Mémoire de Magistère

Damien Robert

11 octobre 2006

Table des matières

Damien ROBERT
45, rue d'Ulm
75005 Paris

Tél. : 06 66 56 25 49
E-mail : robert@clipper.ens.fr
http://www.eleves.ens.fr/home/robert/

Né le 11/11/1984
à Échirolles (Isère)
Nationalité Française

Études

2000–2001	**Bac Scientifique spécialité Mathématiques**, *mention Très Bien* au Lycée René Descartes, Saint-Genis-Laval (Rhône).
2001–2003	**Classes préparatoires MPSI et MP*** au Lycée du Parc, Lyon.
2003–2007	**Entrée à l'École Normale Supérieure de Paris**, *série Informatique (Rang 1).*
2003–2006	**Magistère de Mathématiques (MMFAI)**, École Normale Supérieure.
2003–2004	**Licence et Maîtrise de Mathématiques**, *mentions Très Bien* à l'École Normale Supérieure. Validation de cours d'Informatique de Licence et de Maîtrise.
2004–2005	**Agrégation de Mathématiques, option Calcul Scientifique**, *Rang 9.* **M2 de Mathématiques Pures, inscription pédagogique**, *Algébre et Géométrie* à Paris VI, Paris VII, Paris XI et Polytechnique.
2005–2006	**M2 de Mathématiques Pures**, *Algébre et Géométrie* de Paris VI. Cours d'introductions : Algèbre commutative et géométrie algébrique par Lysenko, Catégorie et faisceaux par Schapira, Introduction à la Théorie algébrique des nombres par Oesterlé, Introduction aux algèbres de Lie par Toledano (Note : 20/20). Introduction à la Géométrie Algébrique par Laszlo (Note : 19/20). Groupes algébriques par Polo (Note : 20/20). Suivi de certains cours du M2 de Paris VII. Mémoire de M2 sur la classification des groupes de réflexions complexes avec Michel Broué (Institut Henri Poincaré), soutenance en septembre 2006.

Exposés

- Co-organisation d'un groupe de travail sur les corps quadratiques et groupes de classes : http://www.eleves.ens.fr/home/robert/gt/.
- Exposé de maîtrise sur les modules de Clifford et leur application à la K-Théorie : http://www.mmfai.ens.fr/exposes/2004/RobertTibouchi04.pdf.

Langues pratiquées

Anglais courant : j'ai vécu un an aux États-Unis (Knoxville, Tennessee), et fait divers séjours dans des pays anglo-saxons.

Allemand moyen.

Compétences en informatique

Systèmes : Unix et Linux.
Langages : C, Java, Latex, Ocaml, Perl, Shell, xhtml/xml.

Expériences

- Je suis membre des tuteurs informatiques (http://www.tuteurs.ens.fr) qui aident les débutants à se familiariser avec les systèmes freebsd/solaris/linux de l'École Normale Supérieure. J'ai organisé et encadré des stages de travaux pratiques dans ce cadre.
- Je fais partie des Administrateurs Élèves de l'École Normale Supérieure qui s'occupent de l'installation logicielle des machines informatiques.

Jacobienne des courbes de genre 2
Applications à la cryptographie

Damien Robert
Directeur de thèse: Guillaume Hanrot

4 Octobre 2006

Table des matières

1 Logarithme discret dans un groupe

Définition 1: Soit G un groupe abélien fini. $g \in G$ un élément du groupe d'ordre n, et $y \in \langle g \rangle$. On note $\log_g(y)$ l'élément $x \in \mathbf{Z}/n\mathbf{Z}$ tel que $y = g^x$, c'est le logarithme de y en base g.

1.1 Logarithme discret en cryptographie

Le logarithme discret dans un groupe est a priori difficile à calculer, alors que sa fonction réciproque l'exponentiation est rapide ($g \mapsto g^m$ est polynomiale en $\log_2(m)$). A l'instar du couplage puissance modulaire et racine modulaire dans $\mathbf{Z}/p\mathbf{Z}$ qui donne RSA, le problème du logarithme discret nous fourni une cryptographie asymétrique.

Ainsi, supposons que Alice et Bob veulent converser sur un canal public. S'ils ont beaucoup de données à échanger, utiliser un protocole à base de clé publique pour l'ensemble de l'échange est coûteux, de tels algorithmes étant environ 100 fois plus longs que les algorithmes à clé secrète. Le meilleur moyen est d'arriver à échanger une clé secrète de manière sécurisée.

Définition 2 (Protocole d'échange de clé de Diffie-Hellmann): Alice choisit un groupe G[1] et un élément $g \in G$ d'ordre n, qu'elle rend publique. Alice choisit ensuite un secret $a \in \mathbf{Z}/n\mathbf{Z}$, et publie $p_a := g^a$. Bob choisit de même $b \in \mathbf{Z}/n\mathbf{Z}$ et publie $p_b := g^b$. Alice et Bob calculent ensuite la clé secrète commune $s := g^{ab} = p_a^b = p_b^a$.

Un attaquant (Eve) qui voudrait retrouver retrouver la clé secrète commune doit trouver g^{ab} à partir de g^a et g^b. Il s'agit du problème de Diffie-Hellman calculatoire pour le couple p_a, p_b. En pratique, on ne sait résoudre le problème de Diffie-Hellman calculatoire qu'en calculant le log discret de p_a ou p_b.

La même idée conduit à un algorithme de cryptographie à clé publique reposant sur le problème de Diffie-Hellmann calculatoire.

Définition 3 (Algorithme d'ElGamal): Alice choisit un groupe G et un élément $g \in G$. Elle choisit une clé secrète $a \in \mathbf{Z}$ et publie $(G, g, p_a := g^a)$. Bob veut envoyer un message $m \in G$ à Alice, sans que Eve qui écoute sur le canal ne puisse le connaître. Il choisit $b \in \mathbf{Z}$ et envoie $(p_b := g^k, s := p_a^k m)$. Alice calcule alors $m = s/p_b^a$.

Eve connaît g^a, g^k et $g^(ak)m$. Retrouver m revient encore une fois à un problème de Diffie-Hellmann calculatoire sur le couple g^a, g^b.

Remarque 4: Bob doit faire attention à changer k à chaque message qu'il envoie, car à partir de $g^k m_1$ et $g^k m_2$, Eve connaît m_1/m_2, ce qui lui permettrait de retrouver m_1 si elle arrive à faire envoyer par Bob un message m_2 qu'elle connaît.

Comme d'habitude, en magouillant ce protocole de cryptographie asymétrique on arrive à un algorithme de signature de message :

Définition 5 (Algorithme de signature d'ElGamal): Alice a toujours $(G, g, p_a := g^a)$ comme clé publique, où cette fois on suppose que $G = \mathbf{Z}/p\mathbf{Z}^\star$ et g est un de ses générateurs. Elle envoie un message m à Bob. Le canal étant non sécurisé, Bob veut vérifier que le message provient bien d'Alice. Alice choisit alors $k \in (\mathbf{Z}/p\mathbf{Z})^\star$ au hasard puis publie

[1] En pratique on prend $G = (\mathbf{Z}/pZ)^\star$ pour p un grand nombre premier

$(r := g^k, s := (m - ar)/k)$[1]. Si $s = 0$, Alice recommence le calcul avec un autre k . Bob n'a plus qu'à vérifier que $g^m = p_a^r r^s$.

Remarque 6:
- Si Bob retrouve a à partir de l'information donnée par Alice, c'est qu'il connaît k et donc connaît le log discret de r.
- Si Eve répond à la place d'Alice, elle doit trouver $r := g^k$ et s tels que $p_a^r r^s = g^m$, c'est à dire que $ar + ks \cong m$, mais alors elle connaît a.
- L'algorithme de signature DSA est basé sur un schéma de même type.

Enfin, le logarithme discret peut aussi servir comme protocole Zero-Knowledge. Alice à un secret s. Elle veut prouver à Bob qu'elle connaît s, mais sans lui révéler.

Définition 7 (Zero-Knowledge): Alice choisit un groupe G et un élément $g \in G$ d'ordre n. Bob veut vérifier que Alice connaît bien $s \in \mathbf{Z}/n\mathbf{Z}$. Alice ne veut pas révéler s à Bob. Le protocole est le suivant : Alice publie $p = g^s$. Puis elle choisit un $x \in \mathbf{Z}/n\mathbf{Z}$ au hasard, et envoie $q = g^x$ à Bob. Bob à deux choix : soit il demande x à Alice et vérifie que $q = g^x$, soit il demande $s + x$ et vérifie que $qp = g^{x+s}$. On recommence un nombre suffisant de choix jusqu'à ce que Bob soit convaincu que Alice connaît bien s.

Remarque 8: Si Alice ne connaît pas s mais connaît le choix de Bob à l'avance, elle peut le tromper ainsi : si Bob va vérifier que $qp = g^{x+s}$, Alice envoie g^x/p au lieu d'envoyer g^x. Mais si Bob demande x, Alice doit alors renvoyer $x - s$, ce qui n'est pas possible si elle ne connaît pas s.

1.2 Difficulté du logarithme discret

Pour toute la suite du texte, p représentera un nombre premier, et q une puissance de p.

Pour que les algorithmes précédents soient sûrs, il faut vérifier que le logarithme discret est effectivement difficile à calculer. On se place dans un groupe $G = \langle g \rangle$ générique, c'est à dire un groupe où l'on utilisera que les opérations suivantes :
- Calculer ab et a^{-1} si l'on se donne $a, b \in G$.
- Tester si $a = b$.
- On suppose que l'on a une bonne représentation informatique de G, c'est à dire en gros que l'on peut trier/hacher/chercher efficacement des éléments dans G.

On se demande alors combien de calculs un attaquant doit faire s'il veut espérer trouver x à partir de g^x. Soit N l'ordre de G. L'algorithme trivial donne un algorithme d'inversion en $O(N)$ [2] opérations. On peut toutefois faire un peu mieux en utilisant une méthode de type « diviser pour régner ».

Algorithme 9 (Pas de bébés, pas de géants): *Soit $u \approx \sqrt{N} \in \mathbf{N}$. On écrit x en base u : $x = x_0 + x_1 u$. Alors $hg^{-x_0} = (g^u)^{x_1}$. Ainsi on construit la liste $\{h, hg^{-}1, \ldots, hg^{-u}\}$ et on calcule $g^u, (g^u)^2, \ldots, (g^u)^u$ jusqu'à tomber sur un élément de la liste.*

L'algorithme à un coût en complexité en $O(\sqrt{N})$ et en mémoire en $O(\sqrt{N})$, ainsi on a cassé le problème de taille N en $\sqrt{N}$ problèmes de tailles $\sqrt{N}$.

[1] En pratique pour la signature on remplace m par un hachage de m

[2] Comme les algorithmes qu'on va présenter dans cette partie sont typiquement exponentiels ou sous-exponentiels (en $\log(N)$), on omettra les polynômes en $\log(N)$ dans les $O(.)$.

Ensuite, le théorème des restes chinois conjugué à un lemme de Hensel trivial permettent de se ramener à un nombre premier divisant N.

Algorithme 10 (Pohlig-Hellmann): *Soit $N = \prod p_i^{e_i}$ la décomposition de N en facteurs premiers. Par les restes chinois, il suffit de trouver $x \mod p_i^{e_i}$. On écrit alors $x = x_0 + px_1 + \cdots + x_{e-1}p^{e-1}$. Soit $\beta = g^{N/p}$. Alors $x_0 = \log_\beta(h^{N/p})$ (car $h^{N/p} = \beta^x = \beta^{x_0}$ puisque β est d'ordre p , $x_1 = \log_\beta\left(hg^{-x_0}\right)^{N/p^2}$, ...*

Ainsi le problème du logarithme discret en taille N est de l'ordre de grandeur du problème du logarithme discret en taille p, où p est le plus grand nombre premier divisant N.

Enfin on peut se passer du coût en mémoire de $O(\sqrt{N})$ de l'algorithme « Pas de bébés, pas de géants » en adaptant la méthode ρ pour la factorisation d'un entier :

Algorithme 11 (Algorithme ρ de Pollard): *On choisit une fonction de hachage $H : \langle()G) \to [1;20]$, et des éléments $m_k = g^{\alpha_k}h^{\beta_k}$, $k \in [1;20]$ où les α_k, β_k sont choisis au hasard.*

On choisit a_0, b_0 au hasard et on calcule $s_0 = g^{a_0}h^{b_0}$. Puis on définit $s_{i+1} = s_i m_{H(s_i)}$, $a_{i+1} = a_i + \alpha_{H(s_i)}$ et $b_{i+1} = b_i + \beta_{H(s_i)}$.

On itère jusqu'à trouver une collision $s_i = s_j$, on a alors $h = g^{\frac{a_i - a_j}{b_i - b_j}}$ ce qui nous donne x sous réserve que $b_i \neq b_j$ (mais ce cas a une probabilité $1/N$ donc très faible de se produire). Le paradoxe des anniversaires montre que i et j sont en $O(\sqrt{N})$. Et on peut ne garder qu'un élément sur 2^k, quitte à itérer un peu plus (c'est à dire remplacer i par la plus petite puissance de deux qui le contient).

D'où un coût en $O(\sqrt{N})$ et essentiellement nul en mémoire.

Théorème 12: *Dans un groupe générique, l'algorithme ρ combiné à l'algorithme de Pohlig-Hellmann est à peu près optimal.*

Le graal de la cryptographie est donc de trouver des groupes suffisamment génériques pour que l'on ait pas d'autres moyens que les algorithmes précédents pour calculer un logarithme discret. Bien évidemment, le problème du logarithme discret étant *NP*, on ne peut espérer prouver qu'une famille de groupe est suffisamment générique (sous peine de prouver que $P \neq NP$).

Un exemple de groupe qui ne convient pas du tout est le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$, puisque le logarithme discret revient à calculer l'inverse par la loi multiplicative de x par g, ce qui se fait par un algorithme d'Euclide étendu et est très rapide (polynomial en $\log(n)$).

Le groupe $(\mathbf{Z}/p\mathbf{Z})^\star$, avec g un générateur de ce groupe, semble plus robuste et les premières applications du logarithme discret se faisaient dans ce groupe. Cependant en adaptant les idées du crible quadratique utilisée pour la factorisation on a des attaques plus efficaces. L'idée est de calculer des éléments g^r (que l'on voit dans $\mathbf{Z}$), de regarder ceux qui sont divisibles par des petits nombres premiers q_i (on dit que ce sont des nombres friables). Une fois que l'on a suffisamment de relations, on utilise de l'algèbre linéaire (avec des matrices très creuses) pour trouver les $\log(q_i)$. Enfin on prends des r au hasard jusqu'à ce que $h.g^r$ soit friable, ce qui permet de trouver le logarithme de h. Le coût de cet algorithme est $L_p(1/2, \sqrt{2})$ où $L_N(\alpha, C) = \exp(C(\log N)^\alpha(\log\log N)^{1-\alpha})$.

On peut même faire encore mieux en adaptant le crible algébrique : dans $(\mathbf{Z}/p\mathbf{Z})^\star$ on aboutit à des algorithems pour le logarithme discret en $L_p(1/3, (64/9)^{1/3}$.

Actuellement, on utilise du logarithme discret dans des courbes elliptiques.

2 Courbes elliptiques

Soit k un corps algébriquement clos de caractéristique différente de 2. On se place dans le plan affine $\mathbf{A}^2(k) = \operatorname{Spec} k[x, y]$ et on considère un polynôme $f \in k[x]$ de degré 3 ayant des racines distinctes. On peut supposer que f est de la forme $f(x) = x^3 + ax + b$. Alors $\operatorname{Var}(y^2 - f(x))$ est une courbe lisse, on dit que c'est une courbe elliptique $\mathcal{C}$. La cloture de $\mathcal{C}$ dans $\mathbf{P}^2_k = \operatorname{Proj} k[x, y, z]$ (que l'on notera toujours $\mathcal{C}$) consiste à rajouter le point à l'infini $P_0 = (0, 1, 0)$.

2.1 Loi de groupe sur les points d'une courbe elliptique

L'intérêt des courbes elliptiques est que l'on peut définir une loi de groupes sur ses points rationnels.

Théorème 13 (Bézout): *Soit $\mathcal{C}_1$ et $\mathcal{C}_2$ deux courbes de degrés s et t dans $\mathbf{P}^2_k$, sans composantes irréductibles communes. Alors elles s'intersectent en st points, avec multiplicités.*

Maintenant une courbe elliptique est de degré 3, et deux points P_1 et P_2 sur la courbe donnent lieu à une droite L (qui n'est autre que la tangente à la courbe en P_1 si $P_1 = P_2$). L intersecte $\mathcal{C}$ en exactement un autre point P_3 par Bézout (car si $P_1 = P_2$ la multiplicité de l'intersection de $L \bigcap \mathcal{C}$ en P_1 est au moins 2), qui peut être égal à P_1 ou P_2. Si $P = (x : y : z)$ est un point de $\mathcal{C}$, $-P := (x : -y : z) \in \mathcal{C}$. On définit alors la loi de groupe sur $\mathcal{C}(k)$ par $P_1 + P_2 := -P_3$.

On vérifie que si P est un point de la courbe, comme la ligne qui passe par P et P_0 est la ligne verticale passant par P, elle intersecte la courbe en $-P$, donc $P + P_0 = P$, P_0 est l'élément neutre (c'est vrai aussi si $P = P_0$ car P_0 est un point d'inflexion, et si $P = -P$ car alors la droite verticale est tangente à $\mathcal{C}$en P). Comme la ligne qui passe par P et $-P$ est verticale, elle passe par P_0 d'où $P + -P = -P_0 = P_0$, donc $-P$ est bien l'inverse de P pour cette loi additive et on a bien un groupe.

Le point délicat que j'ai soigneusement omis de signaler est la vérification de l'associativité. On l'obtiendra plus tard lorsqu'on présentera une autre méthode pour construire le groupe associé à une courbe elliptique.

2.2 Loi de groupe induite sur les points rationnels de la courbe

Pour les besoins cryptographiques, $\mathcal{C}(k)$ étant un groupe infini ne peut convenir. On se ramène à un groupe fini de la manière suivante : on part d'un corps fini $\mathbf{F}_q$ est d'un polynôme f défini sur $\mathbf{F}_q$. Si on considère la courbe sur $\overline{\mathbf{F}}_q$ on peut regarder ses points rationnels $\mathcal{C}(\mathbf{F}_q)$[1].

Il faut vérifier que $\mathcal{C}(\mathbf{F}_q)$ est un sous-groupe fini de $\mathcal{C}(\overline{\mathbf{F}}_q)$. La finitude est claire puisque $\mathbf{P}^2_{\mathbf{F}_q}$ est de cardinal fini. Mais si $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ sont dans $\mathcal{C}(k)$, un calcul explicite (si P_1 et P_2 ne sont pas à l'infini et que $P_1 \neq -P_2$) montre que $P_1 + P_2 = P_3$ où $P_3 = (x_3, y_3)$ avec

[1]Schématiquement, si $\mathcal{C}$ est le schéma défini par $y^2 - f$, regarder la courbe sur $\overline{\mathbf{F}}_q$ revient à considérer le schéma $\overline{\mathcal{C}} := \mathcal{C} \otimes \overline{\mathbf{F}}_q$, et l'on a alors $\overline{\mathcal{C}}^{\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)} = \mathcal{C}$. Les points de $\mathcal{C}$ sont donc en bijection avec les orbites de points dans $\overline{\mathcal{C}}$.

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}m^2 \tag{1}$$

$$y_3 = -y_1 + m(x_1 - x_3) \tag{2}$$

où

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{si } P_1 \neq P_2 \\ f'(x_1)/2y_1 & \text{si } P_1 = P_2 \end{cases} \tag{3}$$

Ce qui montre bien que la somme de deux points rationnels est rationnel (ce qui est d'ailleurs évident géométriquement, trouver l'intersection de la ligne (de degré 1) passant par P_1 et P_2 avec f (de degré 3) revient à calculer les racines d'un polynôme de degré 3, qui a deux racines rationnelles, donc il en va de même pour sa troisième racine).

3 Jacobienne d'une courbe

On aimerait pouvoir généraliser la construction à une courbe $\mathcal{C}$ lisse projective irréductible quelconque. Le problème c'est que si on prend deux points sur la courbe, la ligne qui les rejoint intersecte la courbe en $d-2$ autres points (avec multiplicités), où d est le degré de la courbe, par le Théorème 13.

Mais si l'on réfléchit à la construction qu'on a effectuée pour les courbes elliptiques, on dit que $P_1 + P_2 + P_3 = 0$ si et seulement si ils sont alignés. On va appliquer le même genre d'idées pour la courbe en disant qu'une somme de point est nulle si et seulement si il y a une ligne passant par ces points avec la bonne multiplicité, sauf qu'en fait pour obtenir des relations intéressantes on va remplacer les intersections de la courbe avec une ligne par n'importe quelle intersection de la courbe avec une de ses fonctions rationnelles.

