette intersection est l'union). Le HauptIdealSatz de Krull affirme que si X est une variété algébrique et $f \in S, f \neq 0$ alors la codimension d'une composante irréductible de $X \cap V(f)$ dans X est au plus 1. Par récurrence sur $n - a$, on en déduit que les composantes irréductibles de l'intersection de $n-a$ hypersurfaces sont de dimension $\geq a$; donc les $V_\zeta^*(w\phi)$ sont de dimension $\geq a$; mais par 6.7 ils sont de dimension $\leq a$. Montrons que les restrictions des $\{f_i \mid i \in A\}$ à U sont algébriquement indépendantes ; soit $\Psi : U \to k^a$ le morphisme défini par $v \mapsto \{f_i(v) \mid i \in A\}$. On a $\Psi^{-1}(0) = 0$. Il y a plusieurs façons de voir que ceci implique l'indépendance algébrique des f_i : pour une preuve directe voir l'exercice 5 §5 Ch.V Bourbaki groupes et algèbres de Lie ; sinon, cette indépendance équivaut à l'injectivité du morphisme d'algèbres correspondant à Ψ (morphisme de $k[x_1, \ldots, x_a]$ dans lui-même défini par les f_i). Or on voit qu'un morphisme de variétés correspond à une application injective d'algèbres si et seulement si son image est dense. On peut alors utiliser un résultat général de géométrie algébrique qui dit qu'une application $X \to Y$ dont l'image est dense a des fibres de dimension au moins $\dim X - \dim Y$. Donc le fait qu'une fibre soit triviale implique que la dimension de l'adhérence de l'image de Ψ est a, donc cette adhérence doit être tout k^a et Ψ est bien d'image dense.

On voit aussi que les $V_\zeta^*(w\phi)$ ont même image par tous les f_i (pour $i \in A$ leur image est un fermé de dimension a de k^a donc égale à k^a). Par 7.2 ils sont donc W-conjugués.

Comme on sait que pour l'action de $N_W(U)/C_W(U)$ sur U les $\{f_i \mid i \in A\}$ sont algébriquement indépendants, il suffit pour le (ii) de montrer que $|N_W(U)/C_W(U)| = \prod_{i\in A} d_i$. Comme il y a $|W/N_W(U)|$ espace propres maximaux, et $|C_W(U)|$ éléments qui ont le même, le coefficient de T^a dans le membre de gauche de 6.6 est égal à $|W|/|N_W(U)/C_W(U)|$ donc 6.6 donne (ii).

Montrons maintenant le résultat sur les hyperplans.

Montrons d'abord que tout hyperplan $H \subset U$ d'un élément de $N_W(U)/C_W(U)$ est la trace d'un hyperplan de W : $C_W(H)$ est un sous-groupe de réflexion, dont les points fixes sont $\cap_{s\in Ref(C_W(H))} H_s$. Comme $C_W(H) \neq C_W(U)$ par hypothèse

(puisqu'il existe un élément de $N_W(U)$ qui n'est pas dans $C_W(U)$ qui fixe H), on a donc $\cap_{s\in Ref(C_W(H))}H_s \cap U \neq U$, donc il existe s tel que $H_s \cap U \neq U$, donc $H_s \cap U = H$.

Réciproquement soit s tel que $H_s \cap U = H$ avec $H \neq U$. Il faut montrer qu'il y a un élément de $N_W(U)$ dont les points fixes ont H comme intersection avec U. On remarque que
(i) On peut supposer l'intersection V_0 des hyperplans de réflexion de W triviale : en effet, V_0 est stable par $w\phi$ et le résultat est équivalent au résultat analogue dans V/V_0 pour $(U/U \cap V_0)$.
(ii) $w\phi$ normalise H donc normalise $C_W(H)$.
(iii) U est un ζ-espace propre maximal pour $w\phi C_W(H)$.

Une conséquence de 6.6 est que dès que $U \neq 0$ alors $|A| > 0$. Le (iii) implique alors que $N_W(U)/C_W(U) \neq 1$, en tenant compte de (i) qui implique qu'aucun degré de réflexion de W n'est égal à 1. Si on applique ce résultat en remplaçant W par $C_W(H)$ on obtient $N_{C_W(H)}(U)/C_{C_W(H)}(U) = (N_W(U) \cap C_W(H))/C_W(U) \neq 1$ cqfd.

□

Remarque 7.6. On a $N_W(U) = N_W(C_W(U)w\phi)$. En effet $C_W(U)w\phi$ est l'ensemble de tous les éléments de $W\phi$ qui agissent par le scalaire ζ sur U. Le groupe $N_W(U)$ stabilise clairement cet ensemble. Et dans l'autre sens, si $w\phi \in C_W(U)\phi$ alors $x \in W$ envoie $U = V_\zeta(w\phi)$ sur $V_\zeta(x(w\phi)x^{-1})$; si ce dernier espace propre est encore U, c'est que x normalise U.

Remarque 7.7. On dit que w est ζ-régulier si $V_\zeta(w)$ rencontre le complémentaire des hyperplans de réflexion de W. Alors, si on pose $U = V_\zeta(w)$

(i) $C_W(U) = \{1\}$, par le théorème de Steinberg 5.9. Donc w est le seul élément agissant par ζ sur U.
(ii) U est maximal : si $V_\zeta(w') \supset U$, alors par (i) on a $w' = w$.
(iii) On a $N_W(U)/C_W(U) = C_W(w)$ par (i). Donc $C_W(w)$ est un groupe de réflexions complexes sur U.
(iv) Les éléments ζ-réguliers forment une classe de conjugaison de W.
(v) Si $\zeta^d = 1$ alors $w = 1$ (toujours par 5.9).
(vi) w^i est ζ^i-régulier.

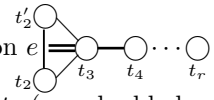
Exercice 7.8. Soit W un groupe de Coxeter fini. Montrer que l'élément de plus grande longueur w_0 est -1-régulier (on utilisera 3.12).

Exercice 7.9. Montrer que dans $W = \mathfrak{S}_n$ (vu comme groupe de Coxeter engendré par les $(i, i+1)$, avec la représentation de réflexion correspondante), les n-cycles sont $e^{2i\pi/n}$-réguliers (on étudiera les valeurs propres d'un élément arbitraire de W).

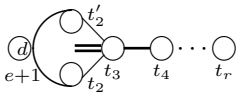
Si $c = (1, \ldots, n)$ est un n-cycle, déterminer pour tout i quel est le groupe de réflexions complexes $C_W(c^i)$.

8. Une table des groupes de réflexion complexes

La table suivante décrit par des graphes analogues aux graphes de Coxeter des présentations des autres groupes de réflexions complexes. Chaque réflexion est représentée par un petit cercle, vide si elle est d'ordre 2, et contenant l'ordre de la réflexion sinon. Par exemple

• $G(e,e,r)$ a pour présentation 

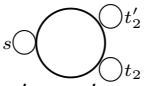
où la double barre signifie relation de tresse double entre $t_2't_2$ et t_3 (une double barre semblable est utilisée pour G_{29} ; quand $e=2$ la barre verticale et la double barre horizontale sautent et on retrouve D_r ; quand $r=2$ on trouve le groupe de Coxeter $I_2(e)$ (ici t_2' est le $s(e)$ de 2.9).