3.1 Diviseurs de Weil sur une courbe

À partir de maintenant on emploie le mot courbe pour définir une variété projective irréductible lisse de dimension 1 sur un corps algébriquement clos k.

Définition 14: Un diviseur D sur $\mathcal{C}$ est une somme formelle de points de $\mathcal{C}$

$$D = \sum_{x \in \mathcal{C}} n_x x$$

où les $n_x \in \mathbf{Z}$ sont presque tous nuls. Le support de D est l'ensemble des $x \in \mathcal{C}$ tels que $n_x \neq 0$. On note $\mathrm{Div}(\mathcal{C})$ l'ensemble des diviseurs de $\mathcal{C}$, c'est le groupe abélien libre engendré par les points de $\mathcal{C}$. Un diviseur D est dit effectif si $n_x \geqslant 0$ pour tout $x \in \mathcal{C}$, on notera $D_1 \geqslant D_2$ lorsque $D_1 - D_2$ est effectif. Enfin on a un épimorphisme $\deg : \mathrm{Div}(\mathcal{C}) \to \mathbf{Z}$ en associant à un diviseur $D = \sum n_x x$, $\deg(D) = \sum n_x$.

À une fraction rationnelle $h \in K(X)$, on peut associer un diviseur de la manière suivante : si P est un point de la courbe, l'anneau des germes en P $\mathcal{O}_P$ est un anneau local régulier, donc factoriel, de dimension 1, c'est donc un anneau de valuation discrète, que l'on notera v_P. Si $v_P(f) > 0$, f est définie au voisinage de P est on dit qu'elle a un zéro d'ordre $v_P(f)$, si

$v_P(f) < 0$ on dit que f a un pôle d'ordre $-v_P(f)$ en P. On définit alors le diviseur (f) associé à f par $(f) = \sum v_P(f).P$. On dit que (f) est un diviseur principal.

(f) est bien un diviseur, en effet f est régulière sur un ouvert U de X, or $X \setminus U$ est fini (car de dimension 0) donc ne fait intervenir qu'un nombre fini de points, et les zéros de f sont dans l'idéal définit par l'idéal de f, donc sont également en nombres finis, qui est fermé, donc fini.

Lemme 15: *(f) est de degré 0.*

DÉMONSTRATION: Voir [Har] pour les détails. Si $f \in K(X)^\star$, l'inclusion $k(f) \subset k(X)$ induit un morphisme birationnel $\varphi : X \mapsto \mathbf{P}^1_k$, qui s'étend en un morphisme fini de $X \mapsto \mathbf{P}^1_k$ car X est projectif. (f) correspond au tiré en arrière du diviseur $(x) = (0) - (\infty)$ dans $\mathbf{P}^1_k$, et est donc de degré 0. ■

3.2 Groupe de Picard

En suivant les idées du début de la partie, on va dire qu'une somme de diviseur est (formellement) nulle s'il est le lieu des zéros (avec multiplicités et en comptant les pôles) d'une fonction rationnelle de $\mathcal{C}$.

Définition 16: On vérifie facilement que $f \mapsto (f)$ est un morphisme de $\mathrm{K}(X)^\star$ sur $\mathrm{Div}(\mathcal{C})$. On notera $\mathrm{PDiv}(\mathcal{C})$ l'image par ce morphisme. Le groupe de Picard de $\mathcal{C}$ est le groupe $\mathrm{Pic}(\mathcal{C})$ quotient de $\mathrm{Div}(\mathcal{C})$ par $\mathrm{PDiv}(\mathcal{C})$. Si D est D' ont la même image dans $\mathrm{Pic}(\mathcal{C})$, on dit qu'ils sont linéairement équivalents, et l'on note $D \sim D'$. Le Lemme 15 montre que l'application degré se factorise par $\mathrm{Pic}(\mathcal{C})$.

Remarque 17: Le groupe de Picard est infini, si D est un diviseur de degré non nul, les $nD, n \in \mathbf{Z}$ sont distincts car de degrés distincts.

Définition 18: La jacobienne d'une courbe $\mathcal{C}$ est le sous-groupe des éléments de degrés 0 dans le groupe de Picard de $\mathcal{C}$.

On a ainsi associé à toute courbe un groupe $\mathrm{Jac}(\mathcal{C})$. Il reste à vérifier que la jacobienne d'une courbe elliptique correspond aux points de la courbe elle même, et que la jacobienne d'une courbe sur un corps fini donne bien lieu à un groupe fini. Pour cela il faut d'abord définir ce qu'on appelle la jacobienne d'une courbe sur un corps non algébriquement clos, où plutôt comment définir les points k-rationnels d'une Jacobienne.

Définition 19: Soit k un corps parfait, et $\mathcal{C}$ une courbe définie sur k. On peut la regarder sur $\overline{k}$ et parler de sa jacobienne dans $\overline{k}$. Soit G le groupe de Galois de $\overline{k}/k$. Alors G agit sur $\mathcal{C}$ puisque $\mathcal{C}$ est définie sur k (et donc $G.\mathcal{C} = \mathcal{C}$ dans $\mathbf{A}^{\overline{k}}_2$). De plus l'image d'un diviseur principal (f) par $g \in G$ est le diviseur principal $(g.f)$. Donc le quotient induit une action naturelle de G sur $\mathrm{Pic}(\mathcal{C})$.

On dit alors qu'un élément du groupe de Picard de $\mathcal{C}$ est rationnel s'il est invariant par G, et on note $\mathrm{Jac}(\mathcal{C})(k)$ l'ensemble des éléments k-rationnels de la Jacobienne.

Remarque 20: Si l'on voit la variété $\mathcal{C}$ comme un schéma X, regarder $\mathcal{C}$ sur $\overline{k}$ revient à considérer $\overline{X} = \mathcal{C}(X) \otimes_k \overline{k}$. Les points de X correspondant à des orbites sour G de points de $\overline{X}$ on voit que $\mathrm{Div}(X) = \mathrm{Div}(\overline{X})^G$.

De plus si D est un diviseur dans X qui devient principal dans $\overline{X}$, alors D est principal dans X. En effet on note $D = (f)$ dans $\overline{X}$, D est invariant par G donc $(g.f) \sim (f)$. Donc la fonction rationnelle $g.f/f$ est dans $\Gamma(\overline{X}, \overline{k}[X]^\star)$ car le schéma étant intègre et lisse de dimension 1 est normal, or un anneau normal est égal à l'intersection de ses localisés en ses idéaux premiers de codimension 1. Mais $\Gamma(\overline{X}, \overline{k}[X]^\star) = \overline{k}^\star$ car $\overline{X}$ est propre. Donc quitte à remplacer f par un multiple, on peut supposer qu'elle est invariante par l'action du groupe de Galois, donc provient d'une fonction dans $X = \overline{X}^G$.

Cependant, on n'a pas $\mathrm{Pic}(\overline{X})^G = \mathrm{Pic}(X)$ en général. En effet on a la suite exacte $0 \mapsto \mathrm{PDiv}(\overline{X}) \mapsto \mathrm{Div}(\overline{X}) \mapsto \mathrm{Pic}(\overline{X}) \mapsto 0$ et si on lui applique le foncteur exact à gauche on a la début de la longue suite exacte de cohomologie correspondante : $0 \mapsto \mathrm{PDiv}(\overline{X}) = \mathrm{PDiv}(\overline{X})^G \mapsto \mathrm{Jac}(X) = \mathrm{Jac}(\overline{X})^G \mapsto \mathrm{Pic}(\overline{X})^G$ mais il peut y avoir des H^1 ensuite.

Il n'est pas clair que $\mathrm{Jac}(\mathcal{C})(k)$ soit un groupe fini si $k = \mathbf{F}_q$ est un corps fini. On verra plus tard que c'est effectivement le cas.

3.3 Fibrés en droite sur une courbe $\mathcal{C}$

On rappelle que se donner un fibré en droite sur $\mathcal{C}$ revient au même que se donner un faisceau de modules inversible.

Si $D = \sum n_P P$ est un diviseur effectif de $\mathcal{C}$ il définit un sous-schéma $\mathrm{Spec} \prod_{P \in \mathcal{C}} \mathcal{O}_{\mathcal{C},P}/P^{n_P}$ fermé fini de $\mathcal{C}$. Ce schéma fermé est défini par un faisceau quasi-cohérent d'idéaux de $\mathcal{O}$ que l'on note $\mathcal{O}(-D)$.

Par définition, les sections de $\mathcal{O}(-D)$ sur un ouvert U de $\mathcal{C}$ sont

$$\Gamma(U, \mathcal{O}(-D)) = \{f \in k[U], v_P(f) \geqslant n_P \text{ pout tout } P \in U\} \tag{4}$$
$$= \{f \in \mathrm{K}(\mathcal{C}), v_P(f) \geqslant n_P \text{ pout tout } P \in U\} \tag{5}$$

L'égalité à lieu puisque les v_P étant positifs, une fonction rationnelle dans la section est en fait définie sur U.

Ceci conduit à poser pour n'importe quel diviseur D.

$$\Gamma(U, \mathcal{O}(-D)) = \{f \in \mathrm{K}(\mathcal{C}), v_P(f) \geqslant -n_P \text{ pout tout } P \in U\} \tag{6}$$

$\mathcal{O}(-D)$ est un sous-faisceau quasi-cohérent de $\mathrm{K}(\mathcal{C})$. Son localisé en $P \in \mathbf{C}$ n'est autre que $\pi_P^{-n_P}\mathcal{O}_P$ où π_P est une uniformisante de l'anneau de valuation discrète $\mathcal{O}_P$, il est donc localement inversible.

Réciproquement, tout sous-faisceau de module M de $\mathrm{K}(\mathcal{C})$ est inversible (car si U est un ouvert affine, $A = \mathcal{O}_\mathcal{C}(U)$ est un anneau de Dedekind, donc $M(U)$ s'écrit comme un produit libre d'idéaux premiers dans A. Autrement dit $M(U)$ correspond sur U au faisceau associé à un diviseur restreint à U. On peut recoller les diviseurs sur un recouvrement ouvert de $\mathcal{C}$ car la décomposition d'un idéal fractionnaire en facteurs premiers sur un anneau de Dedekind est unique.

Donc on a obtenu une correspondance bijective entre diviseurs de $\mathcal{C}$ et sous-modules inversibles de $\mathrm{K}(\mathcal{C})$, cette correspondance envoie un diviseur principal (f) sur $f\mathcal{O}_\mathcal{C}$.

Or tout module inversible sur $\mathcal{C}$ est isomorphe à un sous-module inversible de $\mathrm{K}(\mathcal{C})$ et deux sous-modules inversibles de $\mathrm{K}(\mathcal{C})$ sont isomorphes si et seulement si ils différent par une fonction rationnelle. Autrement dit, l'identification canonique précédente donne lieu à une identification des modules inversibles à isomorphisme près au groupe $\mathrm{Pic}(\mathcal{C})$. Cet isomorphisme est compatible avec les lois de groupe sur $\mathrm{Pic}(\mathcal{C})$ et sur les modules inversibles (où la loi est donnée par le produit tensoriel). Autrement dit ce qu'on appelle usuellement le groupe de Picard correspond bien au groupe ici défini.

Si l'on revient à la définition, on voit que $\Gamma(\mathcal{C}, \mathcal{O}(D)$ est l'ensemble des fonctions rationnelles dont la multiplicité en P est plus grande que $-n_P$, autrement dit c'est l'ensemble des fonctions rationnelles telles que $(f) + D \geqslant 0$. Comme deux diviseurs principaux (f) et (g) sont égaux si et seulement si ils diffèrent d'un élément de $\Gamma(\mathcal{C}, \mathcal{O}_{\mathcal{C}}^{\star}) = k^{\star}$, on voit que le nombre de diviseurs effectifs linéairement équivalents à D a pour dimension $\dim_k \Gamma(\mathcal{C}, \mathcal{O}(D)) - 1 := l(D) - 1$. On notera $|D|$ l'ensemble des diviseurs effectifs linéairement équivalents à D.

En particulier si $l(D) \neq 0$ (i.e. le faisceau associé à D a des sections globales) alors D est équivalent à un diviseur effectif, donc $\deg D \geqslant 0$ (car deux diviseurs équivalents ont le même degré). Si de plus $\deg(D) = 0$, D est équivalent à (1) le seul diviseur de degré 0 effectif.

Connaître $l(D)$ nous aiderait donc pour trouver le nombre de manière que l'on a pour représenter un point de la Jacobienne. C'est l'objet du théorème de Riemann-Roch.

3.4 Riemann-Roch

Soit $\mathcal{C}$ une courbe. Le genre arithmétique de $\mathcal{C}$ est par définition $p_a(\mathcal{C}) = \dim_k H^1(\mathcal{C}, \mathcal{O}_{\mathcal{C}})$. Il coincide avec le genre géométrique[1] $p_g(\mathcal{C})$ car $\mathcal{C}$ est supposé lisse. On notera ce nombre g et on l'appellera genre de $\mathcal{C}$.

Exemple 21: Les courbes elliptiques sont les courbes de genre 1. En effet pour une courbe lisse définie par un polynôme homogène de degré d, le genre de la courbe est $g = (d-1)/2$

Si $k = \mathbf{C}$, le genre de $\mathcal{C}$ est simplement son genre vu comme surface différentielle réelle, c'est à dire son nombre de « trous ».

Théorème 22 (Riemann-Roch):

(i) Si D est un diviseur de $\mathcal{C}$, alors $\dim_k H^0(\mathcal{C}, \mathcal{O}_D) - \dim_k H^1(\mathcal{C}, \mathcal{O}_D) = \deg D + 1 - g$

(ii) Il existe un diviseur positif K sur $\mathcal{C}$ de degré $2g-2$ tel que pour tout diviseur D, $H^1(\mathcal{C}, \mathcal{O}_D)$ est isomorphe à $H^0(\mathcal{C}, \mathcal{O}(K-D))$.

En combinant ce qui précède, on obtient

$$l(D) - l(K - D) = \deg D + 1 - g$$

Ceci permet de monter que pour une courbe elliptique $\mathcal{C}$, il y a bijection entre la jacobienne de $\mathcal{C}$ et les points de la courbe. En effet si on choisit un point P_0 de $\mathcal{C}$ (typiquement on prend le point à l'infini), on a un morphisme de $\mathcal{C}(k) \to \mathrm{Jac}(\mathcal{C}(k))$ en envoyant P sur la classe de $P - P_0$. Pour monter qu'on a un isomorphisme, il suffit de montrer que si D est un diviseur de 0, il existe un unique point $P \in \mathcal{C}(k)$ tel que $D \sim P - P_0$ On applique Riemann-Roch à $D + P_0$ et on obtient

$$l(D + P_0) - l(K - D - P_0) = 1 + 1 - 1$$

[1] Que l'on peut définir comme le genre arithmétique d'une courbe lisse birationnelle à $\mathcal{C}$

Mais $degK = 2g-2 = 0$, donc $deg(K-D-P_0) = -1$ et $l(K-D-P_0) = 0$. Donc $l(D+P_0) = 1$, et $\dim_k |D + P_0| = 0$. Il y a donc un unique diviseur effectif P équivalent à $D + P_0$, il est de degré 1 donc c'est un point.

On va montrer sur un exemple comment fonctionne en pratique la correspondance (c'est à dire on va la montrer sans passer par Riemann-Roch), ce qui nous permettra au passage de vérifier que les deux lois de groupes coincident bien.

Soit donc $\mathcal{C}$ la courbe elliptique donnée par $y^2 = x^3 - x$ (ou $zy^2 = x^3 - xz^2$ en projectif). $\mathcal{C}$ est une sous-variété fermée de $\mathbf{P}^2_k$. Si $\mathcal{L}$ est un faisceau inversible sur $\mathbf{P}^2_k$, son tiré en arrière sur $\mathcal{C}$ est également inversible, et deux faisceaux inversibles isomorphes restent isomorphes quand on tire en arrière. En gardant à l'esprit la seconde caractérisation du groupe de Picard, on voit qu'on a définit un morphisme de $\mathrm{Pic}(\mathbf{P}^2_k) \mapsto \mathrm{Pic}(\mathcal{C})$.

Notons $P_0 = (0, 1, 0)$ le point infini. C'est un point d'inflexion, donc la ligne $z = 0$ rencontre la courbe en le diviseur $3P_0$. Si on prend une ligne quelconque qui rencontre la courbe en le diviseur $D = P + Q + R$ (avec multiplicités), comme deux lignes définissent le même diviseur dans $\mathrm{Pic}(\mathbf{P}^2_k)$, il en va de même de leur tiré en arrière qui n'est autre que le diviseur qu'elles définissent sur la ligne. Ainsi $P+Q+R \sim 3P_0$, soit $P-P_0+Q-P_0+R-P_0 \sim 0$, on retrouve bien la loi de groupe issue des points de la courbe.

On peut vérifier élémentairement que $P \mapsto P - P_0$ donne bien une bijection de $\mathcal{C}(k)$ sur $\mathrm{Jac}(\mathcal{C})$. En effet, si $P - P_0 \sim Q - Q_0$, alors $P \sim Q$ mais il est connu que si deux points sur une courbe sont linéairement équivalents, la courbe est rationnelle (c'est à dire birationnelle à $\mathbf{P}^1_k$), donc de genre 0. Enfin pour la surjectivité, si D est un diviseur de degré 0, on peut l'écrire $D = \sum n_i(P_i - P_0)$, si l'un des n_i est négatif, en remplaçant P_i par son symétrique Q_i par rapport à l'axe des x, on peut se ramener à n_i positif (puisque $P_0 + P_i + Q_i \sim 3P_0$). Enfin, si les n_i sont positifs et qu'il y en a deux non nuls, correspondant à P et Q, alors la droite passant par P et Q intersecte $\mathcal{C}$ en un troisième point R et l'on a $P + Q + R \sim 3P_0$, soit $(P-P_0)+(Q-Q_0) \sim (T-T_0)$ et par un nombre fini d'étapes on se ramène à un diviseur de la forme $P - P_0$.

3.5 La variété jacobienne

On a vu que la Jacobienne d'une courbe est un groupe. En fait on peut montrer qu'elle est représentée par un schéma en groupe, i.e. il existe une variété projective sur k dont les points correspondent aux éléments de la Jacobienne et tels que la loi de groupe sur les points induite par la structure de groupe sur la Jacobienne est algébrique.

Plus précisément, soit X une courbe. Si T est un schéma sur k, on définit $\mathrm{Pic}^0(X \times T)$ comme étant le sous-groupe de $\mathrm{Pic}(X \times T)$ des faisceaux inversibles dont la restriction à chaque fibre X_t est de degré 0. On note $\mathrm{Pic}^0(X/T)$ le quotient de $\mathrm{Pic}^0(X \times T)$ par les faisceaux inversibles sur T tirés en arrière sur $X \times T$. On peut voir $\mathrm{Pic}^0(X/T)$ comme des familles de faisceaux inversibles de degrés 0 sur X paramétrées par T.

Alors le foncteur $Pic^0(X/T)$ est représentable par un schéma J de type fini sur k. C'est à dire qu'on a un élément $\mathcal{L} \in \mathrm{Pic}^0(X/J)$ tel que pour tout schéma T de type fini sur k et $\mathcal{M} \in \mathrm{Pic}^0(X/T)$ il existe un unique morphisme $f : T \mapsto J$ tel que $\mathcal{M} = f^\star\mathcal{L}$.

La propriété universelle de J montre que ses points fermés sont en bijections avec $\mathrm{Pic}^0(X)$, que J est un schéma en groupe, qu'elle est propre sur k (donc projective), lisse et de dimension g (son espace tangent en 0 étant $H^1(X, \mathcal{O}_X)$).

En particulier, si $k = \overline{\mathbf{F}}_q$, on voit que les points $\mathbf{F}_q$ rationnels de la jacobienne sont en

nombre fini.

4 Algorithmes de comptage de points

Pour toute courbe $\mathcal{C}$ définie sur un corps $\mathbf{F}_q$ (lisse, projective, ...) on sait construire un groupe associé $\mathrm{Jac}(\mathcal{C})$, qui est fini si on regarde ses points sur $\mathbf{F}_q$ (ou une extension finie de $\mathbf{F}_q$).

On espère que ce groupe a de bonnes propriétés cryptographiques en terme de logarithme discret. Une condition indispensable pour cela est que le groupe soit divisible par un grand nombre premier (voir l'algorithme de Pohlig-Hellmann). Pour le vérifier il nous faut donc calculer son cardinal. On va voir que cela revient au même que de calculer le nombre de points sur la courbe directement, au moins en genre $g \leqslant 2$.

4.1 Fonction zêta

On note N_k le nombre de points $\mathbf{F}_q^k$ rationnels de $\mathcal{C}$. La fonction zêta de $\mathcal{C}$ est alors

$$Z(t) = \exp\left(\sum_{k \geqslant 1} N_k \frac{t^k}{k}\right)$$

Les conjectures de Weil nous disent que

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

où $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$ est un polynôme de degré $2g$ vérifiant $a_0 = 1$, $a_{2g} = q^g$ et $a_{2g-i} = q^{g-i} a_i$ pour $0 \leqslant i \leqslant g$ et tel que les inverses de ses racines sont de module $\sqrt{(}q)$. En particulier $|a_i| \leqslant \binom{2g}{i} q^{i/2}$.

$\mathrm{Jac}(\mathcal{C})$ étant définie sur $\mathbf{F}_q$, le morphisme de Frobenius $x \mapsto x^q$ laisse stable $\mathrm{Jac}(\mathcal{C})$. Il se trouve que son polynôme caractéristique χ_π est le polynôme réciproque de L. On en déduit que le nombre de $\mathbf{F}_q$ points dans la jacobienne (égal à $\chi_\pi(1)$ se déduit de $Z(t)$. Réciproquement, si l'on connaît $\chi_\pi(1)$ et que le genre est $\leqslant 2$, la forme des coefficients de L permet de retrouver Z.

4.2 L'algorithme de Schoof

Soit A une variété abélienne de dimension g définie sur $\mathbf{F}_q$ pour laquelle on cherche à calculer le polynôme caractéristique χ_π du Frobenius.

Soit l un nombre premier différent de la caractéristique p de k. Alors le groupe des points de l-torsion de A, que l'on note $A[l]$ a une structure de $\mathbf{Z}/l\mathbf{Z}$-espace vectoriel de dimension $2g$, sur lequel le Frobenius agit de manières $\mathbf{Z}/l\mathbf{Z}$ linéaire. Le polynôme caractéristique de cette restriction de l'endomorphisme de Frobenius est alors $\chi_\pi(t) \mod l$.

L'algorithme de Schoof consiste à étudier l'action du Frobenius sur les points de l-torsion pour suffisamment de l de manière à déduire χ_π par restes chinois. Le plus grand coefficient de χ_π a un nombre de chiffres de l'ordre de $O(g \log q)$, il nous faut donc considérer environ $O(g \log q)$ nombres premiers l de taille $O(g \log q)$.

Le problème principal vient du fait que l'on ne sait pas a priori exhiber la structure de $\mathbf{Z}/l\mathbf{Z}$-espace vectoriel de $A[l]$, ce qui oblige à travailler sur tous les points de $A[l]$ (soit l^{2g} points) au lieu d'une base.

Décrire ces l^{2g} points nécessite un polynôme $f(X)$ de degré au moins l^{2g}, donc de taille environ $l^{2g}\log q$. Pour trouver le polynôme caractéristique de l'action de π, il nous faut calculer l'action de π sur les points de $A[l]$ ce qui se traduit par un calcul de type $X^q \mod f(X)$. Ceci nous coûte $O(\log q\,\mathrm{M}(l^{2g}\log q)$ où $\mathrm{M}(n)$ représente le temps de calcul nécessaire pour calculer le produit de deux polynômes de degré n, $\mathrm{M}(n) = O(n\log n\log\log n)$ si l'on utilise une transformée de Fourrier rapide. Il reste aussi à faire un peu d'algèbre linéaire pour trouver le polynôme caractéristique, mais on peut la négliger par rapport aux autres opérations.

Au final on s'attend à faire cette étape en $O(l^{2g}\log^2 q)$ opérations au mieux (en négligeant certains termes en $\log\log$), avec l de taille $O(g\log q)$, et on doit répéter cette étape environ $O(g\log q)$ fois. D'où un coût au mieux en $O(g^{1+2g}(\log q)^{2g+3})$.

Dans le cas des courbes elliptiques, l'algorithme de Schoof donne bien un algorithme en $O((\log q)^5)$, mais pour les courbes de genre 2, le meilleur algorithme que l'on connaît est en $O((\log q)^8)$ alors que l'on espérait du $O((\log q)^7)$. Cela vient de la difficulté à décrire efficacement $A[l]$.

Comme le coût exponentiel de l'algorithme vient de la grande taille de $A[l]$, on peut chercher à travailler dans un sous-espace de $A[l]$ de dimension inférieure qui permet quand même d'extraire de bonnes informations sur χ_π. C'est ce genre d'améliorations qu'ont apportées Atkin et Elkies à l'algorithme de Schoof dans le cas elliptique pour former l'algorithme SEA, qui est de complexité heuristique $O\left((\log q)^4\right)$.

C'est ce genre de méthodes que j'aimerais adapter au genre 2 dans ma thèse.

Références

[CF] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Lecture Note Series 230.

[Eis] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.*

[Gau] Pierrick Gaudry. Algorithmes de comptage de points d'une courbe définie sur un corps fini. Prépublication.

[Har] Robin Hartshorne. *Algebraic Geometry.*

[Kob] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Second edition.

[Las] Yves Laszlo. Introduction à la géométrie algébrique. Polycopié de cours de M2.

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, École Polytechnique, 1997.

[Per] Daniel Perrin. *Géométrie Algébrique, une introduction.*

Mémoire de M2
Classification des groupes de réflexions complexes

Damien Robert
Réalisé sous la direction de Michel Broué

4 Octobre 2006

Table des matières

Introduction

Ce mémoire a pour but de parvenir à la classification (à conjugaison près) des groupes de réflexions complexes.

État de l'art

Si V un espace vectoriel complexe, un groupe de réflexions G est un sous-groupe de $\mathrm{GL}(V)$ engendré par des réflexions. Il est dit réel (resp. rationnel) si il existe une base de V dans laquelle les matrices des éléments de G sont à coefficients réels (resp. rationnels), si ce n'est pas le cas G sera dit complexe. Les groupes de réflexions rationnels (que l'on appelle aussi groupes de Weyl) apparaissent dans la classification des groupes algébriques ou des groupes de Lie. Cependant, lorsqu'on veut étudier plus en détails les groupes algébriques (par exemple étudier leurs représentations), on a besoin d'utiliser les groupes de réflexions complexes.

Leur classification fut effectuée par Shephard et Todd dans [ST54]. Ils donnent directement la classification des groupes de réflexions complexes. Pour classer les groupes de réflexions complexes primitifs, ils remarquent que si $G \subset \mathrm{GL}(V)$ est un groupe de réflexions complexe, quand on regarde son action dans $\mathbf{P}V$, il donne lieu à un groupe de « collineations » (des transformations de l'espace projectif qui conservent la colinéarité) engendré par des « homologies » (ou « collineations » centrales, à savoir des « collineations » qui laissent stables des hyperplans de l'espace projectif et d'ordres fini). Ils s'appuient ensuite sur des résultats précédents disséminés dans la littérature qui ont permis de classifier de tels groupes de « collineations », puis ils remontent aux groupes de réflexions : une matrice représentant une homologie à pour vecteurs propres $\lambda, \ldots, \lambda, \mu$ ($\lambda, \mu \neq 0$ et $\lambda \neq \mu$) et on peut normaliser une telle matrice d'une unique manière si $\dim V \geqslant 3$ pour obtenir une matrice de réflexion (en multipliant par λ^{-1}). Le cas $\dim V = 2$ est un peu plus compliqué puisqu'on peut normaliser en multipliant par λ^{-1} ou μ^{-1} et Shephard et Todd étudient ce cas à part.

À partir de la classification, ils constatent une propriété remarquable des groupes de réflexions (qui explique peut-être le fait qu'ils apparaissent dans beaucoup de domaine des mathématiques) : un groupe fini G est un groupe de réflexions si et seulement si son action sur $\mathrm{S}(V)$ a pour invariants une algèbre de polynômes. La classification effectuée par Shephard et Todd est assez insatisfaisante car la preuve est complètement extrinsèque aux groupes de réflexions (on se ramène à des groupes que l'on connaît mieux), et surtout complètement éparpillée dans la littérature. Or il se trouve que depuis on a trouvé une preuve intrinsèque du théorème caractérisant les

groupes de réflexions en fonction de leurs invariants (voir [Bou68]), ce qui donne un espoir pour trouver une preuve de la classification utilisant la géométrie des groupes de réflexions complexes pour se ramener à un problème purement combinatoire, à la manière de la classification des groupes de réflexions réels, où l'étude des chambres permet par exemple facilement de montrer qu'un tel groupe est un groupe de Coxeter (avec comme système générateur les réflexions fixant les murs d'une chambre donnée, on renvoie encore à [Bou68] pour plus de détails).

C'est justement ce que fait Cohen dans [Coh76], où en généralisant les outils utilisés dans la classification des groupes de réflexions réels (graphes de Coxeter et systèmes de racines), il parvient à obtenir la classification des groupes de réflexions complexes de manière plus « intrinsèque » que Shephard et Todd. Cependant, il faut noter que la classification est plus compliquée dans le cas réel, car il n'y a pas l'équivalent des chambres et des murs. Du coup, il est difficile de savoir exactement quelles informations mettre dans un graphe pour généraliser les graphes de Coxeter. Dans sa preuve Cohen choisit de mettre des informations redondantes (plusieurs graphes correspondent au même groupe), ce qui rend le traitement combinatoire de ces graphes bien plus complexe. En fait, à l'instar de Shephard et Todd, il est obligé d'invoquer un théorème (de Blichfeldt) extrinsèque aux groupes de réflexions pour finir la classification. On renvoie aux Chapitres 4 et 5 pour plus de détails à ce sujet.

Ainsi, si la preuve de Cohen est une amélioration par rapport à la preuve originale de Shephard et Todd, elle n'est pas encore complètement satisfaisante. Récemment, des nouvelles manières de représenter les groupes de réflexions ont été introduites (voir [BMR98] et [Bro00]), mais elles n'ont pas encore abouti à une nouvelle preuve.

Plan et commentaire

Dans ce mémoire donc, nous suivons la preuve de Cohen. Dans le Chapitre 1, nous donnons la définition des groupes de réflexions complexes, et rappelons rapidement les principaux résultats à leurs sujets (même si tous ne nous serviront pas par la suite) pour donner une idée des méthodes que l'on a pour les étudier. Dans le Chapitre 2, nous commençons la classification proprement dite en classifiant tous les groupes imprimitifs (tâche relativement aisée, qui ne nécessite pas l'utilisation des outils introduits dans le Chapitre 4). Il reste à classifier les groupes de réflexions primitifs, or il se trouve que les outils utilisés par Cohen ne sont vraiment efficaces qu'en dimension $\geqslant 3$. Ainsi, comme Shephard et Todd, nous traitons le cas des groupes de réflexions de dimension 2 à part, en utilisant un marteau pilon : on détermine tous les groupes finis de $\mathrm{GL}_2(\mathbf{C})$ puis on regarde lesquels sont des groupes de réflexions. Ce sera l'objet du Chapitre 3. Comme annoncé, on présente la généralisation par Cohen des outils qui permettent de traiter le cas réel au Chapitre 4, et nous nous en servons pour terminer la classification dans le Chapitre 5. C'est dans ce dernier Chapitre que nous donnons le théorème de Blichfeldt (Théorème 5.1) sur les groupes primitifs quelconques qui sert à restreindre les choix possibles pour un groupe de réflexions, afin d'aider à la classification. Comme il ne s'agit pas à proprement parler d'un théorème sur les groupes de réflexions, nous donnons sa preuve dans l'Appendice A.

Nous suivons de très près l'exposition donnée par Cohen dans [Coh76], en corrigeant les petites erreurs typographiques (et en essayant de ne pas trop en rajouter

nous-même...) ainsi qu'une erreur un peu plus sérieuse mais sans grandes conséquences dans le Lemme 4.19. Nous avons cependant considérablement développé les preuves données par Cohen qui se révèlent parfois assez elliptiques (on pourra ainsi comparer les preuves du Lemme 2.10, de la Proposition 2.12, du Théorème 4.20 avec les preuves originales). Nous avons également énoncé quelques résultats triviaux sur les groupes de réflexions dont se sert Cohen sans les expliciter (il s'agit essentiellement du Chapitre 1, notamment la section 1.3). Il en va de même pour les résultats trouvés par Cohen : nous explicitons certaines de leurs conséquences qui servent par la suite mais que Cohen n'énonce pas forcément (voir par exemple le Lemme 4.13, le Lemme 4.28 et le Corollaire 4.30). Enfin, nous avons donné la preuve du théorème de Blichfeldt dans l'Appendice A, et développé un peu sur comment déterminer tous les sous-groupes finis de $\mathrm{GL}_2(\mathbf{C})$ (Chapitre 3).

On trouvera également au début de chaque section un court laïus qui sert à introduire l'objectif de cette section, et les moyens pour y parvenir.

Remerciements

Je remercie évidemment mon directeur de stage, Michel Broué, tout d'abord pour son magnifique cours sur les groupes de réflexions, qui m'a donné envie de faire mon mémoire sur ce sujet, mais aussi pour sa gentillesse et sa disponibilité à me recevoir malgré son emploi du temps chargé. Je tiens également à remercier David Bessis, qui n'a pas hésité à prendre du temps pour me voir et répondre à mes questions. J'ai également beaucoup profité du cours d'introduction à GAP ([GAP06]) de Jean-Michel, ainsi que de son cours en ligne ([Mic04]), et des TDs de Vincent Beck ([Bec06]). Je souhaiterais également remercier Laurence Dreyfus qui s'occupe du M2 Méthodes Algébriques et aide beaucoup les élèves pour toutes les formalités administratives, ainsi que tous les professeurs du M2 pour leurs cours très intéressants. Enfin je remercie mes collègues et amis de l'École Normale Supérieure pour les moments passés ensembles et les enrichissantes conversations.

Chapitre 1

Groupes de réflexions complexes, définitions et premières propriétés

1.1 Définition d'un groupe de réflexions complexe

Soit V un espace vectoriel complexe de dimension n, que l'on supposera muni d'un produit scalaire $(\cdot\,|\,\cdot)_V$.

Définition 1.1 (pseudo-réflexion): Un élément $g \in \mathrm{GL}(V)$ est une (pseudo)-réflexion s'il est d'ordre fini et stabilise un hyperplan de V.

Remarque 1.2: Comme g est d'ordre fini d, il est diagonalisable. Il s'écrit donc dans une base de V comme

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & \zeta \end{pmatrix}$$

où ζ est une racine primitive d^{ieme} de l'unité. Les vecteurs propres de g associés à ζ sont appelés les racines de g.

On remarque que g est à coefficient réel (dans une base de V) équivaut à g d'ordre 2 (et dans ce cas g est une vraie réflexion).

Par la suite, on parlera de réflexions à la place de (pseudo)-réflexions, et on précisera qu'on a une réflexion réelle, ou d'ordre 2 pour parler d'une vraie réflexion. Le lemme suivant est trivial, mais nous sera bien utile.

Lemme 1.3: *Soit W un sous-espace vectoriel de V stable par g. Alors soit W est fixé par g, soit il contient une racine de g. Réciproquement, si l'un des deux cas se produit, alors W est stable par g.*

DÉMONSTRATION: $g_{|W}$ est diagonalisable. ■

Définition 1.4 (Groupe de réflexions): $G \subset \mathrm{GL}(V)$ est un groupe de réflexions s'il est engendré par des réflexions. Un sous-groupe de réflexions de G est un sous-groupe H de G qui est un groupe de réflexions. On note $\mathrm{Ref}(G)$ l'ensemble des réflexions de G et $\mathrm{Rac}(G)$ leurs racines.

Si $\dim V = n$, on dira que G est de dimension n

Définition 1.5 (terminologie): Si $G \subset \mathrm{GL}(V)$, on notera V^G l'ensemble des points fixes par G. Si $g \in G$, on notera $V^g = V^{\langle g \rangle}$ l'ensemble des points fixes de g (où $\langle g \rangle$ note le sous-groupe de G généré par g). Si $W \subset V$ est un sous-espace vectoriel, on dira qu'il est stable par G si $\forall g \in G, g.W \subset W$, et qu'il est fixe par G si $W \subset V^G$.

Remarque 1.6: Soit $G \subset \mathrm{GL}(V)$ un groupe de réflexions fini. Il est classique qu'on peut alors voir G comme un sous-groupe de $\mathrm{U}(V)$, quitte à le conjuguer (prendre une forme hermitienne définie positive et la moyenner par les éléments de G pour obtenir une forme hermitienne définie positive stable par les éléments de G : $(\cdot\,|\,\cdot)_G$. $(\cdot\,|\,\cdot)_G$ est conjugué à $(\cdot\,|\,\cdot)_V$, donc G est conjugué à un sous-groupe fini de $\mathrm{U}(V)$). Par la suite, quand on parle d'un groupe de réflexions $G \subset \mathrm{GL}(V)$, on supposera implicitement qu'il s'agit d'un sous-groupe fini de $\mathrm{U}(V)$.

Si $W \subset V$ est stable par G son orthogonal l'est aussi, ainsi G est complètement réductible[1]

Définition 1.7: Soit s une réflexion unitaire de racine a et de valeur propre non triviale ζ. On notera $s = s_{a,\zeta}$ et on a :

$$s_{a,\zeta}(x) = x - (1-\zeta)\,(a\,|a)^{-1}\,(x\,|a)\,a$$

Si $\zeta = \exp(2i\pi d^{-1})$, on note aussi $s_{a,\zeta} = s_{a,d}$. Enfin si $d = 2$, on notera $s_a = s_{a,2}$.

Remarque 1.8 (Comportement d'une réflexion par conjugaison): Soit $s = s_{a,\zeta}$ une réflexion (avec les notations de la Définition 1.7), et $u \in \mathrm{U}(V)$ une transformation unitaire. Alors $us_{a,\zeta}u^{-1} = s_{u.a,\zeta}$ est toujours une réflexion. Et les racines de usu^{-1} sont les images par u des racines de s.

Définition 1.9 (Groupe de réflexions réel): Soit G un groupe de réflexions. On dit que G est réel s'il fixe un $\mathbf{R}$-sev V_0 de V tel que l'application canonique $\mathbf{C}\otimes_{\mathbf{R}} V_0 \to V$ est bijective. Autrement dit, G est réel s'il existe une base de V telle que la matrice de tout élément de G dans cette base soit à coefficients réels.

Si G n'est pas réel, on dira que G est un groupe de réflexions complexe.

Remarque 1.10: Si G est un groupe de réflexions réel, toute réflexion de G est d'ordre 2. On peut montrer (cf. [Bou68]) que les groupes de réflexions réels sont exactement les groupes de Coxeter. On connaît donc la classification des groupes de réflexions réels ([Bou68]).

Réciproquement, si G est un groupe de réflexions dont toutes les réflexions sont d'ordres 2, pour qu'il soit réel, la Définition 1.7 montre qu'il faut et suffit qu'on puisse choisir pour toute réflexion s de G une racine a_s tel que $\left\{(a_s\,|a_{s'})_{s,s'\in \mathrm{Ref}(G)}\right\} \subset \mathbf{R}$ (car alors il suffit de prendre un système libre maximal parmi les $\{a_s\}$ et de le compléter par une base de V^G ; voir le Lemme 1.18, en fait il suffit même de trouver de telles racines a_{s_i} pour des réflexions qui engendrent G).

[1] Et l'intérêt de prendre un produit scalaire c'est que l'on a un moyen canonique d'obtenir un supplémentaire stable de W

La théorie des caractères nous donne la proposition suivante :

Proposition 1.11: *Soit G un groupe fini, ρ une représentation irréductible de G et χ son caractère. On pose*

$$v(\rho) = |G|^{-1} \sum_{g \in G} \chi(g^2)$$

Alors

$$v(\rho) = \begin{cases} 1 & \text{si } \rho \text{ est réel} \\ -1 & \text{si } \rho \text{ n'est pas réel, mais est conjugué à } \overline{\rho} \\ 0 & \text{sinon, i.e. si } \chi \text{ est à valeurs complexes} \end{cases}$$

Démonstration (Rapide): On sait qu'il existe un produit scalaire hermitien G-invariant sur V. De plus, χ est réel $\Leftrightarrow$ il existe une forme bilinéaire b G-invariante et non dégénérée sur V. Et ρ est réel $\Leftrightarrow$ il existe une forme bilinéaire symétrique b G-invariante et non dégénérée sur V. Enfin si V est irréductible, l'espace des formes bilinéaires G-invariantes est de dimension au plus 1, en particulier toute forme bilinéaire est nulle ou non dégénérée, et dans ce cas est soit symétrique, soit antisymétrique. Comme $C := |G|^{-1} \sum_{g \in G} \chi(g^2)$ est le produit scalaire de $\chi_{\mathrm{Sym}^2(V^\star)} - \chi_{\mathrm{Alt}^2(V^\star)}$ avec la représentation triviale 1_G de G, la théorie des caractères montre que C est la dimension des formes bilinéaires symétriques invariantes par G sur V moins celle des formes bilinéaires antisymétriques, et la proposition découle de ce qui précède. ■

Remarque 1.12: On sait que pour un groupe de réflexions, le deuxième cas ne peut se produire, car son corps de définition est donné par son caractère.

1.2 Invariants d'un groupe de réflexions

L'intérêt majeur qui pousse à étudier les groupes de réflexions, et par là à comprendre leur classification, vient de ce qu'ils ont une caractérisation algébrique extrêmement jolie, en termes d'invariants.