• $G(de,e,r)$ a pour présentation 

, ce qui signifie que s est d'ordre d, que

$$\underbrace{t_2st_2't_2t_2't_2\dots}_{e+1 \text{ termes}} = \underbrace{st_2't_2t_2't_2\dots}_{e+1 \text{ termes}},$$

que s commute à $t_2't_2$ et à t_3, et mêmes relations que $G(e,e,r)$ (ici s est le $t(d)$ de 2.9, et t_2' est le $s(ed)$ de 2.9).

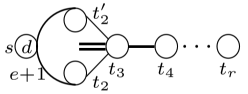
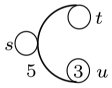
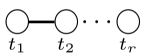
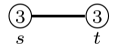
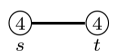
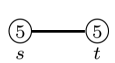
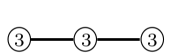
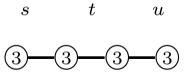
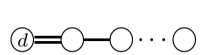
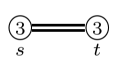
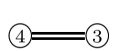
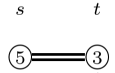
• $G(4,2,2)$ a pour présentation 

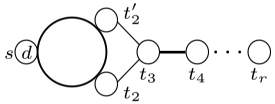
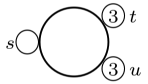
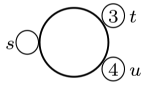
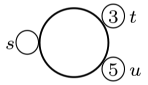
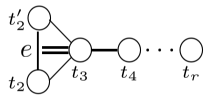
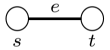
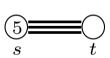
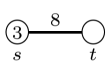
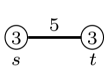
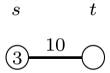
ce qui signifie la relation circulaire de longueur 3 donnée par $st_2t_2' = t_2t_2's = t_2'st_2 = 1$.

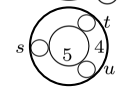
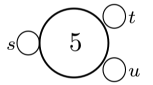
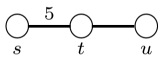
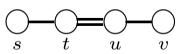
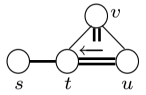
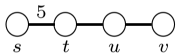
Le 7 et le 6 qui apparaissent dans les triangles de G_{24}, G_{33}, G_{34} signifient aussi des relations circulaires de longueur 6 et 7 (en plus des relations spécifiées par les côtés du triangle), tandis que le double cercle pour G_{12} signifie une relation circulaire de longueur 4.

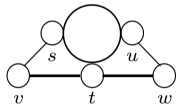
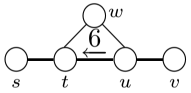
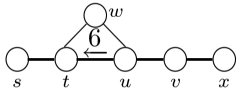
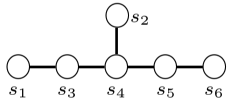
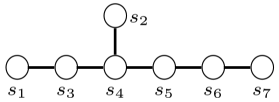
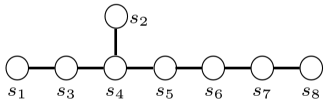
• Le Δ qui apparait dans la présentation de G_{27} signifie $ustusts = tustust$.

• Enfin G_{13} a pour relations $tust = tstu$ et $stust = ustus$, et G_{15} a pour relations $tus = stu$ et $ustut = stutu$.

nom	diagramme	degrés	codegrés	orbites	corps	$\lvert ZG\rvert$	**z**	#cl.	G/ZG
$G(de,e,r)$ $e,d\geq 2$		$ed[1\,..\,r-1]$ rd	$ed[0\,..\,r-1]$		$\mathbb{Q}(\zeta_{de})$	$d(e\wedge r)$	$s^{\frac{r}{e\wedge r}}(t_2't_2t_3\dots t_r)^{\frac{e(r-1)}{e\wedge r}}$		
G_{15}		$12,24$	$0,24$	$s6,t12,u8$	$\mathbb{Q}(\zeta_{24})$	12	$ustut=s(tu)^2$	42	$\mathfrak{S}_4$
A_r		$[2\,..\,r+1]$	$[0\,..\,r-1]$	$t:\frac{r(r+1)}{2}$	$\mathbb{Q}$	1	$(t_1\dots t_r)^{r+1}$		
G_4		$4,6$	$0,2$	$s4$	$\mathbb{Q}(\zeta_3)$	2	$(st)^3$	7	$\mathfrak{A}_4$
G_8		$8,12$	$0,4$	$s6$	$\mathbb{Q}(i)$	4	$(st)^3$	16	$\mathfrak{S}_4$
G_{16}		$20,30$	$0,10$	$s12$	$\mathbb{Q}(\zeta_5)$	10	$(st)^3$	45	$\mathfrak{A}_5$
G_{25}		$6,9,12$	$0,3,6$	$s12$	$\mathbb{Q}(\zeta_3)$	3	$(stu)^4$	24	$3^2\rtimes SL_2(3)$
G_{32}		$12,18,24,30$	$0,6,12,18$	$s40$	$\mathbb{Q}(\zeta_3)$	6	$(stuv)^5$	102	$PSp_4(3)$
$G(d,1,r)$ $d\geq 2$		$d[1\,..\,r]$	$d[0\,..\,r-1]$	$s:r$ $t:\frac{dr(r-1)}{2}$	$\mathbb{Q}(\zeta_d)$	d	$(st_2t_3\dots t_r)^r$		
G_5		$6,12$	$0,6$	$s4,t4$	$\mathbb{Q}(\zeta_3)$	6	$(st)^2$	21	
G_{10}		$12,24$	$0,12$	$s6,t8$	$\mathbb{Q}(\zeta_{12})$	12	$(st)^2$	48	$\mathfrak{S}_4$
G_{18}		$30,60$	$0,30$	$s12,t20$	$\mathbb{Q}(\zeta_{15})$	30	$(st)^2$	135	$\mathfrak{A}_5$
G_{26}		$6,12,18$	$0,6,12$	$s9,t12$	$\mathbb{Q}(\zeta_3)$	6	$(stu)^3$	48	$3^2\rtimes SL_2(3)$