Définition 1.13: Soit $G \subset \mathrm{GL}(V)$ un groupe. Il agit sur $S = S(V)$ via $g.f : v \to f(g^{-1}.v)$. On note $R = S^G$ les invariants polynomiaux par cette action.

On a alors le théorème suivant, qui fut démontré par Shephard et Todd ([ST54]) en se servant de la classification des groupes de réflexions. Chevalley réussit à le démontrer sans se servir de la classification, voir pour une preuve [Bou68].

Théorème 1.14: *Les assertions suivantes sont équivalentes*

(i) G est un groupe de réflexions

(ii) R est une algèbre de polynômes, c'est à dire qu'il existe des polynômes homogènes $f_1, \dots f_n$ algébriquement indépendants qui engendrent R comme algèbre

(iii) Il existe $f_1, \dots f_n \in R$ des polynômes homogènes algébriquement indépendants tels que $|G| = \deg(f_1) \times \cdots \times \deg(f_n)$[1]

Si tel est le cas, soit I l'idéal homogène engendré par les f_i. Alors S/I est isomorphe à la représentation régulière de G.

On note d_i les degrés des f_i qui apparaissent dans le Théorème 1.14. On suppose que $d_1 \leqslant d_2 \dots \leqslant d_n$ Il est facile de voir que les d_i ne dépendent pas du choix des f_i, on les appelle les degrés caractéristiques de G.

Corollaire 1.15: *Soit G un groupe de réflexions irréductible et d_i ses degrés caractéristiques. Alors G est un groupe de réflexions réel si et seulement si $d_1 = 2$.*

DÉMONSTRATION: G est réel $\Leftrightarrow$ il existe une forme bilinéaire symétrique b G-invariante sur V et non dégénérée $\Leftrightarrow \mathrm{Sym}^2(V^\star)^G \neq \{0\}$ vu que V est irréductible. Mais comme $\mathrm{Sym}^2(V^\star) \simeq_G S^2(V)$, cela équivaut au fait qu'il y ait un polynôme invariant de degré 2 dans S. Comme V est irréductible, il n'y a pas de polynôme invariant de degré 1 dans S (sinon on aurait un vecteur stable par G), donc cela équivaut bien au fait qu'un élément de la base algébrique de R soit de degré 2. ■

Il y a encore plusieurs autres caractérisations équivalentes d'un groupe de réflexions, mais comme ce n'est pas le but de ce mémoire, nous ne détaillerons pas davantage.

On peut obtenir des informations numériques sur le groupe G grâce aux séries de Poincaré. Si G agit sur un espace vectoriel gradué $E = \bigoplus E_n$ avec E_n de dimension finie, on définit le caractère gradué de E par $\chi(g) = \sum_{n=0}^{+\infty} \chi_n(g) T^n$, où χ_n est le caractère de l'action de G sur E_n.

Les formules usuelles d'orthogonalité des caractères se conservent pour les caractères gradués. On obtient ainsi :

Lemme 1.16 (Molien): *Soit G un groupe de réflexions et χ un caractère irréductible de G, et χ' le caractère gradué de l'action de G sur S. Alors*

$$\mathrm{grdim}\, S^\chi = \langle \chi', \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \frac{\chi(g^{-1})}{\det(1 - gT)} = P_\chi(T) \prod_{i=1}^{n} \frac{1}{1 - T^{d_i}}$$

où P_χ est un polynôme, appelé le "fake degré" de χ.

DÉMONSTRATION: La première égalité vient de la théorie des caractères (gradués), la seconde vient de ce que $\chi'(g) = \deg(1 - gT)^{-1}$, enfin pour la dernière égalité d'après le paragraphe qui suit le Théorème 1.14 : $S \simeq S_G \otimes I$ pour l'action de G sur S, avec S_G isomorphe à la représentation régulière de G. Donc $S^\chi \simeq S_G^\chi \otimes I$ or $grdim I = \prod_{i=1}^{n} \frac{1}{1 - T^{d_i}}$. ■

En appliquant le Lemme 1.16 au caractère trivial, on obtient les résultats suivants :

[1] En fait, la Proposition 1.17 montre que $f_1, \dots f_n$ vérifient (ii) si et seulement si ils vérifient (iii)

Proposition 1.17: *Soit G un groupe de réflexions et $d_1, \dots d_n$ ses degrés caractéristiques. Alors*

(i) $|G| = d_1 d_2 \dots d_n$

(ii) Soit h le nombre de réflexions dans G. Alors $h = \sum_{i=1}^{n} d_i - 1$

(iii) $|\mathcal{Z}(G)| = \mathrm{pgcd}(d_1, \dots, d_n)$

Pour d'autres résultats obtenus en utilisant les séries de Poincaré (notamment la formule de Solomon qui généralise la Proposition 1.17), on pourra consulter les cours de Broué et ceux de Michel.

Notons que les résultats de cette section ne vont pas réellement servir pour la classification (à part peut-être pour calculer des informations numériques une fois qu'on a exhibé un groupe de réflexion donné, si l'on ne veut pas laisser [GAP06] faire le travail), donc nous ne développerons pas plus sur le sujet.

1.3 Sous-groupes de réflexions

1.3.1 Sous-groupes de réflexions fixant un sous-espace vectoriel de V

Soit $G \subset \mathrm{GL}(V)$ un groupe de réflexion. On change un peu la Définition 1.4 en disant que G est de dimension n lorsque $n = \dim(V^G)^\perp$ (ie la dimension de G est la dimension de tout supplémentaire stable par G des points fixes de V).

De même, on dit que G est irréductible (resp primitif) en dimension n, si G est irréductible (resp primitif) sur un (donc tous) supplémentaire de V^G stable par G.

On emploie cette terminologie pour pouvoir travailler dans $\mathbf{C}^\infty$ plus tard lorsqu'on cherchera les groupes de réflexions de toute dimension.

Lemme 1.18: *Soit $G \subset \mathrm{GL}(V)$ un groupe de réflexions engendré par $(s_1, \dots s_p)$. Alors $W = (V^G)^\perp$ est engendré par les racines des réflexions de G et même par les racines de $(s_1, \dots, s_p)$. Donc si on choisit une racine a_i pour s_i, on a :*

(i) $\dim G = \dim\langle a_1, \dots a_p\rangle$

(ii) Si $s \in G$ est une réflexion, toute racine de s est combinaison linéaire des (a_i).

DÉMONSTRATION: En effet, si s est une réflexion de G, et a une racine de s, alors $V^s = a^\perp$. Comme $V^G = \bigcap_{s \in \mathrm{Ref}(G)} V^s$, W est bien engendré par les racines des réflexions de G. En fait, on a même $V^G = V^{s_1} \bigcap \dots \bigcap V^{s_p}$, donc on a bien $W = \langle s_1, \dots, s_p\rangle$ ■

Définition 1.19: Soit $X \subset V$ un sous-ensemble. On note $G_X = \{g \in G, gx = x$ pour tout $x \in X\}$. Alors G_X est un sous-groupe de réflexions (théorème de Steinberg [Ste74]).

Définition 1.20: Soit $v \in V$ et $W = v^\perp$. Alors G_W est un groupe de réflexions[1], et $G_W \subset \mathrm{GL}(\mathbf{C}) = \mathbf{C}^\star$ donc G_W est un groupe fini cyclique.

[1]En fait le théorème de Steinberg appliqué à un sous-espace de codimension 1 est bien plus facile à montrer que dans le cas général, en effet si $g \in G - \{\mathrm{Id}\}$ fixe W, il stabilise son orthogonal $\mathbf{C}v$, donc est une réflexion

On note $o_G(v) = |(G_W)|$. C'est l'ordre du sous-groupe de réflexions cyclique de G engendré par les réflexions de G qui ont v pour racine.

Remarque 1.21: Ainsi, G est engendré par les réflexions $\{s_{a,o_G(a)}$, où a parcourt les racines de $G\}$. De plus, par la Remarque 1.8, o_G est invariant par G.

1.3.2 Décomposition en sous-groupes irréductibles

Soit $G \subset \mathrm{GL}(V)$ un groupe de réflexions[1]. On définit une relation d'équivalence sur les racines de G comme la cloture transitive de la relation $\sim$ telle que $v \sim w$ si et seulement si v et w ne sont pas orthogonales.

Soit $R = \bigsqcup_{i=1}^{m} R_i$ la décomposition des racines en classes d'équivalences, G_i le sous-groupe de réflexions de G engendré par les réflexions ayant des racines dans R_i, et V_i l'espace vectoriel engendré par R_i. Enfin on note V_R l'espace vectoriel engendre par les racines de G.

Proposition 1.22: *On a les assertions suivantes*

(i) V_i *est stable par* G *et* G_i *(donc* G*) est irréductible sur* V_i

(ii) $V = \bigoplus_{i=1}^{m} V_i \oplus V^G$

(iii) $G = G_1 \times G_2 \times \cdots \times G_n$

On se servira du lemme trivial suivant

Lemme 1.23: *Soit* g *une réflexion unitaire de racine* v*.* g *laisse stable* $W \subset V$ *si et seulement si* $w \in W \bigcup W^{\perp}$*.* g *laisse fixe* W *si et seulement si* $v \in W^{\perp}$*. En particulier,* g *fixe* $w \in V$ *si et seulement si* $(v\,|w) = 0$*.*

Démonstration (du lemme): Cela vient immédiatement du fait que g est unitaire donc stabilise W si et seulement si il stabilise $W^{\perp}$, que $V = W \oplus W^{\perp}$ et du Lemme 1.3. ■

Démonstration (de la proposition):

(i) Par le Lemme 1.23 on remarque déjà que G_i agit trivialement sur $V = \bigoplus_{j \neq i} V_i$- $\oplus\, V^G$. Maintenant soit $s \in G_i$ une réflexion de racine v. Si $w \in V_i$ est une racine d'une réflexion t de G, alors $s(w)$ est une racine de $sts^{-1} \in G$, de plus $(s(w)\,|v) = (w\,|s(v)) \neq 0$ donc $s(v) \in G_i$. Donc V_i est stable par G_i et est laissé fixe par les G_j, $j \neq i$. Or si $g \in G$ est une réflexion, g appartient à l'un des G_l, or comme G est un groupe de réflexions, G est engendré par les G_l, donc laisse stable V_i.

V_i est irréductible car sinon on aurait une décomposition non triviale $V_i = W \oplus W^{\perp}$ Or W (et $W^{\perp}$) contient au moins une racine de G_i, sinon il serait invariant par G_i, or c'est absurde car V_i est généré par des éléments non invariants[2]. Donc on a exhibé deux racines orthogonales dans V_i, ce qui contredit la définition de R_i.

[1] Rappelons que l'on suppose G fini, et par là qu'on peut supposer de plus $G \subset \mathrm{U}(V)$

[2] En effet si v est racine d'une réflexion g, alors par définition v est un vecteur propre associé à une valeur propre non triviale de g, donc n'est pas stabilisé par g

(ii) On a $V_R = \bigoplus_{j\neq i} V_i$, et par le même raisonnement que pour V_i, aucun élément de V_R n'est fixe par G. On en déduit que $V_R^\perp = V^G$.
Enfin on a $V_i \bigcap \sum_{j\neq i} V_j = 0$ car V_i est stable par G_j pour tout $j \neq i$ alors qu'aucun vecteur de V_j n'est stable par G_j.

(iii) Pour terminer, on sait déjà que G est engendré par les G_i, et le même raisonnement nous montre que $G_i \bigcap \prod_{i\neq j} G_j = \{Id\}$ si $i \neq j$, ce qui achève de montrer la proposition.

Corollaire 1.24 (Extension d'un groupe irréductible): *Soit G un groupe de réflexions de V irréductible en dimension r (c'est à dire que si $W = (V^G)^\perp$, $\dim W = r$ et G est irréductible dans W). Soit s une réflexion de $\mathrm{U}(V)$. Alors $\langle G, s\rangle$ est irréductible de dimension $r+1 \Leftrightarrow$ s ne stabilise pas W (ou de manière équivalent s ne stabilise pas V^G) $\Leftrightarrow$ si a est racine de s, $a \notin W \bigcup V^G$.*

DÉMONSTRATION: Rappelons que W est engendré par les racines de G. Si a est une racine de s, $G' = \langle G, s\rangle$ est de dimension $r+1$ si et seulement si $a \notin W$.

La deuxième équivalence vient du Lemme 1.23. Pour la première équivalence, si G' est irréductible de dimension $r+1$, comme G stabilise W, s ne le stabilise pas car $\dim W = r$. Réciproquement, si s ne stabilise pas W, on a vu que G' est de dimension $r+1$ et que si a est une racine de s, $a \notin W^\perp$. a n'est donc pas orthogonale à toutes les racines de G, et G' est irréductible par la Proposition 1.22. ■

Ainsi on a décomposé G en sous-groupes irréductibles. Cela montre qu'il suffit de se restreindre à des groupes de réflexions irréductibles pour obtenir la classification.

1.3.3 Éléments réguliers

On termine cette section par un théorème de Springer concernant les éléments réguliers d'un groupe de réflexions. Encore une fois ce résultat ne va pas nous servir pour la classification, sauf éventuellement pour simplifier les calculs une fois que l'on a exhibé un groupe de réflexions donné.

Définition 1.25: Un élément $v \in V$ est dit régulier s'il n'est fixé par aucune réflexion de G. (c'est à dire $G_v = 1$ avec les notations de la Définition 1.19). Un élément g de G est dit régulier s'il a un vecteur propre régulier.

Théorème 1.26 (Springer [Spr74]): *Soit ζ une racine primitive d^{ieme} de l'unité. Soit $g \in G$ un élément régulier ayant v comme vecteur propre régulier et ζ comme valeur propre associée. Soit W l'espace propre correspondant. Alors*

(i) g est d'ordre d, et les autres vecteurs propres de g sont $\zeta^{1-d_1}, \ldots, \zeta^{1-d_n}$.

(ii) $\dim W = \mathrm{Card}\,\{i, d \text{ divise } d_i\}$

(iii) La restriction à W du centralisateur de g dans G donne un groupe de réflexions dont les degrés sont les d_i divisibles par d

(iv) La classe de conjugaison de g consiste en les éléments de G qui ont $\dim W$ *valeurs propres ζ*

1.4 Caractères linéaires d'un groupe de réflexions

Avant de commencer la classification proprement dite, on va d'abord déterminer tous les caractères linéaires d'un groupe de réflexions, car cela nous sera utile pour la suite (par exemple pour trouver à quoi ressemble l'abélianisé d'un groupe de réflexions).

Soit $a \in V - \{0\}$, on note l_a le polynôme linéraire $l_a(x) = (x\,|a)$.

Lemme 1.27: *Soit a et b des racines de G, ζ une racine de l'unité. On suppose qu'il existe $c \in \mathbf{C}^\star$ tel que $s_{a,\zeta}.l_b = cl_b$. Alors $c = 1$ ou $c = \zeta^{-1}$ et dans ce cas $a \in \mathbf{C}b$*

DÉMONSTRATION: En effet, cela revient à $s_{a,\zeta^{-1}}(b) = cb$, donc b est un vecteur propre de $s_{a,\zeta^{-1}}$ de valeur propre associée c. On a bien $c = 1$, ou $c = \zeta^{-1}$ et dans ce cas b est racine de $s_{a,\zeta^{-1}}$, donc proportionnel à a. ■

Soit $\sim$ la relation d'équivalence définie sur les racines de G par $a \sim b$ ssi a et b sont proportionnels. On prend un système de représentant unitaire pour chaque classe d'équivalence, et on note τ la fonction qui a une racine associe son représentant. Si a est une racine de $s \in \mathrm{Ref}(G)$, on note $a_s = \tau(a)$. Enfin on note $P = \{\mathbf{U}a, a \in \mathrm{Rac}(G)\}$ l'ensemble des classes d'équivalences de racines unitaires.

Soit O une orbite dans $\mathrm{Rac}(G)$, on définit $f_O \in S$ par $f_O = \prod_{x\in O} l_{\tau(x)}$. On définit de plus un caractère linéaire

$$\chi_O : G \to U \text{ par } \chi_O(g) = \prod_{a_{s_i}\in\tau(O)} (\det s_i)^{-1}$$

où $g = s_1 s_2 \dots s_r$ est une décomposition de g en réflexions de G.

Proposition 1.28:

(i) χ_O est bien défini et $g \in G$, $g.f_O = \chi_O(g) f_O$

(ii) Tout caractère linéaire de G est un produit de tels χ_O

DÉMONSTRATION:

(i) Il suffit de vérifier que si $s \in G$ est une réflexion de valeur propre ζ, alors

$$s.f_O = \begin{cases} f_0 & \text{si } a_s \notin \tau(O) \\ \zeta^{-1} f_O & \text{si } a_s \in \tau(O) \end{cases}$$

ce qui montrera au passage que χ_O est bien défini.

Soit $x_1, x_2, \dots x_r$ une orbite de s dans O, telle que $s(x_i) = x_{i+1}$ et $s(x_r) = x_1$ (pour simplifier les notations, on pose $x_{r+1} = x_1$). Il existe donc $c_i \in \mathbf{C}^\star$ tels que $s(\tau(x_i)) = c_i\tau(x_i)$. Soit $h = \prod_{i\leqslant r} l_{\tau(x_i)}$.

On obtient

$$s.h = \left(\prod_{i\leqslant r} \bar{c_i}\right) h \tag{1.1}$$

et

$$s^r(l_{\tau(x_1)}) = \left(\prod_{i\leqslant r} \bar{c}_i\right) l_{\tau(x_1)} \tag{1.2}$$

Si $\prod_{i\leqslant r} \bar{c}_i \neq 1$, alors s^r a $\tau(x_1)$ comme racine (par (1.2) et le Lemme 1.27), donc s aussi. Ainsi $h = l_{a_s}$ et donc par (1.1) $s.h = \zeta^{-1}h$. Or si l'on décompose O en orbite sous l'action de s, il y a au plus une orbite réduite à un multiple de a_s, ce qui conclut la preuve.

(ii) Si φ est un caractère non trivial de G, et soit $f \in S$ un polynôme homogène de degré minimal tel que $g.f = \varphi(g)f$ pour tout $g \in G$ (un tel polynôme existe par le Théorème 1.14). Soit $s \in G$ une réflexion telle que $\varphi(g) \neq 1$. Pour tout $v \in a_s^\perp$, on a $f(v) = f(s^{-1}v) = (s.f)(v) = \varphi(s)f(v)$, donc $f(v)$=0. Ainsi f est divisible par $l_{a_s} = (.\,|a_s)$, et donc par $l_{\tau(v)}$ pour tout v dans l'orbite de a_s par G. Donc f est divisible par f_0, et une induction immédiate permet de conclure. ■

Si O est une orbite de G dans V, alors $o_G(v)$ ne dépend pas de $v \in O$, on note ce nombre $o_G(O)$.

Corollaire 1.29: *$\frac{G}{[G,G]}$ est un produit direct de groupes cycliques d'ordres $o_G(O)$, où O parcourt les orbites par G de* Rac(G).

DÉMONSTRATION: $\frac{G}{[G,G]} \simeq \mathrm{Hom}(G, \mathbf{U})$ est engendré par les χ_O d'après la Proposition 1.28. Il reste à vérifier que si $O_1, O_2, \ldots O_m$ sont des orbites distinctes et $\lambda_1, \lambda_2, \ldots \lambda_m$ des entiers tels que $\chi_{O_1}^{\lambda_1}, \chi_{O_2}^{\lambda_2}, \ldots \chi_{O_m}^{\lambda_m} = 1$, alors $\chi_{O_1}^{\lambda_1} = \chi_{O_2}^{\lambda_2} = \ldots \chi_{O_m}^{\lambda_m} = 1$

Mais cela vient de ce que si $s \in \mathrm{Ref}(G)$ a une racine dans O_1 (et que s est d'ordre $o_G(O_1)$), alors χ_{O_1} agit fidèlement sur $< s_1 >$, et les $\chi_{O_i}(s) = 1$ si $i \neq 1$ (toujours d'après la Proposition 1.28) ■

Chapitre 2

Classification des groupes de réflexions imprimitifs

2.1 Introduction

Le but de ce chapitre est de déterminer tous les groupes de réflexions imprimitifs (mot que l'on va bientôt définir), tâche qui se révèle bien plus facile que la classification des groupes de réflexions primitifs. Ceci sera l'objet de la section 2.2, où l'on verra que les groupes de réflexions imprimitifs irréductibles forment une famille infinie $G(de, e, n)$ à 3 paramètres. Enfin dans la section 2.3 on utilisera cette classification pour obtenir des résultats lorsqu'un groupe de réflexions contient un sous-groupe de réflexions primitif ou imprimitif donné.

Dans la suite du Chapitre, on notera V un $\mathbf{C}$-espace vectoriel de dimension $n \geqslant 2$.

2.2 Structure des groupes de réflexions imprimitifs

Définition 2.1 (Groupes imprimitifs): Soit $G \subset \mathrm{GL}(V)$ un groupe. Il est dit imprimitif si l'on peut décomposer V en une somme directe $V = V_1 \oplus V_2 \oplus \cdots \oplus V_t$ de sous-espaces vectoriels non triviaux, tels que $\{V_i, 1 \leqslant i \leqslant t\}$ soit stable par G. On dit alors que les V_i forment un système d'imprimitivité de G.

G est dit primitif s'il n'est pas imprimitif. Comme un groupe fini est complètement réductible, si G est primitif, il est irréductible.

Remarque 2.2: Si on a une représentation $\rho : G \to \mathrm{GL}(V)$ irréductible, alors ρ est une représentation imprimitive si et seulement si $\rho = \mathrm{Ind}_H^G$ où $H = \mathrm{Stab}(V_1)$ (avec les notations de la Définition 2.1). On rappelle que $\mathrm{Ind}_H^G = \mathbf{C}[G] \otimes_{\mathbf{C}[H]} \cdot$ est le foncteur d'induction, adjoint à gauche du foncteur restriction : $\mathbf{C}[G]-\mathbf{MOD} \to \mathbf{C}[H]-\mathbf{MOD}$. On pourra consulter le Théorème A.1 et la Remarque A.2 pour plus d'informations.

Définition 2.3: Un polynôme $p \in S$ est dit semi-invariant s'il existe un caractère linéaire χ de G tel que $g.p = \chi(g)p$ pour tout $g \in G$

Proposition 2.4 (Structure des groupes de réflexions imprimitifs): *Soit G un groupe de réflexions irréductible et imprimitif dans V ($n = \dim V \geqslant 2$), et soit $(V_i)_{1\leqslant i\leqslant r}$ un système d'imprimitivité de G. Alors :*

(i) $\dim V_i = 1$ *et* $t = n$. *De plus il existe des polynômes linéaires homogènes distincts $l_1, \dots l_n$ tels que $l_1 l_2 \dots l_n$ soit un polynôme homogène semi-invariant de degré n.*

(ii) Si s est une réflexion de G, alors
- *soit $sV_i = V_i$ pour tout i, et il existe un j tel que les racines de s soient dans V_j*
- *soit il existe $i \neq j$ tel que $sV_i = V_j$, $sV_k = V_k$ si $k \neq i, j$, les racines de s sont dans $V_i \oplus V_j$ et s est d'ordre 2.*

(iii) Soit $\psi : G \to S_n$ le morphisme qui à $g \in G$ associe la permutation qu'il induit sur le système d'imprimitivité (V_i). Alors ψ est surjective et admet une section (dans la catégorie des groupes).

(iv) $V_i \perp V_j$ *si* $i \neq j$

(v) Si v est une racine d'une réflexion d'ordre 2 de G, et w une racine d'une réflexion d'ordre > 2 non proportionnelle à v, alors $|(v\,|w)| \in \left\{0, 2^{-1/2}\right\}$.

Démonstration:

(i) Supposons qu'il existe i tel que $\dim V_i > 1$. Comme G est irréductible il existe une réflexion $s \in G$ telle que $sV_i = V_j$ $(i \neq j)$. Comme $\mathrm{Fix}(s) = \mathrm{Ker}(s - \mathrm{Id})$ est de codimension 1, $\dim(V_j \bigcap V_i) > 0$, ce qui contredit $V_j \bigcap V_i = 0$. Pour établir la dernière partie de (i), il suffit de prendre un vecteur unitaire $a_i \in V_i$ et de prendre pour l_i le polynôme linéaire homogène définit par $l_i(a_i) = 1$ et $l_i(a_j) = 0$ si $i \neq j$ (en fait ((iv)) montre que $l_i = (\cdot\,|a_i)$). Comme $V_i = \mathbf{C}a_i$ et que les (V_i) forment un système d'imprimitivité de G, on vérifie immédiatement que $g.l_1 \dots l_n = \lambda l_1 \dots l_n$ où $\lambda \in \mathbf{C}^\star$.

(ii) Soit s une réflexion de G de racine unitaire a et valeur propre non triviale ζ. Si s stabilise chaque V_i, alors le Lemme 1.3 montre que a est dans l'un des V_j. Sinon, on peut supposer que s ne stabilise pas V_1. Par le Lemme 1.3, $(a\,|V_1) \neq 0$ et $a \notin V_1$. On peut supposer que $sV_1 = V_2$. Il existe $x_1 \in V_1 \setminus 0$ et $x_2 \in V_2 \setminus 0$ tel que $s(x_1) = x_2$. Il existe j tel que $s^2(x_1) \in V_j$. On a

$$x_2 = s(x_1) = x_1 - (1 - \zeta)\,(x_1\,|a)\,a \tag{2.1}$$

$$\begin{aligned} s^2(x_1) &= x_1 - (1 - \zeta^2)\,(x_1\,|a)\,a \\ &= x_2 - (1 - \zeta)\,(x_2\,|a)\,a \end{aligned} \tag{2.2}$$

(2.1) montre que $a \in (V_1 \oplus V_2) \setminus (V_1 \bigcup V_2)$. Donc $s^2(x_1) \in V_1 \oplus V_2$ et $j = 1, 2$. Mais (2.2) montre que $j \neq 2$ car $a \notin V_2$. Donc $s^2(x_1) = x_1$ et $\zeta^2 = 1$ i.e. $\zeta = -1$ et s est d'ordre 2. Si s ne stabilise pas V_i pour un $i > 2$, c'est à dire si $sV_i = V_j$, $j \neq i$ $(j > 2)$, le même raisonnement nous dit que $a \in (V_i \oplus V_j) \bigcap (V_1 \oplus V_2) = 0$ ce qui nous donne la contradiction cherchée.

(iii) Comme G est irréductible, pour tout $j > 1$, il existe une réflexion s_j telle que $sV_1 = V_j$. (ii) nous donne immédiatement que $\psi(s) = (1j)$. Donc G est surjectif. De plus la preuve de (ii) nous montre que l'on peut trouver $x_1 \in V_1, x_2 \in V_2, \dots x_n \in V_n$ tel que $s_j(x_1) = x_j$, $s_j(x_j) = x_1$ et $s_j(x_i) = x_i$ si $i \notin 1, j$. Donc la restriction de ψ au sous-groupe de réflexions $< s_2, \dots s_n >$ de G est un isomorphisme, d'où la section recherchée.

(iv) $(x, y) \mapsto \sum_{i=1}^{n} l_i(x)\overline{l_i(y)}$ définit un produit scalaire invariant par G (c'est le produit scalaire qui rend orthonormaux les (a_i)) : en effet $g.l_i = \lambda l_j$ avec $\lambda \in \mathbf{U}$ vu que (V_i) est un système d'imprimitivité et que g est unitaire, et $g.\overline{l_i} = \overline{\lambda} l_j$. Il est bien connu que l'espace des produits scalaires sur V invariants par G est de dimension 1 si G est irréductible, donc le produit scalaire ainsi définit est un multiple de $(\cdot\,|\,\cdot)$, et on a donc bien $V_i \perp V_j$.

(v) Soit w une racine d'une réflexion d'ordre > 2, alors par (ii) il existe i tel que $w \in V_i$. Si v est une racine d'une réflexion s d'ordre 2, alors soit $v \in V_j$ pour un j donné, et alors on a bien (v), soit par exemple $v \in (V_1 \oplus V_2) \setminus (V_1 \bigcup V_2)$. Si $j \neq 1, 2$, on a $(v\,|w) = 0$. On peut donc supposer $j = 2$ et $w = x_2$, on est dans la situation de (2.2) et si l'on fait le produit scalaire par x_2, on obtient :

$$0 = 1 - 2\,|(x_2\,|a)|^2$$

donc $|(x_2\,|a)| = 2^{-1/2}$. ■

Remarque 2.5: La preuve de Proposition (v) montre plus généralement que si v est une racine d'une réflexion d'ordre 2 de G, et $w \in V_i$ est non proportionnelle à v, alors $|(v\,|w)| \in \left\{0, 2^{-1/2}\right\}$

Si l'on ne spécifie pas une base de $\mathbf{C}^n$, lorsqu'on considère la matrice d'une application linéaire, cela sera par rapport à la base canonique $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$.

Définition 2.6: Soit Π_n le groupe des matrices de permutations $n \times n$. On note $\mathrm{A}(de, e, n)$ où $d, e \in \mathbf{N}^\star$ le groupe des matrices diagonales à coefficients dans $\mathbf{U}_{de}$ et dont le déterminant est dans $\mathbf{U}_d$[1]. Comme Π_n normalise $\mathrm{A}(de, e, n)$, on peut donc définir $\mathrm{G}(de, e, n) = \mathrm{A}(de, e, n) \rtimes \Pi_n$, c'est un sous-groupe du groupe des matrices monômiales.

On vérifie que $\mathrm{G}(de, e, n)$ est un groupe de réflexion imprimitif, avec comme système d'imprimitivité $(\mathbf{C}\varepsilon_i)$. En effet, on vérifie immédiatement que $\mathrm{A}(de, e, n) = \mathrm{A}(d, 1, n).\,\mathrm{A}(de, de, n)$ donc $\mathrm{G}(de, e, n) = \mathrm{G}(d, 1, n).\,\mathrm{G}(de, de, n)$. Or $\mathrm{G}(d, 1, n)$ est engendré par les matrices de transpositions $(1, i)$ (qui sont bien des réflexions) et par la matrice

$$\begin{pmatrix} e^{2i\pi/d} & 0 \\ 0 & \mathrm{Id} \end{pmatrix}$$

et $\mathrm{G}(de, de, n)$ est engendré par les matrices de transpositions et par la matrice

$$\begin{pmatrix} 0 & e^{-2i\pi/de} & 0 \\ e^{2i\pi/de} & 0 & 0 \\ 0 & 0 & \mathrm{Id} \end{pmatrix} j$$

[1]Ainsi $\mathrm{A}(de, e, n)$ est composé des matrices $(a_{ij})_{1 \leqslant i,j \leqslant n}$ où $a_{ij} = \zeta_{i,j}\delta_i^j$ avec $\zeta_{i,j}^{de} = 1$ et $\det(a_{ij})^d = 1$

(réflexion d'ordre 2 de racine $\varepsilon_1 - \exp(2\pi i/de)\varepsilon_2$). ♢

On posera $m = de$ pour alléger les notations.

Remarque 2.7: Le groupe symétrique pouvant être engendré par les transpositions $(12), (23), \dots ((n-1)n)$, c'est à dire des réflexions d'ordres 2 et de racine $\varepsilon_1 - \varepsilon_2, \dots, \varepsilon_{n-1} - \varepsilon_n$ on voit que $G(de, e, n)$ est engendré par $n+1$ réflexions (et même n réflexions si $e = 1, m$).

Théorème 2.8: *Soit $n \geqslant 2$ et soit G un groupe de réflexions irréductible et imprimitif de V. Alors G est conjugué*[1] *à un certain* $\mathrm{G}(de, e, n)$. *Réciproquement* $\mathrm{G}(de, e, n)$ *est irréductible si et seulement si $de > 1$ et $(de, e, n) \neq (2, 2, 2)$*

Démonstration:

– Soit donc un tel G. La Proposition 2.4 nous fournit une base orthonormale $e_1, e_2, \dots e_n$ telle que $V_i = \mathbf{C}e_i$ forme un système d'imprimitivité de G. De plus, pour tout $j > 1$ il existe une réflexion $s_j \in G$ telle que $s(e_1) = e_j$. Quitte à conjuguer G, on peut supposer que $e_i = \varepsilon_i$. Toujours d'après la Proposition 2.4, Π_n est un sous-groupe de G. Soit $d = o_G(e_1)$ c'est à dire d est l'ordre du sous-groupe de réflexions de G qui laisse $e_1^\perp$ invariant. Alors $\mathrm{A}(d, 1, n)$ est un sous-groupe de G.
Toujours d'après la Proposition 2.4, les réflexions de G qui ne sont pas dans $\mathrm{G}(d, 1, n)$ sont les réflexions $s' \in G$ telles que $s'(e_i) = \lambda e_j$ où $i \neq j$ et $\lambda \in \mathbf{U} \setminus 1$, avec $s'(e_k) = e_k$ si $k \neq i, j$. On peut supposer que $i = 1$ et $j = 2$ quitte à conjuguer par une permutation. Soit $s = s_2$ la permutation $(1, 2)$. Alors

$$ss' = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda^{-1} & 0 \\ 0 & 0 & \mathrm{Id} \end{pmatrix}$$

Donc λ est une racine de l'unité et $H = \{st$, où t est une réflexion telle que $tV_1 = V_2\}$ est un groupe cyclique fini d'ordre m. On vérifie que $d|m$ (considérer $s \begin{pmatrix} e^{2i\pi/d} & 0 \\ 0 & \mathrm{Id} \end{pmatrix} : V_1 \to V_2$). Ainsi si l'on pose $m = de$, $\mathrm{A}(de, de, n)$ est également un sous-groupe de G, donc $G \supset \mathrm{G}(de, e, n)$. Or tout réflexion s de G est dans $\mathrm{G}(de, e, n)$. C'est le cas si s a une racine dans V_1 (dans ce cas $s \in \mathrm{A}(d, 1, n)$, où si s envoit V_1 sur V_2 par définition de d et $m = de$. Mais par conjugaison par une permutation, on peut toujours se ramener à un de ces deux cas. Donc $G = \mathrm{G}(de, e, n)$

– On sait que $V = W \oplus W^\perp$ où $W = \mathbf{C}(e_1 + \dots + e_n)$ est la décomposition de w en somme d'irréductibles sous l'action de Π_n. Comme chaque représentation irréductible de Π_n n'apparaît qu'une fois dans V, c'est aussi la décomposition en composantes isotypiques. Ainsi les espaces non triviaux stables de V par Π_n sont W ou $W^\perp$. Ainsi si $\mathrm{G}(de, e, n)$ n'est pas irréductible, comme il contient Π_n, il fixe W (quitte à passer à l'orthogonal). Or pour que $\mathrm{A}(de, e, n)$ stabilise W, il faut que les coefficients diagonaux des éléments de $\mathrm{A}(de, e, n)$ doivent être

[1] Rappel : on cherche à trouver les groupes de réflexions à conjugaison près dans $\mathbf{U}(V)$

tous égaux. Il est facile de voir que cela impose $(de, e, n) \in \{(1, 1, n), (2, 2, 2)\}$. Réciproquement, il est évident que $\mathrm{G}(1, 1, n)$ et $\mathrm{G}(2, 2, 2)$ sont réductibles sur V. ■

Remarque 2.9:

(i) La liste des groupes de réflexions réels sera donnée dans Théorème 4.18. Les groupes de réflexions imprimitifs réels qui y apparaissent sont $\mathrm{W}(B_n)$ et $\mathrm{W}(D_n)$. L'action de $\Pi_n = \mathrm{G}(1, 1, n)$ sur $(\varepsilon_1 + \cdots + \varepsilon_n)^\perp$ représente $\mathrm{W}(A_{n-1})$ $(n \geqslant 2)$. $\mathrm{W}(A_n)$ est primitif.

(ii) On note $X_1, \ldots X_n$ les éléments $\varepsilon_1, \ldots \varepsilon_n$ dans S, on a alors $S = \mathbf{C}[X_1, \ldots, X_n]$. Les $(n-1)$ premiers polynômes symétriques en les $(X_i)^{de}$ (i.e. $X_1^m + \cdots + X_n^m$, $\sum i < j X_i^m X_j^m$, ..., $\sum i = 1^n \prod j \neq i X_j^m$) ainsi que $(X_1 X_2 \ldots X_n)^d$ sont invariants sous $\mathrm{G}(de, e, n)$, homogènes et algébriquements indépendants, de plus le produit de leur degré est égal à $e^{-1}(de)^n n! = |\mathrm{G}(de, e, n)|$. Ainsi le Théorème 1.14 montre que les degrés caractéristiques de $\mathrm{G}(de, e, n)$ sont $m, 2m, \ldots (n-1)m, dn$ et la Proposition 1.17 montre que $|\mathcal{Z}(\mathrm{G}(de, e, n))| = d \times \mathrm{pgcd}(e, n)$ Enfin le polynôme semi-invariant qui correspond à au système d'imprimitivité $\mathbf{C}\varepsilon_1, \ldots \mathbf{C}\varepsilon_n$ dans la Proposition 2.4(i) est $X_1 \ldots X_n$.

(iii) Le calcul des degrés caractéristiques de $\mathrm{G}(de, e, n)$ et le Corollaire 1.15 montrent que les groupes irréductibles imprimitifs réels sont $\mathrm{G}(2, 1, n) = \mathrm{W}(B_n) = \mathrm{W}(C_n)$ $(n \geqslant 2)$ et $\mathrm{G}(2, 2, n) = \mathrm{W}(D_n)$ $(n \geqslant 3)$

(iv) $\mathrm{G}(4, 4, 2)$ est conjugué à $\mathrm{G}(2, 1, 2)$ et se sont les seuls groupes conjugués parmis les $\mathrm{G}(de, e, n)$ irréductibles (celà se voit à l'aide de (ii) en regardants les polynômes invariants).

(v) Enfin, les caractères linéaires de $\mathrm{G}(de, e, n)$ sont déterminés par les orbites de G dans P (Rappel : $P = \{\mathbf{C}a,\ a \text{ racine de } G\}$ est la classe d'équivalence des racines de G). Or les racines de $\mathrm{G}(de, e, n)$ sont de deux sortes : les racines qui sont dans $\mathbf{C}\varepsilon_i$ (il n'y en a que si $d \neq 1$), qui donnent lieu à une orbite de longueur n. Et il y les racines qui sont dans $V_i \oplus V_j \setminus (V_i \bigcup V_j)$ qui sont des racines (de réflexions) d'ordre 2. Comme $\mathrm{G}(de, e, n) \supset \Pi_n$, on peut supposer que $i = 1, j = 2$ et que la racine correspond à la réflexion

$$s = \begin{pmatrix} 0 & \zeta & 0 \\ \overline{\zeta} & 0 & 0 \\ 0 & 0 & \mathrm{Id} \end{pmatrix}$$

s a pour racine $-\zeta\varepsilon_1 + \varepsilon_2$. Si $n \geqslant 3$, toutes les racines de ce type sont sur la même orbite car :

$$\begin{pmatrix} 0 & 0 & \mu & 0 \\ 0 & 1 & 0 & 0 \\ \overline{\mu} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{Id} \end{pmatrix} \begin{pmatrix} -\zeta \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -\overline{\mu}\zeta \\ 0 \end{pmatrix}$$

Ainsi on obtient une orbite de longueur $de \times n(n-1)/2$. Si $n = 2$, on a

$$\begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\zeta \\ 1 \end{pmatrix} = \begin{pmatrix} -\mu\zeta \\ 1 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & \mu \\ \overline{\mu} & 0 \end{pmatrix} \begin{pmatrix} -\zeta \\ 1 \end{pmatrix} \sim \begin{pmatrix} -\overline{\zeta}\mu^2 \\ 1 \end{pmatrix}$$

donc on a également une seule orbite de longueur m pour les racines de ce type, sauf si e est pair et d impair, dans ce cas on a deux orbites de longueurs $de/2$

2.3 Sous-groupes de réflexions primitifs

La classification des groupes de réflexions imprimitifs va nous permettre de déduire des informations sur un groupe de réflexions lorsqu'il contient un sous-groupe de réflexions primitif. Celà nous sera très utile pour la classification des groupes de réflexions primitifs.

Lemme 2.10: *Soit G un groupe de réflexions irréductible de V. Si G a un sous-groupe de réflexions H primitif en dimension $r > 1$ et non conjugué à $\mathrm{W}(A_r)$, alors G est primitif.*

DÉMONSTRATION: Soit $W = (V^H)^\perp$ l'espace vectoriel de dimension r sur lequel H agit primitivement. Si $r = n$, G est primitif. Supposons donc que $r < n$ et que G a pour système d'imprimitivité $L_1, \dots L_n$. H est primitif, donc irréductible sur W. Si $L_i \subset W$ pour un certain i, alors comme HL_i engendre W et que HL_i est la somme directe des L_j contenus dans W (par définition d'un système d'imprimitivié), on obtient donc que W est imprimitif, sauf si $W = L_i$. Mais dans ce cas, $r = 1$, ce qui contredit notre hypothèse. Ainsi

$$L_i \not\subset W \text{ pour tout } 1 \leqslant i \leqslant n \tag{2.3}$$

Soit $s \in H$ une réflexion de racine $a \in V$. Comme $s \in H$, $a \in W$. Si s stabilise tous les L_i, alors il existe j tel que $a \in L_j$ par la Proposition 2.4(ii), mais comme L_j est de dimension 1, $L_j \subset W$, ce qui contredit (2.3). Donc on peut supposer que $sL_1 = L_2$ et que s est d'ordre 2. Si s' est une autre réflexion de H qui envoie L_1 sur L_2, et a' une racine de s', alors $a \nsim a'$, car si c'était le cas, on aurait $s, s' \in o_H(a)$ or par ce qui précède, $|o_H(a)| = 2$, et on aurait $s = s'$. Donc $\mathbf{C}a + \mathbf{C}a'$ est de dimension 2 et $a, a' \in L_1 + L_2$ d'où $W \supset \mathbf{C}a + \mathbf{C}a' = L_1 + L_2$, ce qui contredit (2.3).