nom	diagramme	degrés	codegrés	orbites	corps	$\lvert ZG\rvert$	$\mathbf{z}$	#cl.	G/ZG
$G(2d,2,r)$ $d\geq 2$		$2d[1\,..\,r-1]$ rd	$2d[0\,..\,r-1]$	s:r,t:$r(r-1)d$ except r=2: s:2,t_2:2,t_2':2	$\mathbb{Q}(\zeta_{2d})$	$d(2\wedge r)$	$s^{\frac{r}{2\wedge r}}(t_2't_2t_3\dots t_r)^{\frac{2r-2}{2\wedge r}}$		
G_7		$12,12$	$0,12$	$s6,t4,u4$	$\mathbb{Q}(\zeta_{12})$	12	stu	42	$\mathfrak{A}_4$
G_{11}		$24,24$	$0,24$	$s12,t8,u6$	$\mathbb{Q}(\zeta_{24})$	24	stu	96	$\mathfrak{S}_4$
G_{19}		$60,60$	$0,60$	$s30,t20,u12$	$\mathbb{Q}(\zeta_{60})$	60	stu	270	$\mathfrak{A}_5$
$G(e,e,r)$ $e\geq 2, r>2$		$e[1\,..\,r-1]$ r	$e[0\,..\,r-2]$ $(r-1)e-r$	$t_2:\frac{er(r-1)}{2}$	$\mathbb{Q}(\zeta_e)$	$e\wedge r$	$(t_2't_2t_3\dots t_r)^{\frac{e(r-1)}{e\wedge r}}$		
$G(e,e,2)=I_2(e)$ $e\geq 3$		$2,e$	$0,e-2$	e odd s:e else s:$e/2$,t:$e/2$	$\mathbb{Q}(\zeta_e+\zeta_e^{-1})$	$e\wedge 2$	$(st)^{e/(e\wedge 2)}$		
G_6		$4,12$	$0,8$	$s4,t6$	$\mathbb{Q}(\zeta_{12})$	4	$(st)^3$	14	$\mathfrak{A}_4$
G_9		$8,24$	$0,16$	$s6,t12$	$\mathbb{Q}(\zeta_8)$	8	$(st)^3$	32	$\mathfrak{S}_4$
G_{17}		$20,60$	$0,40$	$s12,t30$	$\mathbb{Q}(\zeta_{20})$	20	$(st)^3$	90	$\mathfrak{A}_5$
G_{14}		$6,24$	$0,18$	$s8,t12$	$\mathbb{Q}(\zeta_3,\sqrt{-2})$	6	$(st)^4$	24	$\mathfrak{S}_4$
G_{20}		$12,30$	$0,18$	$s20$	$\mathbb{Q}(\zeta_3,\sqrt{5})$	6	$(st)^5$	27	$\mathfrak{A}_5$
G_{21}		$12,60$	$0,48$	$s20,t30$	$\mathbb{Q}(\zeta_{12},\sqrt{5})$	12	$(st)^5$	54	$\mathfrak{A}_5$

nom	diagramme	degrés	codegrés	orbites	corps	$\lvert ZG\rvert$	**z**	#cl.	G/ZG
G_{12}		$6,8$	$0,10$	$s12$	$\mathbb{Q}(\sqrt{-2})$	2	$(stu)^4$	8	$\mathfrak{S}_4$
G_{13}		$8,12$	$0,16$	$s6, tu12$	$\mathbb{Q}(\zeta_8)$	4	$(stu)^3$	16	$\mathfrak{S}_4$
G_{22}		$12,20$	$0,28$	$s30$	$\mathbb{Q}(i,\sqrt{5})$	4	$(stu)^5$	18	$\mathfrak{A}_5$
$G_{23}=H_3$		$2,6,10$	$0,4,8$	$s15$	$\mathbb{Q}(\sqrt{5})$	2	$(stu)^5$	10	$\mathfrak{A}_5$
G_{24}	 $\triangle : u(stu)^2=(stu)^2t$	$4,6,14$	$0,8,10$	$s21$	$\mathbb{Q}(\sqrt{-7})$	2	$(stu)^7$	12	$GL_3(2)$
G_{27}	 $\triangle : (uts)^2t=s(uts)^2$	$6,12,30$	$0,18,24$	$s45$	$\mathbb{Q}(\zeta_3,\sqrt{5})$	6	$(uts)^5$	34	$\mathfrak{A}_6$
$G_{28}=F_4$		$2,6,8,12$	$0,4,6,10$	$s12, t12$	$\mathbb{Q}$	2	$(stuv)^6$	25	$2^4{\rtimes}(\mathfrak{S}_3\times\mathfrak{S}_3)$
G_{29}		$4,8,12,20$	$0,8,12,16$	$s40$	$\mathbb{Q}(i)$	4	$(stvu)^5$	37	$2^4{\rtimes}\mathfrak{S}_5$
$G_{30}=H_4$		$2,12,20,30$	$0,10,18,28$	$s60$	$\mathbb{Q}(\sqrt{5})$	2	$(stuv)^{15}$	34	$(\mathfrak{A}_5\times\mathfrak{A}_5){\rtimes}2$

nom	diagramme	degrés	codegrés	orbites	corps	$\lvert ZG\rvert$	$\mathbf{z}$	#cl.	G/ZG
G_{31}		$8, 12, 20, 24$	$0, 12, 16, 28$	$s60$	$\mathbb{Q}(i)$	4	$(stuwv)^6$	59	$2^4 \rtimes \mathfrak{S}_6$
G_{33}		$4, 6, 10, 12, 18$	$0, 6, 8, 12, 14$	$s45$	$\mathbb{Q}(\zeta_3)$	2	$(stuvw)^9$	40	$SO_5(3)'$
G_{34}		$6, 12, 18, 24, 30, 42$	$0, 12, 18, 24, 30, 36$	$s126$	$\mathbb{Q}(\zeta_3)$	6	$(stuvwx)^7$	169	$PSO_6^-(3)'.2$
$G_{35} = E_6$		$2, 5, 6, 8, 9, 12$	$0, 3, 4, 6, 7, 10$	$s36$	$\mathbb{Q}$	1	$(s_1 \dots s_6)^{12}$	25	$SO_6^-(2)'$
$G_{36} = E_7$		$2, 6, 8, 10, 12, 14, 18$	$0, 4, 6, 8, 10, 12, 16$	$s63$	$\mathbb{Q}$	2	$(s_1 \dots s_7)^9$	60	$SO_7(2)$
$G_{37} = E_8$		$2, 8, 12, 14, 18, 20, 24, 30$	$0, 6, 10, 12, 16, 18, 22, 28$	$s120$	$\mathbb{Q}$	2	$(s_1 \dots s_8)^{15}$	112	$SO_8^+(2)$

Deuxième partie

Cette partie se place après un cours de Michel Broué sur les groupes de tresses des groupes de réflexion complexes.

9. Monoïdes et groupes de Garside

Nous commençons par passer en revue diverses notions qui interviennent dans la définition des monoïdes de Garside.

Divisibilité. Les monoïdes que nous considérons ont tous un élément neutre noté 1. Soit M un monoïde. Étant donnés $x, y \in M$, on dit que x divise y à gauche et on note $x \leq y$ si il existe $z \in M$ tel que $xz = y$. On définit de façon analogue la divisibilité à droite, notée $\geq$. Nous notons $x < y$ si $x \leq y$ et $x \neq y$, et disons alors que x est un diviseur strict à gauche de y.

Attention ! Malgré la notation, la relation $\leq$ n'est en général pas un ordre partiel. Elle est transitive, mais n'est pas en général antisymétrique. Par exemple, si x est inversible, on a $x < 1 < x$.

Nous allons considérer des conditions qui font de $\leq$ un ordre partiel.

On dit que M est simplifiable à gauche (resp. à droite) si toute égalité dans M de la forme $ab = ac$ (resp. $ba = ca$) implique $b = c$.

Une première remarque est que si M est simplifiable à gauche et 1 est le seul élément inversible de M, alors $\leq$ est un ordre partiel. En effet si $y \leq x$ car $x = yz$ et $x \leq y$ car $y = xt$ on a $x = xtz$ d'où par simplifiabilité $tz = 1$ d'où $t = z = 1$ par absence d'éléments inversibles.

Un exemple de monoïde vérifiant les conditions ci-dessus est le monoïde $\mathbb{N}^\times$ des entiers ≥ 1 munis de la multiplication (de façon générale, tout sous-monoïde d'un groupe est simplifiable).

Condition Noetherienne. On dit que la relation de divisibilité $\leq$ est Noethérienne si la longueur des chaînes décroissantes pour la divisibilité à gauche à partir d'un élément donné a est bornée (*i.e.* les n tels qu'il existe une chaîne $a_n < \ldots < a_1 < a$).

Cela implique que $\leq$ est ordre partiel, mais implique plus. On dit que x est un *atome* si dans toute écriture $x = yz$ on a soit $y = 1$ soit $z = 1$ (cela correspond aux nombres premiers dans $\mathbb{N}^\times$). Si la divisibilité est Noetherienne, alors tout élément est produit d'un nombre fini d'atomes.

Groupe de fractions. Le sujet de ce paragraphe est le théorème de Öre :

Proposition 9.1. *Si M est simplifiable à droite et à gauche et que deux éléments de M ont toujours un multiple commun à gauche, alors M admet un groupe de fractions dans lequel il se plonge.*

Démonstration. Les fractions seront des couples (x, y) d'éléments de M, que pour la circonstance nous noterons $x^{-1}y$ (la fraction sera égale à ce quotient dans le groupe construit) ; ces couples sont pris modulo la relation d'équivalence engendrée par $x^{-1}y \sim (ax)^{-1}(ay)$. On définit le produit de la fraction $x^{-1}y$ et de $x'^{-1}y'$ comme suit : on choisit un multiple commun à gauche $x''y = y''x'$ de y et x' et on pose $x^{-1}y \times x'^{-1}y' = (x''x)^{-1}(y''y)$.

Commençons par remarquer que la définition ne dépend pas du multiple commun choisi. En effet si $x'''y = y'''x'$ est un autre multiple commun, ces deux multiples communs ont a leur tour un multiple commun, et par simplifiabilité il existe a, b

tels que $ax'' = bx'''$ et $ay'' = by'''$. On a bien $(x''x)^{-1}(y''y) \sim (ax''x)^{-1}(ay''y) = (bx'''x)^{-1}(by'''y) \sim (x'''x)^{-1}(y'''y)$.

Le même genre de raisonnement montre que le produit défini est compatible avec la relation d'équivalence.

Pour le produit défini l'élément $x^{-1}y$ a un inverse qui est xy^{-1}. L'élément neutre est $1^{-1}1$. Le plus compliqué est de vérifier l'associativité du produit, que nous laissons en exercice au lecteur.

L'application $x \mapsto 1^{-1}x$ est un plongement de M dans son groupe des fractions. □

Le monoïde $\mathbb{N}^\times$ illustre toujours le théorème ci-dessus.

Notons que si les éléments possèdent un pgcd à gauche, toute fraction a une écriture unique $x^{-1}y$ où x et y n'ont pas de diviseur commun à gauche non trivial. Notons aussi que l'existence de pgcd et de multiples communs implique celle de ppcm : on prend le pgcd de tous les multiples communs.

Monoïdes de Garside. On dit qu'un monoïde est de Garside s'il est simplifiable, que la divisibilité est Noethérienne, qu'il possède des pgcd et ppcm, et si il existe un *élément fondamental* (dit aussi *élément de Garside*) Δ tel que les ensembles $\leq \Delta$ des diviseurs à gauche de Δ et $\Delta \geq$ des diviseurs à droite de Δ coïncident, sont finis et engendrent M.

On note alors $P = \leq \Delta = \Delta \geq$ et les éléments de P sont appelés les *éléments simples* de M. Tout atome doit être simple, donc le nombre d'atomes est donc fini. Il peut y avoir plusieurs choix de Δ (si Δ en est un, une puissance de Δ en est un autre) mais il y en a un canonique qui est le pgcd de tous les Δ possibles (qui par définition est le même à droite ou à gauche ; il est souvent égal au ppcm des atomes mais pas toujours).

Nous montrerons que les monoïdes de tresses $B(W)^+$ associés à un groupe de Coxeter fini sont de Garside. Le lemme de Matsumoto 3.2(iii) implique que W possède une section $\mathbf{W}$ dans $B(W)^+$ obtenue en relevant les décompositions réduites. Dans la structure de Garside, $\mathbf{W}$ est l'ensemble des simples (et $\mathbf{S}$ l'ensemble des atomes). L'élément Δ est $\mathbf{w}_0$.

Un *groupe de Garside* est le groupe des fractions d'un monoïde de Garside. On note $G(M)$ le groupe de Garside des fractions du monoïde de Garside M.

Donnons une série de propriétés des monoïdes et groupes de Garside qui montrent leur intérêt :

Lemme 9.2. *La conjugaison par Δ induit un automorphisme qui stabilise l'ensemble des atomes (donc le treillis $(P, \leq)$).*

Démonstration. Pour $x \in P$ on a $\Delta x \Delta^{-1} = \Delta(\Delta x^{-1})^{-1}$ et $\Delta x^{-1} \in P$ puisque les simples divisent Δ ; on a donc de même $\Delta(\Delta x^{-1})^{-1} \in P$. Le fait que la conjugaison préserve la relation de divisibilité est évident. □

Puisque P est fini, une puissance finie de Δ agit trivialement sur P donc partout. Donc Δ possède une puissance centrale dans M (et dans $G(M)$). On en déduit que pour tout $g \in G(M)$, il existe i tel que $\Delta^i g \in M$. En effet, soit Δ^c une puissance centrale de Δ, soit $g = x^{-1}y$ une fraction pour g, et soit $x = x_1 \dots x_n$ une décomposition en simples de x. Alors $x_i^{-1}\Delta^c \in M$ d'où $\Delta^{cn}x^{-1} = x_n^{-1}\Delta^c \dots x_1^{-1}\Delta^c \in M$, d'où $\Delta^{cn}g \in M$.

Plus généralement, on définit une forme normale pour tout élément de $g \in G(M)$ comme suit : soit i la plus petite puissance telle que $x = \Delta^i g \in M$ (cette puissance peut être négative si on part d'un élément de M). La forme normale de g sera Δ^{-1}, suivi de la forme normale de x qui est une suite d'éléments de P définie comme suit : on pose $\alpha(x) =$ pgcd à gauche de x et $\Delta =$ le plus grand élément de P qui divise x à gauche, et on pose $\omega(x) = \alpha(x)^{-1}x$. Alors la forme normale de x et $(x_1, \ldots, x_k)$ où $x_1 = \alpha(x)$, $x_2 = \alpha(\omega(x))$, $x_3 = \alpha(\omega^2(x))$, etc...