Ainsi pour tout $i \neq j$, il y a au plus une réflexion de $s \in H$ telle que $sL_i = L_j$. Donc la Proposition 2.4(iii) montre que H est conjugué à un sous-groupe de Π_n engendré par les transpositions (ij) telles qu'il existe une réflexion dans H qui envoie V_i sur V_j. Il est classique qu'un tel sous-groupe est un produit de groupes symétriques $\Pi_{m_1} \times \cdots \times \Pi_{m_k}$[1]. Mais $H \hookrightarrow \mathbf{U}(W)$ est irréductible sur W, donc le théorème de structure des algèbres semi-simples nous dit que $\mathbf{C}[H]$ est simple, et donc H est conjugué à un Π_t. Comme H est de dimension r, $t = r + 1$ et H est bien conjugué à $\mathrm{W}(A_r)$. ■

[1]Considérer le graphe de sommets $\{1, 2, \dots n\}$ et tel qu'il existe une arrête entre i et j ssi la transposition (ij) fait partie des transpositions qui engendrent le sous-groupe. Alors le sous-groupe est égal à $\Pi_{m_1} \times \cdots \times \Pi_{m_k}$ où les m_i sont les cardinaux de chaque composante connexe du graphe

Lemme 2.11: $\mathrm{G}(de, e, n)$ *($n \geqslant 2$) a un unique système d'imprimitivité (et est irréductible) si et seulement si* $(de, e, n) \notin \{(2,1,2),(4,4,2),(3,3,3),(2,2,4)\}$

DÉMONSTRATION: On sait que $L_i = \mathbf{C}\varepsilon_i$ constitue un système d'imprimitivité de $\mathrm{G}(de, e, n)$. Supposons qu'il existe une orbite de P qui donne lieu à un autre système d'imprimitivité, c'est à dire qu'il y a une autre orbite dans P de longueur n. La Remarque 2.9(v) nous donne

$$n = 2 \text{ et } n = m \times \mathrm{pgcd}(2, d) \times \mathrm{pgcd}(2, de)^{-1} \tag{2.4}$$

ou

$$n > 2 \text{ et } 2n = de \times n(n-1) \tag{2.5}$$

Or (2.4) conduit à $(de, e, n) \notin \{(2,1,2),(4,4,2),\}$ et (2.5) est impossible car $de > 1$ vu que l'on suppose $\mathrm{G}(de, e, n)$ irréductible.

Supposons qu'il existe un système d'imprimitivité $V_1, \ldots, V_n$ différent de $L_1, \ldots, L_n$. $V_1, \ldots, V_n$ ne vient pas d'une orbite de P par ce qui précède. Soit $l_1, \ldots, l_n$ les polynômes linéaires homogènes définis par rapport à $V_1, \ldots V_n$ dans Proposition 2.4(i) et posons $f = l_1 l_2 \ldots l_n$. C'est un polynôme semi-invariant. Ainsi $f = I f_{O_1} f_{O_2} \ldots f_{O_m}$ où I est invariant et les O_i des orbites de G dans P (voir la Proposition 1.28). Si f n'est pas invariant, il existe i tel que $l_i | f_{O_1}$ (car S est factoriel), mais G étant irréductible, pour tout j il existe $g \in G$ tel que $g.l_i = l_j$ (en fait il suffit de prendre la réflexion qui correspond à (ij)), donc $\prod_{1 \leqslant i \leqslant n} l_i | f_{O_1}$, $f = f_{O_1}$ et $\deg f_{O_1} = \deg f = n$ ce qui contredit ce qui précède. f est donc invariant. La Remarque 2.9(ii) nous dit que f est un polynôme en les X_i^{de} et $(X_1 \ldots X_n)^d$. Mais comme $\deg f = n$, f n'est pas un polynôme en $(X_1 \ldots X_n)^d$ sauf si $d = 1$, et dans ce cas f est proportionnel à $X_1 \ldots X_n$, ce qui contredit le fait que les V_i forment un système d'imprimitivité différent des L_i. Donc f est un polynôme homogène en les $X_i^{de} m$, d'où $de | n$.

On écrit $l_1 = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_n X_n$ et l'on pose $r_j = |\{i, \alpha_i = \alpha_j\}|$ et $r_0 = |\{i, \alpha_i \neq 0\}|$. Si $g \in \Pi_n$ stabilise $\mathbf{C}l_1$, il doit permuter entre eux les α_i égaux à α_j, donc $\mathrm{Stab}_{\Pi_n} \mathbf{C}l_1 \leqslant r_j!(n - r_j)!$. Cette inégalité est toujours valable, si $j = 0$. Mais comme l'orbite est de longueur au plus n, on obtient

$$n \geqslant n!(r!)^{-1}((n - r_j)!)^{-1} = \binom{n}{r_j}$$

Donc $r_j = 1, n-1, n$. Or $r_0 \neq 1$. Supposons que $r_0 = n - 1$. Comme le stabilisateur de $\mathbf{C}l_1$ dans $\mathrm{G}(de, e, n)$ est d'ordre $\leqslant d^2 e \times (n-1)!$ [1] , d'où

$$n \geqslant \frac{d(de)^{n-1} n!}{d^2 e (n-1)!} = (de)^{n-2} n$$

[1] En effet, on regarde d'abord le stabilisateur dans $\mathrm{A}(de, e, n)$: il faut multiplier tous les éléments non nuls de l_1 par le même élément pour stabiliser $\mathbf{C}l_1$, ce qui donne de choix, et on peut multiplier l'élément nul de l_1 par le coefficient que l'on veut, du moment que le déterminant est respecté, ce qui donne d choix. Ainsi $\left|\mathrm{Stab}_{A(de,e,n)} l_0\right| = d^2 e$ et $\left|\mathrm{Stab}_{\Pi_n} l_0\right| \leqslant (n-1)!$ et l'on vérifie facilement que l'on a $\left|\mathrm{Stab}_{\mathrm{G}(de,e,n} l_0\right| = \left|\mathrm{Stab}_{A(de,e,n)} l_0\right| \times \left|\mathrm{Stab}_{\Pi_n} l_0\right| \leqslant d^2 e(n-1)!$ (Attention, il n'est pas vrai en général que pour un groupe $G = H.K$, $Stab_G x = Stab_K x \times Stab_H x$, mais pour ce cas particulier c'est vrai).

et $n = 2$, et $l_1 \in \mathbf{C}X_1$ ou $l_1 \in \mathbf{C}X_2$ ce qui contredit le fait que $V_1, \dots V_n$ est différent de $L_1, \dots L_n$ (à permutation près). Donc $r_0 = n$. Par les mêmes arguments que la note 1 page 25 on a que $\left|\mathrm{Stab}_{G(de,e,n}\, l_0\right| \leqslant (de)n!$ d'où

$$n \geqslant \frac{d(de)^{n-1}n!}{den!} = (de)^{n-2}d$$

Comme $de|n$, cela donne $(de, e, n) \in \{(2,1,2),(2,2,4),(3,3,3)\}$ ■

Proposition 2.12: *Soit G un groupe de réflexions primitif de V, et H un sous-groupe de réflexions irréductible et imprimitif de dimension m, avec $1 < m < n$. Si H a un unique système d'imprimitivité $L_1, \dots L_m$ dans $(V^H)^\perp$, alors il existe une réflexions s_0 de G tel que $\langle H, s_0\rangle$ est primitif de dimension $m+1$.*

DÉMONSTRATION: Posons $W = (V^H)^\perp$; $\dim W = m$. On procède par récurrence sur $n - m$.

Supposons $m = n - 1$ et posons $L_n = V^H$. Alors $L_1, \dots, L_m$ est un système d'imprimitivité de H dans V. C'est l'unique système d'imprimitivité de H dans V constitué d'espaces de dimensions 1. En effet, supposons que l'on ait un autre système d'imprimitivité $V_1, \dots, V_n$ avec $\dim V_i = 1$. Alors si

$$V_i \not\subset W \text{ pour tout } 1 \leqslant i \leqslant n \tag{2.6}$$

le preuve du Lemme 2.10 montre que H est conjugué à $\Pi_n = G(1,1,n)$. Mais ce dernier groupe agit primitivement sur W (il agit comme $\mathrm{W}(A_{n-1})$), ce qui contredit le fait que H est imprimitif. Donc on peut supposer par exemple que $V_1 \subset W$. Comme H est irréductible sur W, $HV_1 = W$ et W est la somme des $V_i \subset W$ (et on peut supposer que ce sont $V_1, \dots, V_{n-1}$ car $\dim W = n-1$). Comme H a un unique système d'imprimitivité, $\{V_1, \dots, V_{n-1}\} = \{L_1, \dots, L_{n-1}\}$, et comme W est stable par H, on a aussi $V_n = W^\perp = L_n$.

Comme G est primitif, il existe une réflexion s de G qui ne respecte pas ce système d'imprimitivité (par exemple $sL_1 \neq L_i (\forall i)$). Cependant $\langle H, s\rangle$ n'est pas de dimension n si s a ses racinesdans W, donc s ne convient pas forcément. Mais dans ce cas, s stabilise W. Comme G est irréductible, il existe une réflexion t de G qui ne stabilise pas L_n (une telle réflexion a alors ses racines dans $W \bigcup W^\perp$). Si t ne respecte pas le système d'imprimitivité L_i, $s_0 = t$ convient[1], sinon on a $tL_n = L_i$, $L_i \subset W$. Mais si on conjugue t par une réflexion de H qui envoit L_i sur L_1 (cf. la Proposition 2.4) puis par s, on obtient une réflexion s_0 qui ne respecte pas le système d'imprimitivité (L_i) et qui ne stabilise pas W, ce qu'on voulait.

Maintenant, supposons que $n < m-1$ et qu'il n'existe pas de réflexion s_0 comme dans la Proposition. G étant irréductible, il existe une réflexion s de G qui a pour racine $a \notin W \bigcup W^\perp$. $H' = \langle H, s\rangle$ est de dimension $m+1$, irréductible dans $W + sW$ (par choix de s) et imprimitif par hypothèse. La preuve du cas $n = m - 1$ traitée précédemment montre que H et donc a fortiori H' a un unique système d'imprimitivité (dans $W+sW$) : $L_1, L_2, \dots, L_m, L_{m+1}$ ou $L_{m+1} = W^\perp \bigcap (W+sW) =$

[1]En effet, $\langle H, t\rangle$ est irréductible de dimension n, donc s'il a un système d'imprimitivité (V_i), $\dim V_i = 1$ (Proposition 2.4), donc par ce qui précède $(V_i) = (L_i)$ (à permutation près), mais cela contredit le choix de t

$W^\perp \bigcap sW$. Comme $a \notin W \bigcup W^\perp$, il existe i tel que $sL_i = L_{m+1}$. La Proposition 2.4 dit alors que s est d'ordre 2, et quitte à renuméroter on peut supposer que $sL_i = L_i$ si $i < m$, $sL_m = L_{m+1}$. Choisissons $(a_i \in L_i)$ des vecteurs unitaires tels que $sa_i = a_i$ si $i < m$ et $sa_m = a_{m+1}$. L'hypothèse de récurrence nous donne une réflexion s' de G, de racine unitaire $b \in V$, telle que $H'' = \langle H, s, s' \rangle$ est primitif dans $W'' = W + sW + s'W + s'sW$. Soit a_{m+2} un vecteur unitaire de $W'' \bigcap (W + sW)^\perp$.

Comme H'' est primitif (donc irréductible), il existe un $i \leqslant m+1$ tel que $s'a_i \notin W + sW$. La Proposition 2.4 montre qu'il existe $g \in H'$ tel que $ga_i = \alpha a_m$ $(\alpha \in \mathbf{U})$. Quitte à remplacer s' par $gs'g^{-1}$, on peut supposer que $s'a_m \notin W + sW$. Comme $\langle H, s' \rangle$ est imprimitif (de dimension $m+1$), le même raisonnement que pour H' montre que s' est d'ordre 2, et s' laisse stable le système d'imprimitivité $(L_1, \ldots, L_m, W^\perp \bigcap s'W)$, d'où $s'a_m \in W^\perp \bigcap s'W \subset W^\perp \bigcap W'' = \mathbf{C}a_{m+1} \oplus \mathbf{C}a_{m+1}$. Or $s'a_m = a_m - 2 \times 2^{-1/2} b$ (par la Remarque 2.5), donc $\exists \lambda, \mu \in \mathbf{C}$ tels que $b = 2^{-1/2}(a_m - \lambda a_{m+1} - \mu a_{m+2})$. Ainsi, $sa_m = a_{m+1}$, $s'a_{m+1} = a_{m+1} - 2^{1/2}\lambda b$ et $(ss'sa_m \,|a_m) = (s'a_{m+1} \,|a_{m+1}) = 1 - |\lambda|^2$. Mais $\langle H, ss's \rangle$ est irréductible[1] et imprimitif en dimension $m+1$, donc $|(ss'sa_m \,|a_m)| \in \{0, 1\}$ (selon que $ss's$ stabilise ou non L_m). D'où $b = 2^{-1/2}(a_m - \lambda a_{m+1})$ ou $2^{-1/2}(a_m - \mu a_{m+2})$, et donc $s'a_m = \lambda a_{m+1}$ ou $s'a_m = \mu a_{m+1}$. Donc s' conserve le système $(\mathbf{C}a_i)$, comme c'est aussi le cas des réflexions de H' vu que $a_{m+2} \in W''^{H'}$, on a exhibé un système d'imprimitivité de H'', contradiction. ■

[1]En effet $ss's$ a pour racine sb qui n'appartient pas à W car $b \notin W + sW$ puisque H'' est irréductible

Chapitre 3

Groupes de réflexions de rang 2

3.1 Introduction

Comme on l'a dit dans l'introduction, déterminer les groupes de réflexions imprimitifs est une tâche aisée. Les $\mathrm{G}(de, e, n)$ donnent ainsi lieu à une famille infinie de groupes de réflexions irréductibles (et imprimitifs). La classification des groupes de Coxeter finis et par là des groupes de réflexions réels irréductibles donne lieu à une seconde famille infinie (et primitive) : les $\mathrm{W}(A_n)$

Il reste 34 groupes sporadiques, qui sont des groupes de réflexions primitifs. Or il se trouve que parmi eux, 19 groupes sont de rang 2 (tous complexes). Les outils développés dans la suite du mémoire, qui cherchent à généraliser (de manière pas totalement satisfaisante) la combinatoire sur les graphes de Coxeter qui aboutit à la classification des groupes de réflexions réels ne fonctionnent vraiment qu'en rang $\geqslant 3$ (voir le Lemme 4.19(ii)). Il reste donc le problème de trouver ces 19 groupes sporadiques de rang 2. Pour cela, il semble que le plus simple est de donner la liste de tous les sous-groupes finis de $\mathrm{U}_2(\mathbf{C})$, puis de déterminer lesquels parmi ceux-ci sont des groupes de réflexions.

Or il se trouve que $\mathrm{PSU}_2(\mathbf{C}) \simeq \mathrm{SO}_3(\mathbf{R})$ et les sous-groupes finis de $\mathrm{SO}_3(\mathbf{R})$ sont bien connus. Comme $\mathrm{PSU}_2(\mathbf{C}) = \mathrm{SU}_2(\mathbf{C})/\{\pm \mathrm{Id}\}$, on remonte facilement aux sous-groupes finis de $\mathrm{SU}_2(\mathbf{C})$. Enfin, $\mathrm{U}_2(\mathbf{C})$ est engendré par $\mathrm{SU}_2(\mathbf{C})$ et les matrices scalaires $\lambda \,\mathrm{Id}, \lambda \in \mathbf{U}$, ce qui va nous permettre de remonter aux sous-groupes finis de $\mathrm{U}_2(\mathbf{C})$ par le Proposition 3.2

3.2 Sous-groupes finis de $\mathrm{SU}_2(\mathbf{C})$

Soit

$$\begin{array}{rccc} \psi : & \mathbf{R}^3 & \to & \mathrm{M}_2(\mathbf{C}) \\ & \begin{pmatrix} x \\ y \\ z \end{pmatrix} & \mapsto & \begin{pmatrix} z & x - iy \\ x + iy & -z \end{pmatrix} \end{array}$$

ψ est un isomorphisme de $\mathbf{R}^3$ sur l'espace $\mathcal{H}_0$ des matrices hermitiennes de $\mathrm{M}_2(\mathbf{C})$ de trace nulle, telle que $\det \psi(v) = \|v\|_2$.

Et soit

$$\begin{array}{rccc} \varphi : & \mathrm{SU}_2(\mathbf{C}) & \to & \mathrm{Aut}(\mathcal{H}_0) \\ & M & \mapsto & (V \mapsto MVM^{-1}) \end{array}$$

Or $\forall M \in \mathrm{SU}_2(\mathbf{C})$, $\varphi(M)$ préserve le déterminant, donc si on la voit comme un automorphisme de $\mathbf{R}^3$, $\varphi(M)$ est une rotation. Si $M \in \operatorname{Ker}\varphi$, M commute à $\mathcal{H}_0$ et donc aussi à $i\mathcal{H}_0$. On vérifie que $\mathcal{H}_0 + i\mathcal{H}_O$ est l'ensemble des matrices de trace nulle, donc M est une matrice scalaire, d'où $\operatorname{Ker}\varphi = \{\pm \mathrm{Id}\}$. Ainsi $\varphi : \mathrm{PSU}_2(\mathbf{C}) \hookrightarrow \mathrm{SO}_3(\mathbf{R})$ réalise une injection entre deux groupes algébriques connexes et de même dimension[1], comme l'image est fermée, φ est une bijection, donc un isomorphisme de groupes (en fait c'est même un isomorphisme de groupes algébriques car on est en caractéristique nulle).

D'où $\mathrm{PSU}_2(\mathbf{C}) \simeq \mathrm{SO}_3(\mathbf{R})$. Or les groupes finis de $\mathrm{SO}_3(\mathbf{R})$ sont bien connus, ils se déduisent des groupes d'automorphismes des solides réguliers de dimension 2 et 3. Il y a :

- Les groupes cycliques de rotations
- Les groupes diédraux d'ordre $2m$ ($m > 1$)
- Le groupe du tétraèdre, d'ordre 12, isomorphe à $\mathfrak{A}_4$
- Le groupe du cube (isomorphe au groupe de l'octaèdre car ce sont deux polygones réguliers duaux), d'ordre 24, isomorphe à $\mathfrak{S}_4$
- Le groupe de l'icosaèdre (isomorphe au groupe du dodécaèdre car ce sont deux polygones réguliers duaux), d'ordre 60, isomorphe à $\mathfrak{A}_5$.

Il nous reste à remonter à $\mathrm{SU}_2(\mathbf{C})$. Si H est un sous-groupe fini de $\mathrm{PSU}_2(\mathbf{C})$, on cherche à trouver les sous-groupes G de $\mathrm{SU}_2(\mathbf{C})$ dont il est image. On a :

- Son image réciproque
- Des relevés qui s'envoient bijectivement dessus (*a priori* plus durs à déterminer)

Mais ici, comme $-Id$ est l'unique élément d'ordre 2 de $\mathrm{SU}_2(\mathbf{C})$, tout sous-groupe d'ordre pair de $\mathrm{SU}_2(\mathbf{C})$ contient $-Id$, donc est l'image réciproque de son image dans $\mathrm{PSU}_2(\mathbf{C})$. Au vu de la liste des sous-groupes finis de $\mathrm{PSU}_2(\mathbf{C})$, il n'y a que les groupes cycliques d'ordres impair comme relevés dans $\mathrm{SU}_2(\mathbf{C})$.

On a donc la liste suivante des sous-groupes finis de $\mathrm{SU}_2(\mathbf{C})$:

- Les groupes cycliques d'ordre m, $\mathbf{C}_m$ (qui sont réductibles).
- Les groupes diédraux binaires d'ordre $4m$ ($m > 1$), $\mathbf{D}_m$ (irréductibles mais imprimitifs).
- Le groupe binaire du tétraèdre d'ordre 24, $\mathbf{T}$ (imprimitif).
- Le groupe binaire de l'octaèdre (ou du cube) d'ordre 48, $\mathbf{O}$ (imprimitif).
- Le groupe binaire de l'icosaèdre d'ordre 120, $\mathbf{I}$ (imprimitif).

Remarque 3.1: La liste précédente est la liste des sous-groupes finis de $\mathrm{SU}_2(\mathbf{C})$ à conjugaison près. En effet c'est le cas pour la liste des sous-groupes finis de $\mathrm{PSU}_2(\mathbf{C})$, et on vérifie facilement que ça reste le cas pour $\mathrm{SU}_2(\mathbf{C})$, vu qu'on prend leur image réciproque.