Le fait qu'une forme est normale se voit localement : $(x_1, \ldots, x_k)$ est normale si et seulement si $x_i x_{i+1}$ l'est pour tout i. Cela vient de ce que l'on a $\alpha(xy) = \alpha(x\alpha(y))$ pour $x \in P$. En effet le pgcd de xy et Δ est x fois le pgcd de z et y où $xz = \Delta$, et comme $z \leq \Delta$, le pgcd de z et y divise $\alpha(y)$.

Un des intérêts des groupes de Garside vient de ce que ce sont des *groupes automatiques*, ce qui veut dire qu'il existe une forme normale des mots (ici, celle que nous venons de décrire) qui peut être reconnue par un automate fini. Dans de tels groupes, un grand nombre de problèmes (problèmes des mots, conjugaison, etc...) peuvent être résolus algorithmiquement. Un exemple de propriétés des groupes de tresses qui n'était connu que dans le cas des tresses ordinaires avec une preuve topologique compliquée avant qu'on les identifie à des groupes de Garside est :

Proposition 9.3. *Les groupes de Garside sont sans torsion*

Démonstration. On peut étendre $\leq$ à un ordre partiel sur tout $G(M)$ en posant $x \leq y$ si $x^{-1}y \in M$. On montre que $\leq$ est encore un treillis sur G : si $x, y \in G$ et i est tel que $\Delta^i x \in M$ et $\Delta^i y \in M$ alors on définit le pgcd de x et y comme étant Δ^{-i} fois le pgcd de $\Delta^i x$ et $\Delta^i y$ dans M. Si $x^p = 1$ on pose alors $c =$ ppcm à droite de $1, x, \ldots, x^{p-1}$. Alors $x^{-1}c$ est multiple commun de $x^{-1}\{1, \ldots, x^{p-1}\}$ qui est le même ensemble. On en déduit que $x^{-1}c = c$, *i.e.* $x = 1$. □

Mentionnons encore que si ϕ est un automorphisme de $G(M)$ qui stabilise l'ensemble des atomes, alors les points fixes de $G(M)$ sous ϕ forment encore un groupe de Garside (dont les atomes sont certains ppcm d'orbites d'atomes sous ϕ).

Le problème de la conjugaison dans les groupes de Garside possède une solution efficace ; la méthode initiale de Garside a été améliorée successivement par El Rifai et Morton, puis Franco et Gonzales-Meneses, et enfin le plus récemment par Gebhardt.

10. Groupes engendrés

Nous allons décrire une méthode générale de construction de monoïdes de Garside à partir de sections de groupes finis qui suffira pour définir les structures de Garside sur les monoïdes de tresses.

Soit W un groupe fini et S un système de générateurs engendrant W comme monoïde. Dans cette situation nous définissons la longueur $l(w)$ de $w \in W$ comme la longueur de la plus courte décomposition en générateurs de w, et nous définissons un ordre partiel $\leq_S$ (que nous appelons encore "divisibilité") par $x \leq_S y$ si il existe z tel que $xz = y$ et $l(x) + l(z) = l(y)$.

On dit que $c \in W$ est *équilibré* si les ensembles $\leq_S c$ et $c \geq_S$ de diviseurs à droite et à gauche de c coïncident.

Soit c un élément équilibré et soit $P = \leq_S (c)$. Soit $\mathbf{P}$ un ensemble muni d'une bijection $P \to \mathbf{P} : p \mapsto \mathbf{p}$. Nous définissons un monoïde par générateurs et relations :

$$M(P) = \langle \mathbf{P} \mid \mathbf{xy} = \mathbf{z} \text{ quand } x, y, z \in P, xy = z \text{ et } l(x) + l(y) = l(z) \rangle.$$

Notons que si l'ensemble partiellement ordonné P admet des bornes inférieures (pgcd) alors il admet des bornes supérieures : le ppcm de deux éléments est le pgcd des multiples communs (et par hypothèse il y a un multiple commun c).

Le but du reste de la section est de démontrer le

Théorème 10.1. *Si $(P, \leq_S)$ et $(P, \geq_S)$ sont des treillis, alors $M(P)$ est un monoïde de Garside avec atomes $\mathbf{S} = \{\mathbf{s} \mid s \in P \cap S\}$, avec simples $\mathbf{P}$ et avec $\Delta = \mathbf{c}$.*

Avant de démontrer ce théorème nous allons en donner deux applications.

Le monoïde usuel des groupes d'Artin. Nous avons vu que le monoïde de tresses $B^+(W)$ associé à un système de Coxeter fini (W, S) est de la forme $M(P)$ où ici $P = W$ (l'élément équilibré est w_0). Pour voir que 10.1 est applicable, il faut démontrer l'existence de pgcd dans W pour $\leq_S$. Nous démontrons l'existence de pgcd à droite ; la question étant symétrique cela suffit. Nous utilisons l'ensemble $N(w)$ (*c.f.* 3.3) qui vérifie $N(xy) = N(y) + N(x)^y$ si $l(xy) = l(x) + l(y)$, *i.e.* si $xy \geq y$. On voit donc que tout diviseur à droite y de $w = xy$ vérifie $N(y) \subset N(w)$. Réciproquement, on démontre par récurrence sur $l(w)$ que $N(y) \subset N(w)$ implique $w \geq y$: comme pour $y \neq 1$ on a $N(y) \cap S \neq \emptyset$ on peut choisir $s \in S \cap N(y)$ et on écrit $y = y's$ et $w = w's$ et on a $N(w') \supset N(y')$ d'où par récurrence $w' \geq y'$ d'où $w \geq y$. Donc si l'on démontre qu'il existe z tel que $N(z) = N(w) \cap N(w')$ ce sera donc le pgcd de w et w'. Si w et w' ont un diviseur commun ils ont un élément de S en commun dans leur N. On démontre alors le résultat par récurrence sur $l(w) + l(w')$: si $w \geq s$, $w' \geq s$ et $w = w_1 s$, $w' = w'_1 s$ alors $N(w) = s + N(w_1)^s$, $N(w') = s + N(w'_1)^s$. Par récurrence il existe z_1 tel que $N(z_1) = N(w_1) \cap N(w'_1)$, et $z = z_1 s$ fait l'affaire.