[1] $\dim \mathrm{SO}_3(\mathbf{R}) = \dim \mathrm{O}_3(\mathbf{R}) - 1 = \dim \mathrm{M}_3(\mathbf{R}) - 3 - 1 = 5$, et $\dim \mathrm{PSU}_2(\mathbf{C}) = \dim \mathrm{SU}_2(\mathbf{C}) = \dim \mathrm{M}_2(\mathbf{C}) - 2 - 1 = 5$

Donc à conjugaison près, on a :

$$\mathbf{C}_m = \langle \begin{pmatrix} e^{2i\pi/m} & 0 \\ 0 & e^{-2\pi i/m} \end{pmatrix} \rangle$$

$$\mathbf{D}_m = \langle \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \mathbf{C}_{2m} \rangle$$

$$T = \langle \frac{1}{\sqrt{2}} \begin{pmatrix} \varepsilon & \varepsilon^3 \\ \varepsilon & \varepsilon^7 \end{pmatrix}, \mathbf{D}_2 \rangle \quad (\varepsilon = \exp(2i\pi/8))$$

$$O = \langle \begin{pmatrix} \varepsilon^3 & 0 \\ 0 & \varepsilon^5 \end{pmatrix}, \mathbf{T} \rangle$$

$$I = \langle \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^4 - \eta & \eta^2 - \eta^3 \\ \eta^2 - \eta^3 & \eta - \eta^4 \end{pmatrix}, \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^4 & \eta^4 - 1 \\ 1 - \eta & \eta^3 - \eta \end{pmatrix} \rangle \quad (\eta = \exp(2i\pi/5)) \qquad \diamondsuit$$

3.3 Sous-groupes finis de $\mathrm{U}_2(\mathbf{C})$

$\mathrm{U}_2(\mathbf{C})$ est engendré par $\mathrm{SU}_2(\mathbf{C})$ et $\mathcal{Z}(\mathrm{U}_2(\mathbf{C})) = \{\lambda \,\mathrm{Id}, \lambda \in \mathbf{U}\} \simeq \mathbf{U}$. On va appliquer à $\mathrm{U}_2(\mathbf{C})$ la proposition suivante :

Proposition 3.2: *Soit S un groupe engendré par des sous-groupes H et K, qui commutent entre eux (ainsi H et K sont distingués dans S). On note $\psi : H \times K \twoheadrightarrow S$ l'épimorphisme $(h,k) \mapsto hk$. Soit G un sous-groupe de S. On pose $A = GH \bigcap K$, $A' = G \bigcap K$, $B = GK \bigcap H$ et $B' = G \bigcap H$ ($GH = HG$ et $GK = KG$ sont bien des groupes car H et K sont distingués). Alors*

(i) $A/A' \simeq B/B'$

(ii) Si de plus K est abélien, alors $\psi(B \times_{A/A' \simeq B/B'} A) = G$[1]

Démonstration:

(i) $\frac{A}{A'} \simeq \frac{(GH \bigcap K)G}{G}$ et $\frac{B}{B'} \simeq \frac{(GK \bigcap H)G}{G}$ donc il suffit de vérifier que $(GH \bigcap K)G = (GK \bigcap H)G$. Or si $x \in (GK \bigcap H)G$, $x = kg$ où $k \in K \bigcap HG$, $g \in G$ et $k = hg'$, $h \in H$ et $g' \in G$. D'où $x = \underbrace{kg'^{-1}}_{\in H} \underbrace{g'g}_{\in G}$, donc $x \in (KG \bigcap H)G$. Par symétrie on a l'autre inclusion. L'isomorphisme de A/A' sur B/B' est donné par $\sigma' : \overline{k} = \overline{hg} \in A/A' \mapsto \overline{h} \in B/B'$, avec des notations évidentes.

(ii) On note G' le produit fibré $B \times_{A/A' \simeq B/B'} A$. Ici il convient de noter que G' va dépendre de l'isomorphisme qu'on choisit entre A/A' et B/B'. Comme K est abélien, on va prendre pour isomorphisme : $\sigma(\overline{k}) = \sigma'(\overline{k^{-1}})$ On veut montrer que $\psi(G') = G$. Si $g \in G$, on peut écrire $g = hk$, $h \in B$ et $k \in A$. De plus

[1] $B \times_{A/A' \simeq B/B'} A$ représente le produit fibré de B par A au dessus de $A/A' \simeq B/B'$:

$$\begin{array}{ccc} B \times_{A/A' \simeq B/B'} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A & \longrightarrow & A/A' \simeq B/B' \end{array}$$

$\sigma'(\overline{k}) = \sigma'(\overline{h^{-1}g}) = \overline{h^{-1}}$, donc $(h,k) \in G'$. Réciproquement, si $x = hk$, $h \in B$ et $k \in A$ tels que $\sigma'(\overline{k}) = \overline{h^{-1}}$, alors $\exists g \in G$ tel que $\overline{k} = \overline{h^{-1}g}$ par définition de σ', donc $\overline{x} = \overline{g}$ et $x \in G$. ■

Remarque 3.3: Comme on l'a remarqué dans la preuve, $B \times_{A/A' \simeq_\sigma B/B'} A$ dépend de l'isomorphisme σ entre A/A' et B/B'. On notera

$$(A\,|A'\,;B\,|B')_\sigma = \psi(B \times_{A/A' \simeq_\sigma B/B'} A)$$

Ainsi si on applique ce qui précède à $\mathrm{U}_2(\mathbf{C})$, on obtient que ses sous-groupes finis sont de la forme

$$(\mu_{wd}\,|\mu_w\,;A\,|A')_\sigma$$

où μ_m représente le groupe des racines m^{ieme} de l'unité, et $A' \lhd A$ sont des sous-groupes finis de $\mathrm{SU}_2(\mathbf{C})$. Comme μ_{wd}/μ_w est cyclique, A/A' doit l'être aussi. Enfin, comme $G = (\mu_{wd}\,|\mu_w\,;A\,|A')_\sigma$ est engendré par A et des matrices scalaires $\lambda\,\mathrm{Id}$, le caractère irréductible (resp. primitif) de G ne dépend que du caractère irréductible (resp. primitif) de A.

Or en regardant la liste donnée dans la section 3.2, on voit que les inclusions distinguées à quotient cycliques de sous-groupes de $\mathrm{SU}_2(\mathbf{C})$ sont $\mathbf{C}_m \lhd_r \mathbf{C}_{mr}$, $\mathbf{C}_{2m} \lhd_2 \mathbf{D}_m \lhd_2 \mathbf{D}_{2m}$ et $\mathbf{D}_2 \lhd_3 \mathbf{T} \lhd_2 \mathbf{O}$. (où $A' \lhd_r A$ signifie que A/A' est cyclique d'ordre r). Comme on se restreint à des sous-groupes finis irréductibles, $A \neq \mathbf{C}_m$, et on vérifie que dans ce cas la classe de $G = (\mu_{wd}\,|\mu_w\,;A\,|A')_\sigma$ ne dépend pas de σ. De plus $-1 \in G$, donc $-1 \in \mu_w = G \bigcap \mathcal{Z}(\mathrm{U}_2(\mathbf{C}))$, d'où w est pair. On a ainsi (presque) démontré :

Théorème 3.4: *Tout sous-groupe fini irréductible de* $\mathrm{U}_2(\mathbf{C})$ *est conjugué à l'un des groupes suivant :*

- $\mu_{2q}\mathbf{D}_m$, $\mu_{2q}\mathbf{T}_m$, $\mu_{2q}\mathbf{O}_m$, $\mu_{2q}\mathbf{I}_m$.
- $(\mu_{4q}\,|\mu_{2q}\,;\mathbf{D}_m\,|\mathbf{C}_{2m})$, $(\mu_{4q}\,|\mu_{2q}\,;\mathbf{D}_{2m}\,|\mathbf{D}_{2m})$, $(\mu_{4q}\,|\mu_q\,;\mathbf{D}_m\,|\mathbf{C}_m)$ *(si* $m \wedge 2 = 1$*)*
- $(\mu_{6q}\,|\mu_{2q}\,;\mathbf{T}\,|\mathbf{D}_2)$, $(\mu_{4q}\,|\mu_{2q}\,;\mathbf{O}\,|\mathbf{T})$

Parmi ces groupes, les groupes de réflexions imprimitifs sont :

$$\mathrm{G}(de,e,2) \text{ conjugé à } \begin{cases} (\mu_{4q}\,|\mu_{2q}\,;\mathbf{D}_m\,|\mathbf{C}_{2m}) & \text{si } e \text{ est pair, } d \text{ impair} \\ (\mu_{2q}\,|\mu_q\,;\mathbf{D}_m\,|\mathbf{D}_{m/2}) & \text{si } e \text{ est impair, } d \text{ pair} \\ \mu_{2q}\mathbf{D}_m & \text{si } e \text{ est pair, } d \text{ pair} \\ (\mu_{4q}\,|\mu_q\,;\mathbf{D}_m\,|\mathbf{C}_m) & \text{si } e \text{ est impair, } d \text{ impair} \end{cases}$$

les autres groupes sont imprimitifs. Pour trouver lesquels sont des groupes de réflexions, on calcule les invariants de $\mathbf{T}$, $\mathbf{O}$ et $\mathbf{I}$, et on regarde les racines de l'unité à ajouter pour que ces invariants forment une algèbre de polynômes.

On obtient

Théorème 3.5: *Les groupes de réflexions primitifs de dimension 2, sont à conjugaison près :*

- $\mu_{6m}\mathbf{T}$, $(\mu_{6m}\,|\mu_{2m}\,;\mathbf{T}\,|\mathbf{D}_2)$ $(m = 1, 2)$.
- $\mu_{4m}\mathbf{O}$, $(\mu_{4m}\,|\mu_{2m}\,;\mathbf{O}\,|\mathbf{T})$ $(m = 1, 2, 3, 6)$.

– $\mu_{4m}\mathbf{I}$ $(m = 2, 3, 5, 6, 10, 15, 30)$.

On trouvera ci-dessous un tableau récapitulatif, où les groupes sont ordonnés suivant la numérotation de Shephard et Todd, et où on donne leurs degrés caractéristiques, leurs ordres, et l'ordre des centres.

Numéro	Groupe	Degrés	Ordre	Ordre du centre	Nombre de réflexions d'ordres			
					2	3	4	5
4	$(\mu_6 \,\vert \mu_2 \,; \mathbf{T} \,\vert \mathbf{D}_2)$	4,6	24	2	-	8	-	-
5	$\mu_6\mathbf{T}$	6,12	72	6	-	16	-	-
6	$(\mu_{12} \,\vert \mu_4 \,; \mathbf{T} \,\vert \mathbf{D}_2)$	4,12	48	4	6	8	-	-
7	$\mu_{12}\mathbf{T}$	12,12	144	12	6	16	-	-
8	$(\mu_8 \,\vert \mu_4 \,; \mathbf{O} \,\vert \mathbf{T}_2)$	8,12	96	4	6	-	12	-
9	$\mu_8\mathbf{O}$	8,24	192	8	18	-	12	-
10	$(\mu_{24} \,\vert \mu_{12} \,; \mathbf{O} \,\vert \mathbf{T}_2)$	24,12	288	12	6	16	12	-
11	$\mu_{24}\mathbf{O}$	24,24	576	24	18	16	12	-
12	$(\mu_4 \,\vert \mu_2 \,; \mathbf{O} \,\vert \mathbf{T}_2)$	6,8	48	2	12	-	-	-
13	$\mu_4\mathbf{O}$	8,12	96	4	18	-	-	-
14	$(\mu_{12} \,\vert \mu_6 \,; \mathbf{O} \,\vert \mathbf{T}_2)$	6,24	144	6	12	16	-	-
15	$\mu_{12}\mathbf{O}$	12,24	288	12	18	16	-	-
16	$\mu_{10}\mathbf{I}$	20,30	600	10	-	-	-	48
17	$\mu_{20}\mathbf{I}$	20,60	1200	20	30	-	-	48
18	$\mu_{30}\mathbf{I}$	30,60	1800	30	-	40	-	48
19	$\mu_{60}\mathbf{I}$	60,60	3600	60	30	40	-	48
20	$\mu_6\mathbf{I}$	12,30	360	6	-	40	-	-
21	$\mu_{12}\mathbf{I}$	12,60	720	12	30	40	-	-
22	$\mu_4\mathbf{I}$	12,20	240	4	30	-	-	-

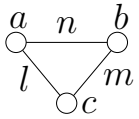
TAB. 3.1 – Groupes de réflexions primitifs de rang 2

Chapitre 4

Graphes de racines et systèmes de racines

4.1 Introduction

Il nous reste maintenant à classifier les groupes de réflexions complexes primitifs de rang $\geqslant 3$. Avant de le faire, nous allons introduire des outils généralisant les graphes de Coxeter et les systèmes de racines qui permettent la classification des groupes de réflexions réels. C'est ici qu'apparaît la difficulté, on n'a pas vraiment de bonne généralisation des graphes de Coxeter. Rappelons sur un exemple comment on construit les graphes de Coxeter : si l'on a un groupe G engendré par des (vraies) réflexions $\{s_a, s_b, s_c\}$, on choisit des racines $\{a, b, c\}$ correspondantes, et l'on relie par exemple la racine a à la racine b par une arrête valuée, la valuation correspondant à l'ordre de $s_a s_b$ (qui est n si $|(a\,|b)| = cos(k\pi/n)$, k premier à n).



L'exemple précédent contient déjà beaucoup d'informations sur G, par exemple il est fini si et seulement si $1/a + 1/b + 1/c > 1$, ce qui implique déjà que a, b ou $c < 2$.

Si par contre G est un groupe de réflexions complexe, il peut déjà contenir des réflexions d'ordre > 3. De plus, même si $s \in \mathrm{Ref}(G)$ est d'ordre 2, il existe une infinité de racines unitaires de s (alors que dans le cas réel, si v est racine unitaire de s, seul $-v$ l'est aussi, et on peut choisir canoniquement entre v et $-v$ en mettant un ordre sur les racines, cf. [Bou68]). Ainsi il nous faut rajouter un paramètre supplémentaire (qui varie dans $\mathbf{U}$) pour chaque racine d'une réflexion qui engendre G. Ces paramètres supplémentaires, on les représentera en mettant directement le produit scalaire des deux racines sur l'arrête du graphe. De plus, si pour un groupe de réflexions réel, il existe un moyen quasi canonique de considérer un système de réflexions génératrices (grâce aux chambres), ce qui aboutit à des graphes de Coxeter sans cycles, il n'en est absolument pas de même pour les groupes de réflexions complexes (et en fait le Lemme 4.15 montre que si G est complexe, on ne peut pas le représenter par un graphe sans cycles). Autrement dit, un groupe

de réflexions complexe ne possède pas la géométrie d'un groupe de réflexions réel, qui permet de se ramener d'un groupe de réflexions réel à un groupe de Coxeter (grâce aux murs des chambres), c'est à dire d'un groupe qui vérifie une condition combinatoire sur les mots que l'on peut former avec, puis du groupe de Coxeter fini en question à un graphe de Coxeter, correspondance qui est bijective, ce qui fait qu'il n'y a plus ensuite qu'à classifier les graphes de Coxeter (et ces derniers sont suffisamment simple pour que leur classification se fasse assez facilement).

Ainsi on généralise les graphes de Coxeter en construisant des graphes (que l'on appellera graphes de racines) qui contiennent trop d'information, puisque plusieurs de ces graphes peuvent conduire au même groupe de réflexions complexe. De même on va généraliser les systèmes de racines réels, sauf qu'on n'aura pas de condition $\langle v, v^\vee \rangle \in \mathbf{Z}$, condition qui n'a pas vraiment de sens dans le cas complexe. Pour nous un système de racines sera juste un ensemble fini de vecteurs, stables par le groupe qu'ils engendrent. Dans le cas réel, les systèmes de racines n'interviennent pas vraiment dans la classification, à part une fois que l'on a classifié les graphes de Coxeter, pour exhiber un groupe de réflexions réel représenté par ce graphe. Pour le cas complexe, leur rôle est plus important, notamment à cause de la notion d'extension propre, voir la Définition 4.32 et l'explication au début du Chapitre 5.

Il faut noter que comme pour les graphes de racines, il n'y a aucun espoir de pouvoir classifier les systèmes de racines directement, ils ne sont pas assez rigides puisqu'un même groupe de réflexions complexe peut être représenté par énormément de systèmes de racines (cela vient du fait que l'on a abandonné la condition $\langle v, v^\vee \rangle \in \mathbf{Z}$)), ce qui fait que l'on sera obligé d'utiliser un théorème sortant du cadre combinatoire pour finir la classification. Là encore, voir le Chapitre 5 pour plus de détails.

Pour simplifier les notations, on va travailler à partir de maintenant dans $\mathbf{C}^\infty$, muni du produit scalaire canonique $(\cdot\,|\,\cdot)$. Si $G \subset \mathrm{U}_n(\mathbf{C})$, on peut voir G comme un groupe de réflexions dans $\mathbf{C}^\infty$ en identifiant $\mathbf{C}^n$ avec le sous-espace de $\mathbf{C}^\infty$ engendré par les n premiers vecteurs de la base canonique : $\varepsilon_1, \ldots, \varepsilon_n$. Ceci nous permet de travailler dans $\mathbf{C}^\infty$ pour chercher la liste des groupes de réflexions. Comme on cherche les groupes de réflexions finis, on obtient bien des groupes de réflexions de dimension finie. C'est ici que la notation introduite dans la section 1.3.1 va nous être utile : si un groupe de réflexions G est de dimension r, alors r est le plus petit entier tel qu'un conjugué de G est contenu dans $\mathrm{U}_r(\mathbf{C})$.

4.2 Graphes de racines

Définition 4.1 (graphe de vecteurs): Un graphe de vecteurs (unitaires) est la donnée d'un couple (B, w) où B (l'ensemble des points du graphe, que l'on appellera les racines du graphe) est un ensemble fini de vecteurs unitaires de $\mathbf{C}^\infty$, et w (la valuation) est une fonction de B dans $\mathbf{N} \setminus \{1\}$. Si $a \in B$, $w(a)$ est appelée l'ordre de a.

Deux graphes de vecteurs (B, w) et (B', w') sont dits isomorphes s'il existe une transformation unitaire t de $\mathbf{C}^\infty$ qui envoie B sur B' et w sur w'. (i.e. $tB = B'$ et $w'(ta) = w(a)$ pour tout $a \in B$)

Remarque 4.2: On fera souvent l'abus de notation qui consiste à parler d'un graphe de vecteurs (B, w), où B est un ensemble fini de vecteurs pas forcément unitaires (mais non proportionnels). Lorsqu'on parle d'un tel graphe de vecteurs (B, w), on considère en réalité le graphe de vecteurs (B', w') où $B' = \{a/\|a\|, a \in B\}$ et $w'(a/\|a\|) = w(a)$.

Un graphe de vecteurs (B, w) peut être représenté par un graphe valué orienté Γ de la manière suivante : les points de Γ sont les éléments de B, valués par w. Pour tout couple $\{a, b\} \subset B$ on fixe une orientation (a, b) et on trace une arrête de a vers b valuée par $(a\,|b)$ si $(a\,|b) \neq 0$.

Ainsi on a plusieurs représentations de (B, w) selon l'orientation que l'on a choisie. On a besoin de définir une orientation entre deux vecteurs complexes a et b pour pouvoir définir correctement la valuation de l'arrête qui les relie car $(a\,|b) = \overline{(b\,|a)}$. Cependant si $(a\,|b) \in \mathbf{R}^\star$, alors la valuation de l'arrête ne dépend pas de l'orientation choisie, et donc pour simplifier on ne choisira pas d'orientation pour cette arrête.

Pour imiter les graphes de Coxeter, on fera de plus les simplifications suivantes :
- Si un point $a \in B$ est d'ordre 2, la valuation de a dans le graphe Γ sera omise.
- Si $(a\,|b) = -1/2$, $w(a) = 2$ et $w(b) = 2$, la valuation $-1/2$ de l'arrête connectant a et b sera omise.

Exemple 4.3: Soit $a = \varepsilon_3$ et $b = i3^{-1/2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)$. Alors le graphe de vecteurs $L_2 = \{a, b\}, w(a) = 3, w(b) = 3$ peut être représenté par le graphe orienté suivant :

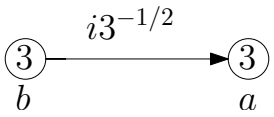


FIG. 4.1 – Le graphe L_2

Soit (B, w) un graphe de vecteurs et Γ le graphe orienté associé. Comme la donnée de Γ permet de retrouver (B, w), on commettra l'abus de notation consistant à identifier Γ et (B, w). Par exemple, un cycle de (B, w) sera un cycle de Γ, et on dira que (B, w) est connexe ssi Γ l'est. (on ne prend pas on compte l'orientation des arrêtes de Γ lorsqu'on regarde les cycles et la connexité). Un triangle de Γ est un cycle de 3 points.