Le lemme suivant implique que les groupes d'Artin associés à un groupe de Coxeter irréductible fini ont un centre cyclique :

Lemme 10.2. *Soient $\mathbf{S}$ les atomes de $B^+(W)$. Supposons que w est central et que $\mathbf{s}, \mathbf{t} \in \mathbf{S}$ avec $\mathbf{s} \leq w$ et $\mathbf{st} \neq \mathbf{ts}$. Alors on a $\mathbf{t} \leq w$.*

Démonstration. Sous les hypothèses du lemme, $\mathbf{s}$ et $\mathbf{t}$ divisent tous deux $w\mathbf{t} = \mathbf{t}w$. Donc si on définit z par $\Delta_{\mathbf{s},\mathbf{t}} = \mathbf{t}z$ on a $z \leq w$. Maintenant dans un groupe de Coxeter $\Delta_{\mathbf{s},\mathbf{t}}$ est la "relation de tresse" de la forme $\mathbf{tsts}\ldots$ ($m_{s,t}$ termes) donc si $\mathbf{st} \neq \mathbf{ts}$ on a $\mathbf{st} \leq z \leq w$. Il existe donc x tel que $w = \mathbf{stx}$ d'où $\mathbf{stxs} = w\mathbf{s} = \mathbf{s}w = \mathbf{sstx}$ et simplifiant par $\mathbf{x}$ on a $\mathbf{txs} = \mathbf{stx} = w$ cqfd. □

Le monoïde dual. Il existe un autre monoïde pour les groupes de tresses, qui a d'abord été construit pour les tresses ordinaires par Birman, Ko et Lee en 1997, puis a été généralisé au type B par Digne, Michel et Bessis en 1999, puis à tous les types de Coxeter finis par Bessis en 2001, et enfin en novembre 2004 par Bessis à tous les groupes de réflexions complexes bien engendrés (c'est-à-dire les groupes irréductibles $W \subset \mathrm{GL}(\mathbb{C}^n)$ engendrés par n réflexions).

Il se trouve (on ne sait que le constater) que les groupes bien engendrés ont un unique degré de réflexion maximal que l'on note h et appelle *nombre de Coxeter*, et que ce degré est régulier, c'est-à-dire que si $\zeta = e^{2i\pi/h}$, il existe des éléments ζ-réguliers (qu'on appelle éléments de Coxeter) ; le produit des réflexions qui engendrent W dans un certain ordre est un élément de Coxeter (dans n'importe quel ordre dans le cas où W est de Coxeter).

Nous commençons par décrire la construction dans le cas des groupes de Coxeter finis. On considère cette fois W engendré par $R = \mathrm{Ref}(W)$ tout entier. Cette fois la

plus grande longueur d'un élément possible est n et cette longueur est atteinte pour un élément de Coxeter (mais un tel élément n'est pas unique et même, d'autres éléments que les éléments de Coxeter peuvent atteindre cette borne). Soit c un élément de Coxeter ; le théorème (difficile) qui permet de faire la construction est de démontrer que $P = \leq_R c$ est un treillis pour $\leq_R$ et $\geq_R$ (le fait que c soit équilibré est conséquence de ce que l'ensemble des réflexions est stable par conjugaison). Le fait que le groupe $G(M(P))$ associé au monoïde de Garside $M(P)$ n'est pas dur à voir ; on montre directement qu'on a une présentation équivalente à la présentation usuelle.

Dans le cas des groupes bien engendrés non réels, la construction est plus compliquée. Nous commençons par une définition : étant donné un groupe W, on appelle action de Hurwitz l'action du groupe de tresses ordinaire à n brins B_n de générateurs standard σ_i sur W^n donnée par

$$\sigma_i(s_1,\dots,s_n) = (s_1,\dots,s_{i-1},s_{i+1},s_{i+1}^{-1}s_is_{i+1},s_{i+2},\dots,s_n)$$
$$\sigma_i^{-1}(s_1,\dots,s_n) = (s_1,\dots,s_{i-1},s_is_{i+1}s_i^{-1},s_i,s_{i+2},\dots,s_n).$$

Cette action préserve le produit du n-uple. Si on l'applique à une décomposition d'un élément de Coxeter c en produit de réflexions, on obtient une autre décomposition du même type. Bessis montre que l'action de Hurwitz est transitive sur toutes les décompositions de c en n réflexions et que le nombre de telles décompositions est $n!h^n/|W|$. Dans le cas où W est réel, toute réflexion apparaît dans une de ces décompositions. Dans le cas général, seulement une partie R stricte de $\mathrm{Ref}(W)$ apparaît dans ces décompositions. On considère W engendré par cette partie R. Le fait que $P = \leq_R c$ soit un treillis pour $\leq_R$ et $\geq_R$ est ici encore un théorème difficile prouvé cas par cas. Si $d_1,\dots,d_n$ sont les degrés de réflexion de W, le monoïde $M(P)$ de Garside obtenu possède $\prod_i (d_i+h)/d_i$ simples (cette égalité n'a été vérifiée que cas par cas). Le fait que $G(M(P))$ soit isomorphe au groupe de tresses $B(W)$ est un autre théorème difficile mais dont la preuve est générale.

Preuve de 10.1. Notons d'abord que $\mathbf{p} \mapsto p$ est un morphisme de monoïdes $M(P) \xrightarrow{\pi} W$, dont le composé avec $P \mapsto \mathbf{P}$ est l'identité sur P. Donc $\mathbf{P}$ s'injecte dans $M(P)$. On voit aussi qu'on peut simplifier une égalité dans $M(P)$ quand le reste est dans $\mathbf{P}$: si $\mathbf{p}x = \mathbf{q}x$ où $\mathbf{p},\mathbf{q} \in \mathbf{P}$ alors on en déduit $\mathbf{p} = \mathbf{q}$ en prenant l'image par π.

Aussi, les relations définissant $M(P)$ étant homogènes pour la longueur l, ceci montre que la longueur l s'étend en une fonction additive sur tout $M(P)$ (qui est encore la longueur par rapport à l'ensemble générateur $\mathbf{S}$). En particulier il n'y a pas dans $M(P)$ d'élément inversible autre que 1, et si nous notons $\leq$ la divisibilité dans $M(P)$, c'est un ordre partiel. Notons que $l(\pi(x)) \leq l(x)$.

Lemme 10.3. *Si $x \in M(P)$ vérifie $l(\pi(x)) = l(x)$ et $\pi(x) \in P$ alors $x \in \mathbf{P}$.*

Démonstration. Commençons par remarquer que tout diviseur d'un élément qui vérifie $l(\pi(x)) = l(x)$ le vérifie aussi. Si $z = \pi(x)$ nous allons montrer par récurrence sur $l(x)$ que $x = \mathbf{z}$. On écrit $x = y\mathbf{s}$ avec $\mathbf{s} \in \mathbf{S}$. On a $l(\pi(y)) = l(y)$ d'où on déduit $\pi(y) \leq_S z$ d'où $\pi(y) \in P$ d'où (par récurrence) $y \in \mathbf{P}$. Mais alors $y\mathbf{s} = \mathbf{z}$ est une relation de $M(P)$ par définition donc $x = \mathbf{z}$. □

On en déduit que tout diviseur d'un élément de $\mathbf{P}$ est dans $\mathbf{P}$: en effet si $xy = \mathbf{p} \in \mathbf{P}$ alors on a $\pi(x) \leq_S p$ d'où $\pi(x) \in P$ et on applique le lemme.

Nous notons $\leq x$ l'ensemble des diviseurs à gauche de $x \in M(P)$. Puisque $(P, \leq_S)$ est un treillis, deux éléments $s, t \in S \cap P$ ont un ppcm à droite dans P dont nous noterons $\Delta_{\mathbf{s},\mathbf{t}}$ le relevé dans $\mathbf{P}$.

Lemme 10.4. *Soit $X \subset M(P)$ une partie finie telle que pour $x \in X$ on ait $\leq x \subset X$ et telle que si $\mathbf{s}, \mathbf{t} \in \mathbf{S}$ et $x\mathbf{s}, x\mathbf{t} \in X$ alors $x\Delta_{\mathbf{s},\mathbf{t}} \in X$. Alors il existe $y \in M(P)$ tel que $X = \leq y$.*

Démonstration. Prenons y de longueur maximale dans X et raisonnons par l'absurde, c'est-à-dire supposons qu'il existe un élément de X qui ne divise pas y. Il existe alors $x \in X$ et $\mathbf{s} \in \mathbf{S}$ tels que $x \leq y$ et $x\mathbf{s} \in X$, $x\mathbf{s} \not\leq y$. Supposons qu'on ait choisi un tel x de longueur maximale. Comme y est de longueur maximale, on a $l(x) < l(y)$ donc $x < y$ donc il existe $\mathbf{t} \in \mathbf{S}$ tel que $x\mathbf{t} \leq y$. Comme $x\mathbf{s}$ et $x\mathbf{t}$ sont dans X, l'hypothèse implique que $x\Delta_{\mathbf{s},\mathbf{t}} \in X$. Comme $x\Delta_{\mathbf{s},\mathbf{t}}$ est multiple de $x\mathbf{s}$, il ne divise pas y. Mais $x\mathbf{t}$ est un diviseur de $x\Delta_{\mathbf{s},\mathbf{t}}$ qui divise y, donc il possède un multiple x' qui divise $x\Delta_{\mathbf{s},\mathbf{t}}$ et y et tel que multiplié par l'atome suivant de $\Delta_{\mathbf{s},\mathbf{t}}$ il ne divise plus y. Ceci contredit le choix de x comme étant de longueur maximale pour cette propriété. □

Corollaire 10.5. *Si $\mathbf{x}, \mathbf{y} \in \mathbf{P}$ il existe un unique $\mathbf{z} \in \mathbf{P}$ maximal tel que $\mathbf{z} \leq \mathbf{y}$ et $\mathbf{xz} \in \mathbf{P}$.*

Démonstration. Le lemme 10.4 appliqué à l'ensemble des $\mathbf{u} \leq \mathbf{y}$ tels que $\mathbf{xu} \in \mathbf{P}$ donne le résultat. □

Dans la situation ci-dessus on pose $\alpha_2(\mathbf{x}, \mathbf{y}) = \mathbf{xz}$ et $\omega_2(\mathbf{x}, \mathbf{y}) = \mathbf{t}$ où $\mathbf{t}$ est tel que $\mathbf{y} = \mathbf{zt}$ ($\mathbf{t}$ est bien défini par la simplifiabilité quand le reste est dans $\mathbf{P}$). Les applications α_2 et ω_2 seront les applications α et ω d'un monoïde de Garside, que nous avons définies ici que pour des éléments produits de deux éléments de $\mathbf{P}$. Nous allons les définir partout par récurrence sur le nombre de termes d'une décomposition en éléments de $\mathbf{P}$. On pourrait penser qu'il suffit de définir α, et que ω sera définie en prenant le reste de la division par α : mais nous ne savons pas encore que $M(P)$ est simplifiable, et l'existence de ω nous servira pour cela ; ceci explique la démarche.

Pour faire notre récurrence, le plus commode est d'identifier $M(P)$ à l'ensemble des suites d'éléments de $\mathbf{P}$, munies de la relation d'équivalence :

$$(\mathbf{p}_1, \ldots, \mathbf{p}_{i-1}, \mathbf{p}_i, \ldots, \mathbf{p}_r) \sim (\mathbf{p}_1, \ldots, \mathbf{q}, \ldots, \mathbf{p}_r)$$

quand $\mathbf{p}_{i-1}\mathbf{p}_i = \mathbf{q}$ est une relation de $M(P)$; l'identification est via le produit de la suite.

Proposition 10.6. *Il existe des fonctions uniques $\alpha : M(P) \to \mathbf{P}$ et $\omega : M(P) \to M(P)$ telles que pour $\mathbf{p}, \mathbf{q} \in \mathbf{P}$ on ait $\alpha(\mathbf{pq}) = \alpha_2(\mathbf{p}, \mathbf{q})$ et $\omega(\mathbf{pq}) = \omega_2(\mathbf{p}, \mathbf{q})$, et telles que pour $x, y \in M(P)$ on ait $\alpha(xy) = \alpha(x\alpha(y))$ et $\omega(xy) = \omega(x\alpha(y))\omega(y)$. De plus, $\alpha(x)$ est le plus grand diviseur à gauche dans $\mathbf{P}$ de x.*

Démonstration. Nous allons définir α et ω sur les décompositions en éléments de $\mathbf{P}$ par récurrence, en posant :

$$\alpha(()) = 1, \alpha((\mathbf{p})) = \mathbf{p} \text{ et } \alpha(\mathbf{p}_1, \ldots, \mathbf{p}_r) = \alpha_2(\mathbf{p}_1, \alpha((\mathbf{p}_2, \ldots, \mathbf{p}_r)))$$

et

$$\omega(()) = \omega((\mathbf{p})) = 1 \text{ et } \omega(\mathbf{p}_1, \ldots, \mathbf{p}_r) = \omega_2(\mathbf{p}_1, \alpha((\mathbf{p}_2, \ldots, \mathbf{p}_r)))\omega((\mathbf{p}_2, \ldots, \mathbf{p}_r)).$$

Il nous faut voir que ces définitions sont compatibles à la relation d'équivalence sur les suites. Nous allons d'abord voir le

Lemme 10.7. *Si* $\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{xy} \in \mathbf{P}$ *alors*

(i) $\alpha_2(\mathbf{xy},\mathbf{z}) = \alpha_2(\mathbf{x},\alpha_2(\mathbf{y},\mathbf{z}))$.

(ii) $\omega_2(\mathbf{xy},\mathbf{z}) = \omega_2(\mathbf{x},\alpha_2(\mathbf{y},\mathbf{z}))\omega_2(\mathbf{y},\mathbf{z})$.

Démonstration. Voyons (i). Par définition $\alpha_2(\mathbf{xy},\mathbf{z}) = \mathbf{xyu}$ où $\mathbf{u}$ est maximal tel que $\mathbf{xyu} \in \mathbf{P}$ et $\mathbf{u} \leq \mathbf{z}$. De même $\alpha_2(\mathbf{y},\mathbf{z}) = \mathbf{yv}$ où $\mathbf{v}$ est maximal tel que $\mathbf{yv} \in \mathbf{P}$ et $\mathbf{v} \leq \mathbf{z}$. Comme $\mathbf{yu} \in \mathbf{P}$ et $\mathbf{u} \leq \mathbf{z}$ on a donc $\mathbf{u} \leq \mathbf{v}$ donc $\mathbf{yu} \leq \alpha_2(\mathbf{y},\mathbf{z})$. Comme $\mathbf{xyu} \in \mathbf{P}$ on a donc $\mathbf{xyu} \leq \alpha_2(\mathbf{x},\alpha_2(\mathbf{y},\mathbf{z}))$. Donc il existe $\mathbf{w} \in \mathbf{P}$ tel que $\alpha_2(\mathbf{x},\alpha_2(\mathbf{y},\mathbf{z})) = \mathbf{xyuw}$. Par simplifiabilité quand le reste est dans $\mathbf{P}$, on en déduit $\mathbf{uw} \leq \mathbf{v} \leq \mathbf{z}$; comme $\mathbf{xyuw} \in \mathbf{P}$ on a $\mathbf{w} = 1$ cqfd.

Montrons (ii). Par le (i) et la définition de ω_2, le produit à gauche des deux membres par $\alpha_2(\mathbf{xy},\mathbf{z})$ est égal à $\mathbf{xyz}$. Si nous démontrons que le membre de droite est dans $\mathbf{P}$ nous aurons gagné par simplifiabilité quand le reste est dans $\mathbf{P}$. Par définition il existe $\mathbf{u} \in \mathbf{P}$ tel que $\alpha_2(\mathbf{y},\mathbf{z}) = \mathbf{yu}$, et $\mathbf{z} = \mathbf{u}\omega_2(\mathbf{y},\mathbf{z})$. Comme $\mathbf{xy} \in \mathbf{P}$, on a $\mathbf{u} \geq \omega_2(\mathbf{x},\mathbf{yu})$ donc $\mathbf{z} = \mathbf{u}\omega_2(\mathbf{y},\mathbf{z}) \geq \omega_2(\mathbf{x},\mathbf{yu})\omega_2(\mathbf{y},\mathbf{z})$, et on a gagné car un diviseur d'un élément de $\mathbf{P}$ est dans $\mathbf{P}$. □

Pour voir que la définition de α est compatible à la relation d'équivalence sur les suites, il ne se passe quelque chose que si cette relation est appliquée au début et ce qu'il faut vérifier est alors que quand $\mathbf{p}_1\mathbf{p}_2 \in \mathbf{P}$ on ait $\alpha_2(\mathbf{p}_1\mathbf{p}_2,\alpha((\mathbf{p}_3,\ldots,\mathbf{p}_r))) = \alpha_2(\alpha_2(\mathbf{p}_2,\alpha((\mathbf{p}_3,\ldots,\mathbf{p}_r))))$ ce qui est 10.7(i).

Il est clair que $\alpha(x)$ est le plus grand diviseur à gauche de x dans $\mathbf{P}$: si $\mathbf{p}$ est un diviseur à gauche de x dans $\mathbf{P}$, alors x peut être représenté par une suite de la forme $(\mathbf{p},\ldots)$ et la construction montre que $\alpha(x)$ est multiple à droite de $\mathbf{p}$.

Enfin, il est immédiat par récurrence sur le nombre de termes dans une décomposition de x en termes dans $\mathbf{P}$ que $\alpha(xy) = \alpha(x\alpha(y))$.

De même, pour vérifier que la définition de ω est compatible à la relation d'équivalence il faut vérifier si $\mathbf{p}_1\mathbf{p}_2 \in \mathbf{p}$ et qu'on pose $\mathbf{z} = \alpha((\mathbf{p}_3,\ldots,\mathbf{p}_r))$ que $\omega_2(\mathbf{p}_1\mathbf{p}_2,\mathbf{z}) = \omega_2(\mathbf{p}_1,\alpha_2(\mathbf{p}_2,\mathbf{z}))\omega_2(\mathbf{p}_1,\mathbf{z})$ ce qui est 10.7(ii).

Enfin, la propriété $\omega(xy) = \omega(x\alpha(y))\omega(y)$ se démontre encore par récurrence sur le nombre de termes dans un décomposition en éléments de $\mathbf{P}$ de x. □

La proposition ci-dessus nous donne déjà un début de simplifiabilité : si $x \in M(P)$, il y a un unique y tel que $x = \alpha(x)y$, et cet y vaut $\omega(x)$. Nous le montrons par récurrence sur $l(x)$. En effet on a $\omega(x) = \omega(\alpha(x)y) = \omega(\alpha(x)\alpha(y))\omega(y)$; mais comme $\alpha(\alpha(x)\alpha(y)) = \alpha(x)$ et qu'on est dans le cas où ω est défini en termes de ω_2, on a $\omega(\alpha(x)\alpha(y)) = \alpha(y)$. Mais par récurrence sur la longueur on a $y = \alpha(y)\omega(y)$ d'où finalement $\omega(x) = y$ cqfd.

On en déduit la simplifiabilité en général. Faisons-le à gauche (comme la définition de $M(P)$ est symétrique entre la droite et la gauche il est clair que cela suffit), *i.e.* voyons que $ab = ac$ implique que $b = c$. Il est clair qu'il suffit de le démontrer quand $a \in \mathbf{P}$ (alors on peut simplifier par les termes d'une décomposition de a tout à tour). Comme $\alpha(ab) = \alpha(a\alpha(b)) = \alpha_2(a,\alpha(b))$ on a $\alpha(ab) = ax$ où $x \leq b$, *i.e.* $b = xb'$. De même $\alpha(ac) = ay$ où $c = yc'$. Mais par la simplifiabilité dans $\mathbf{P}$ l'égalité $ax = ay$ implique $x = y$. Donc $ab = \alpha(ab)b' = \alpha(ab)c'$ donc $b' = c' = \omega(ab)$ cqfd.

Il ne reste plus qu'à montrer l'existence de pgcd et ppcm pour tout $M(P)$. L'existence du pgcd est une conséquence immédiate de 10.4 une fois qu'on remarque

que si $\mathbf{s}, \mathbf{t} \in \mathbf{S}$, et $\mathbf{s} \leq x$, $\mathbf{t} \leq x$ implique $\Delta_{\mathbf{s},\mathbf{t}} \leq x$ car on a dans ce cas $\mathbf{s} \leq \alpha(x)$, $\mathbf{t} \leq \alpha(x)$ d'où $\Delta_{\mathbf{s},\mathbf{t}} \leq \alpha(x) \leq x$.

Pour voir l'existence d'un ppcm, on démontre d'abord qu'il existe une permutation σ de $\mathbf{P}$ telle que $\Delta\mathbf{p} = \sigma(\mathbf{p})\Delta$. En effet, si $\mathbf{p}'\mathbf{p} = \Delta$ et $\mathbf{p}''\mathbf{p}' = \Delta$ on a $\Delta\mathbf{p} = \mathbf{p}''\mathbf{p}'\mathbf{p} = \mathbf{p}''\Delta$. On en déduit qu'il existe une puissance Δ^a de Δ centrale dans $M(P)$. On démontre alors par récurrence sur le nombre de termes d'une décomposition $x = \mathbf{p}_1 \dots \mathbf{p}_n$ en éléments de $\mathbf{P}$ que $x \leq \Delta^{an}$. En effet par récurrence $\mathbf{p}_2 \dots \mathbf{p}_n \leq \Delta^{a(n-1)}$ donc $x \leq \mathbf{p}_1\Delta^{a(n-1)} = \Delta^{a(n-1)}\mathbf{p}_1 \leq \Delta^{an}$. Donc deux éléments ont un multiple commun ; pour avoir un ppcm il suffit de prendre le pgcd des multiples communs. □