Un graphe de vecteurs $\Gamma = (B, w)$ permet de représenter un groupe de réflexions si l'on pense à $a \in B$ comme une racine d'une réflexion d'ordre $w(a)$.

Définition 4.4 (Groupe de réflexions engendré par un graphe):

Soit $\Gamma = (B, w)$ un graphe de vecteur. On note $\dim(\Gamma)$ la dimension de l'espace vectoriel engendré par Γ et $\mathrm{W}(\Gamma)$ le groupe de réflexions (pas forcément fini) engendré par les réflexions $\{s_{a,w(a)}, a \in B\}$ (avec les notations de la Définition 1.7).

Γ est appelé un graphe de racines si :
- $\dim(\Gamma) = |B|$ (c'est à dire si les éléments de B sont linéairement indépendants).
- $\mathrm{W}(\Gamma)$ est un groupe de réflexions fini. ♢

Remarque 4.5:

(i) Si G est un groupe de réflexions, il existe un graphe de vecteurs Γ tel que $G = \mathrm{W}(\Gamma)$. En effet, si G est engendré par $s_1, \ldots, s_n$, on choisit une racine a_i pour chaque réflexion s_i, et l'on pose $B = \{a_1, \ldots, a_n\}$, $w(a_i) = o_G(a_i)$. $\Gamma = (B, w)$ est un graphe de racines si et seulement si $n = \dim(G)$, c'est à dire si et seulement si les (a_i) sont linéairement indépendants (d'après le Lemme 1.18). Ainsi les graphes de racines ne permettent pas de représenter tout les groupes de réflexions. On a cependant besoin de la condition $\dim(\Gamma) = |B|$ dans la définition d'un graphe de racines pour pouvoir travailler efficacement avec. En fait la classification des groupes de réflexions montre que tout groupe de réflexions primitif (sauf un) de rang $r > 2$ peut être engendré par r réflexions, donc sera représentable par un graphe de racines. Ceci explique pourquoi la condition précédente n'est finalement pas un obstacle à la classification des groupes de réflexions. Bien sûr on aura besoin d'un outil pour représenter les groupes de réflexions qui ne proviennent pas d'un graphe de racines (ne serait-ce que pour prouver que les groupes de réflexions primitifs de rang supérieur à 2 n'en font pas partie), ce sera le rôle des systèmes de racines.

(ii) Si $\Gamma = \Gamma_1 \bigsqcup \ldots \bigsqcup \Gamma_p$ est la décomposition de Γ en cycles, alors $\mathrm{W}(\Gamma) = \mathrm{W}(\Gamma_1) \times \cdots \times \mathrm{W}(\Gamma_p)$ est la décomposition de $\mathrm{W}(\Gamma)$ en produit de sous-groupes de réflexions irréductibles donnée par la Proposition 1.22.

Avant d'étudier plus en avant les graphes de racines, on note déjà que la condition que les vecteurs du graphe de racines soient libres implique que leur matrice de Gram est non nulle. Ceci nous servira quand on étudiera des graphes de racines explicites dans le Chapitre 5.

Lemme 4.6: *Si $\Gamma = (B, w)$ est un graphe de vecteurs avec $B = \{e_1, \ldots, e_n\}$, alors $\det((e_i \,|e_j\,))_{1 \leqslant i,j \leqslant n} \in \mathbf{R}^+$ et ce nombre est nul si et seulement si les (e_i) sont linéairement dépendants, dans ce cas Γ ne peut pas être un graphe de racines.*

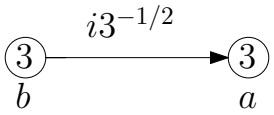
Définition 4.7: Si $\Gamma = (B, w)$ est un graphe de racines, on dit que Γ est réel (resp. complexe, primitif) si $\mathrm{W}(\Gamma)$ est réel (resp. complexe, primitif). On dit que Γ est irréductible si $\mathrm{W}(\Gamma)$ l'est en dimension $\dim(\Gamma)$, i.e. si Γ est connexe (d'après la Remarque 4.5(ii)).

Si $\Gamma' = (B', w')$ est un autre graphe de racines, on dit que Γ est équivalent à Γ' si $\mathrm{W}(\Gamma)$ est conjugué à $\mathrm{W}(\Gamma)$. Si $B \subset B'$ et $w'|_B = w$, on dit que Γ' est une extension de Γ ou que Γ est un sous-graphe de racines de Γ'.

Enfin on dit que Γ est congruent à Γ' s'il existe une transformation unitaire t de $\mathbf{C}^\infty$ qui rend Γ isomorphe à Γ' et telle que les éléments de B sont des vecteurs propres de t.

Remarque 4.8: Si Γ est isomorphe à Γ', $\mathrm{W}(\Gamma)$ est conjugué à $\mathrm{W}(\Gamma')$ donc Γ est équivalent à Γ', mais la réciproque n'est pas vraie, par exemple si on prend des réflexions différentes engendrant le même groupe, les graphes de vecteurs associés n'ont aucune raison d'être isomorphes. Enfin, si Γ est congruent à Γ', alors $\mathrm{W}(\Gamma) = \mathrm{W}(\Gamma')$ (en effet, cela revient à constater que si a est une racine d'une réflexion s, alors $\lambda a, \lambda \in \mathbf{U}$ est également racine de s).

Exemple 4.9: Soit L_2 le graphe de vecteur de l'Exemple 4.3 :



L_2 est un graphe de racines irréductible, et $W(L_2) = (\mu_6 \,|\mu_2\,; \mathbf{T}\,|\mathbf{D}_2)$.

Nous allons maintenant introduire un invariant indispensable pour étudier les groupes de réflexions composés de réflexions d'ordres 2.

Soit $\Gamma = (B, w)$ un graphe de racines, et $u, v \in B$ d'ordres 2. Soit $G = \langle s_u, s_v \rangle$. G est un groupe engendré par deux éléments d'ordre 2, c'est donc un groupe diédral $\mathbf{D}_m$[1] d'ordre $2m$. De plus m est l'ordre de (uv), d'où $|(u\,|v)| = \cos(\pi k/m)$ pour un certain k premier à m (cf. le début de [Bou68]).

Définition 4.10: On pose[2] :

$$d(\Gamma) = \max\{\text{ordre}(uv) | u, v \in B \text{ d'ordres } 2\}$$

Si G est un groupe de réflexions, on pose également :

$$d(G) = \max\{\text{ordre}(uv) | u, v \text{ sont des réflexions de } G \text{ d'ordres } 2\} \qquad \diamondsuit$$

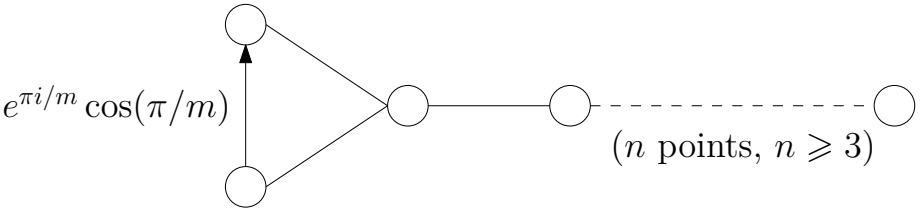
Remarque 4.11: Si Γ est un graphe de racines, on peut avoir $d(\Gamma) < d(\mathrm{W}(\Gamma))$, comme le montre l'exemple suivant.

Exemple 4.12: (cf. la Définition 2.6 et la Remarque 2.7)

– Soit $B_n(m)$ (ou $\Gamma(m, 1, n)$) le graphe de vecteurs :

Alors $B_n(m)$ est un graphe de racines tel que $\mathrm{W}(B_n(m)) = \mathrm{G}(m, 1, n)$

– Soit $D_n(m)$ (ou $\Gamma(m, m, n)$) le graphe de vecteurs



Alors $D_n(m)$ est un graphe de racines tel que $\mathrm{W}(D_n(m)) = \mathrm{G}(m, m, n)$

Or

$$d(B_n(m) = \begin{cases} 4 & \text{si } m = 2 \\ 3 & \text{sinon} \end{cases}$$

$$d(D_n(m) = \max(3, m)$$

[1] Il y a un conflit de notation avec la section 3.2, ici $\mathbf{D}_m$ est le groupe diédral d'ordre $2m$, pas le groupe diédral binaire d'ordre $4m$

[2] on convient que $\max(\varnothing) = -\infty$

mais

$$d(\mathrm{G}(de,e,n) = \begin{cases} de & \text{si } de \geqslant 3 \\ 4 & \text{si } de < 3 \text{ et } d = 2 \\ 3 & \text{si } de < 3 \text{ et } d = 1 \end{cases} \qquad \diamondsuit$$

Le lemme suivant nous sera extrêmement utile pour transformer un graphe de racines représentant un groupe de réflexions G en un graphe de racines équivalent, mais plus facile à étudier.

Lemme 4.13: *Soit $\Gamma = (B, w)$ un graphe de racines, et $(a, b) \in B$. Alors Γ est équivalent à $\Gamma' = (B', w')$, où $B' = \left\{b' = s_{a,w(a)b}\right\} \bigcup B \setminus \{b\}$ et*

$$w'(x) = \begin{cases} w(x) & si\ x \in B \setminus \{b\} \\ w(b) & si\ x = b' \end{cases}$$

DÉMONSTRATION: Il suffit de remarquer que $s_{b',w(b')} = s_{a,w(a)} s_{b,w(b)} s_{a,w(a)}^{-1}$ par la Remarque 1.8. ■

Exemple 4.14: Si a est d'ordre d, soit $\zeta = \exp(2i\pi/d)$. Alors $(s_a(b)\,|c) = (b\,|c) - (1-\zeta)\,(b\,|a)\,(a\,|c)$. Ainsi si a n'est pas lié à b, $\Gamma' = \Gamma$. Sinon, la transformation précédente $\Gamma \mapsto \Gamma'$ est décrite dans la Figure 4.2.

Ainsi si x n'est pas lié à a, il n'y a pas de changements, si x est lié à a mais pas à b, il devient lié à b' dans Γ', enfin si x est lié à b et à a, x sera lié ou non à b' suivant la valeur de $\mu + (1-\zeta)\lambda\nu$ (avec les notations de la figure 4.2). On peut remarquer cependant que si $d = 2$, i.e. si $\zeta = -1$ et que $\lambda\mu\nu \in \mathbf{C} \setminus \mathbf{R}$, alors $\mu = \gamma\overline{\lambda\nu}$ où $\gamma \in \mathbf{C} \setminus \mathbf{R}$, donc $\mu' = \mu - 2\overline{\lambda\nu} = (\gamma - 2)\overline{\lambda\nu} \neq 0$ et x_3 reste lié à b'. De plus on a toujours $\lambda\mu'\nu = (\gamma - 2) \in \mathbf{C} \setminus \mathbf{R}$ (cela nous servira par la suite).

4.2.1 Graphes de racines réels

Le lemme suivant permet de caractériser les graphes de racines réels.

Lemme 4.15: *Soit $\Gamma = (B, w)$ un graphe de racines (ou même un graphe de vecteurs).*

(i) Soit $C = \{e_1, \ldots, e_m\}$ un cycle de Γ[1]. C est complexe (i.e. $\mathrm{W}(C)$ engendre un groupe complexe lorsqu'on voit C comme un sous-graphe de racines de Γ) si $\mathrm{Val}(C)$[2] $:= \prod_{i=1}^{m} (e_i\,|e_{i+1}) \in \mathbf{C} \setminus \mathbf{R}$.

(ii) Γ est réel si et seulement si $w(B) = \{2\}$, et pour tout cycle $C = \{e_1, \ldots, e_m\}$ de Γ, $\prod_{i=1}^{m} (e_i\,|e_{i+1}) \in \mathbf{R}$

[1]Lorsqu'on notera un cycle $C = \{e_1, \ldots, e_m\}$, on posera $e_{m+1} = e_1$ et on supposera qu'on a numéroté les e_i de telle sorte que e_i est relié à e_{i+1} c'est à dire $(e_i\,|e_{i+1}) \neq 0$

[2]$\mathrm{Val}(C)$ dépend de l'ordre dans lequel on parcours C, cependant si C est un cycle minimal, $\mathrm{Val}(C)$ ne va dépendre que de l'orientation du parcours de C, et prendre le parcours dans le sens opposé va changer $\mathrm{Val}(C)$ en son conjugué, et donc n'affectera pas le fait que $\mathrm{Val}(C) \in \mathbf{C} \setminus \mathbf{R}$ ou non, ce qui est ce qui nous intéresse en vertu du Lemme 4.15

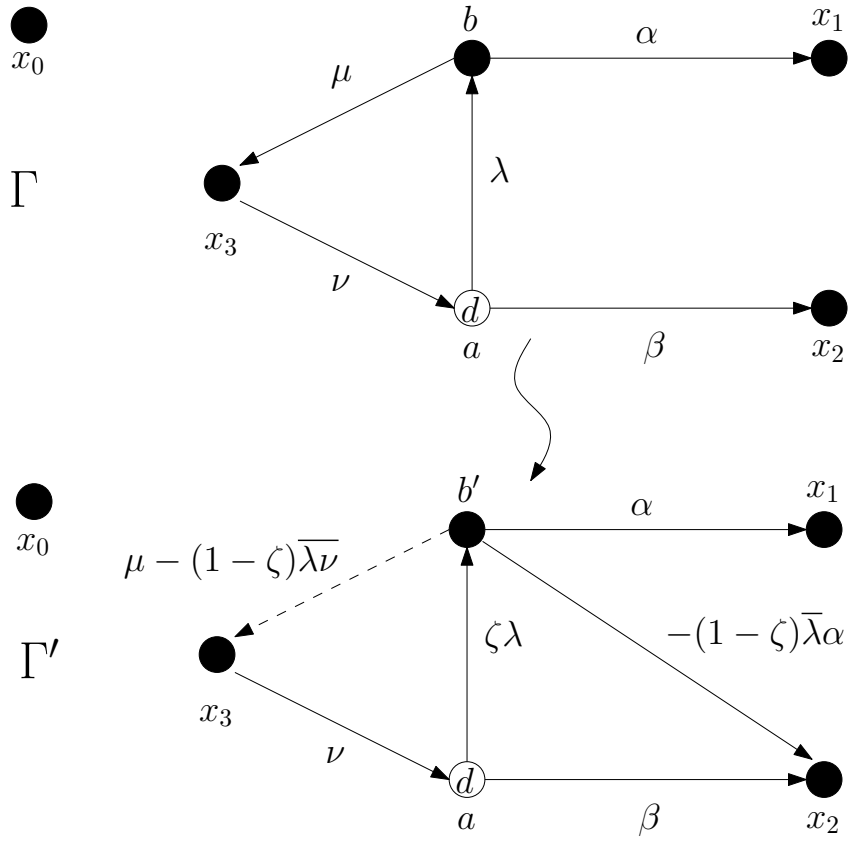


FIG. 4.2 – Γ et Γ' sont équivalents

Corollaire 4.16: *Soit $\Gamma = (B, w)$ un graphe de racines tel que $w(B) = \{2\}$. Alors si Γ n'a pas de cycles, Γ est réel. En particulier un graphe de racines complexe sans cycles est de dimension $d \geqslant 3$.*

DÉMONSTRATION (DU LEMME):

(i) Soit C un cycle comme dans le lemme. On voit facilement que si $\mathrm{W}(C)$ est réel si et seulement s'il existe un graphe de racines C' congruent à C tel que tous les produits scalaires dans C' soient réels (voir la Remarque 1.10). Or prendre un cycle congruent C' ne va pas changer $\prod_{i=1}^{m}(e_i\,|e_{i+1})$, donc si $\prod_{i=1}^{m}(e_i\,|e_{i+1}) \in \mathbf{C} \setminus \mathbf{R}$, $\mathrm{W}(C)$ ne peut pas être réel.
Par contre, parmi ces m produits scalaires, on peut en changer $m-1$ pour qu'ils soient réels, et le dernier le sera ssi $\prod_{i=1}^{m}(e_i\,|e_{i+1}) \in \mathbf{R}$, ce qui va nous servir pour prouver (ii).

(ii) Si $\mathrm{W}(\Gamma)$ contient un sous-groupe complexe, il est également complexe, en particulier si Γ contient un cycle $C = \{e_1, \ldots, e_m\}$ tel $\prod_{i=1}^{m}(e_i\,|e_{i+1}) \in \mathbf{C} \setminus \mathbf{R}$ Γ est complexe. Il en est de même si Γ contient une réflexion d'ordre > 2, ce qui est le cas si $w(B) \neq \{2\}$. Réciproquement, si Γ vérifie les conditions du Lemme 4.15(ii), alors la preuve de (ii) montre que Γ est congru à un graphe dont tous les produits scalaires sont réels, donc $\mathrm{W}(\Gamma)$ est réel. ■

Exemple 4.17: Si Γ est un triangle complexe (i.e. un graphe de racines irréductible complexe de dimension 3) tel que toutes les racines de Γ sont d'ordres 2 alors la transformation décrite dans le Lemme 4.13 donne à nouveau un triangle complexe comme le montrent le Lemme 4.15 et la discussion à la fin de l'Exemple 4.14.

Si $\Gamma = (B, w)$ est un graphe de racines tel que ses racines sont d'ordres 2, alors tous les produits scalaires sont de la forme $(u\,|v) = \cos(k\pi/m)$, avec k premier à m comme on l'a vu dans la discussion qui a conduit à la Définition 4.10. Quitte à remplacer u par une de ses orbites sous l'action de la rotation $s_u s_v$, on peut se ramener à un graphe équivalent où $(u\,|v) = -\cos(\pi/m)$[1]. Si l'on replace $-\cos(\pi/m)$ par m, on tombe sur un graphe de Coxeter. Donc la classification des graphes de Coxeter (cf. [Bou68]) nous donne :

Théorème 4.18: *Tout groupe de réflexions réel et irréductible peut être représenté par l'un des graphes de Coxeter Γ de la Figure 4.3. De plus $d(\Gamma) = d(\mathrm{W}(\Gamma))$.*

En particulier, si $\Gamma = (B, w)$ est un graphe de racines irréductible et sans cycles tel que $w(B) = \{2\}$, alors Γ est équivalent à un graphe de Coxeter irréductible.[2]

4.2.2 Graphes de racines complexes

Lemme 4.19: *Soit $\Gamma = (B, w)$ un graphe de racines irréductible.*

(i) Si G est un groupe de réflexions de dimension n qui contient $\mathrm{W}(\Gamma)$, alors Γ peut être étendu en un graphe de racines Γ' tel que $\mathrm{W}(\Gamma')$ est un sous-groupe de réflexions irréductible de G de dimension n.

(ii) Si Γ est de plus complexe, $w(B) = \{2\}$, $d(\Gamma) = d(\mathrm{W}(\Gamma))$, et $\dim(\Gamma) \geqslant 3$, alors il existe un graphe de racines Γ_0 complexe, irréductible et de dimension 3 tel que $\mathrm{W}(\Gamma_0) \subset \mathrm{W}(\Gamma)$ et $d(\Gamma_0) = d(\mathrm{W}(\Gamma))$.

Démonstration:

(i) Soit W le sev de $\mathbf{C}^n$ engendré par les racines de Γ. On peut supposer que W est un sev propre, sinon $\Gamma' = \Gamma$ convient. Comme G est irréductible, il ne stabilise pas W, et il existe une racine unitaire v de G qui n'est pas dans $W \bigcup W^\perp$. Si l'on rajoute v à Γ (avec $w(v) = o_G(v)$), on obtient un graphe de racines Γ_1 irréductible (car $v \notin W^\perp$) de dimension $\dim(\Gamma) + 1$ (car $v \notin W$). On conclut par récurrence.

(ii) Soit $n = \dim(\Gamma)$. On peut supposer $n > 3$. Par induction, il suffit de construire un graphe de racines Γ_1 de dimension $< n$ tel que $\mathrm{W}(\Gamma_1) \subset \mathrm{W}(\Gamma)$ et $d(\Gamma_1) = d(\Gamma))$. Soit $a, b \in B$ tels que $|(a\,|b)| = \cos(\pi/d(\Gamma)$. Soit $C = \{e_1, \ldots, e_m\}$ un cycle complexe minimal (c'est à dire qui ne contient pas de sous-cycles) de Γ. Comme C est minimal, $(e_i\,|e_j) = 0$ si $|j - i| > 1$ et $\{i, j\} \neq \{1, m\}$. Grâce au Lemme 4.15(ii), on peut supposer que $\prod_{i=1}^{m} (e_i\,|e_{i+1}) \in \mathbf{C} \setminus \mathbf{R}$. Quitte à permuter les (e_i) et (a, b), on peut supposer de plus qu'il existe un chemin

[1] À partir de maintenant, on fera implicitement cette transformation dès que $w(u) = w(v) = 2$

[2] En fait Γ est même un des graphes de Coxeter irréductible si l'on a fait la transformation décrite dans la note 1

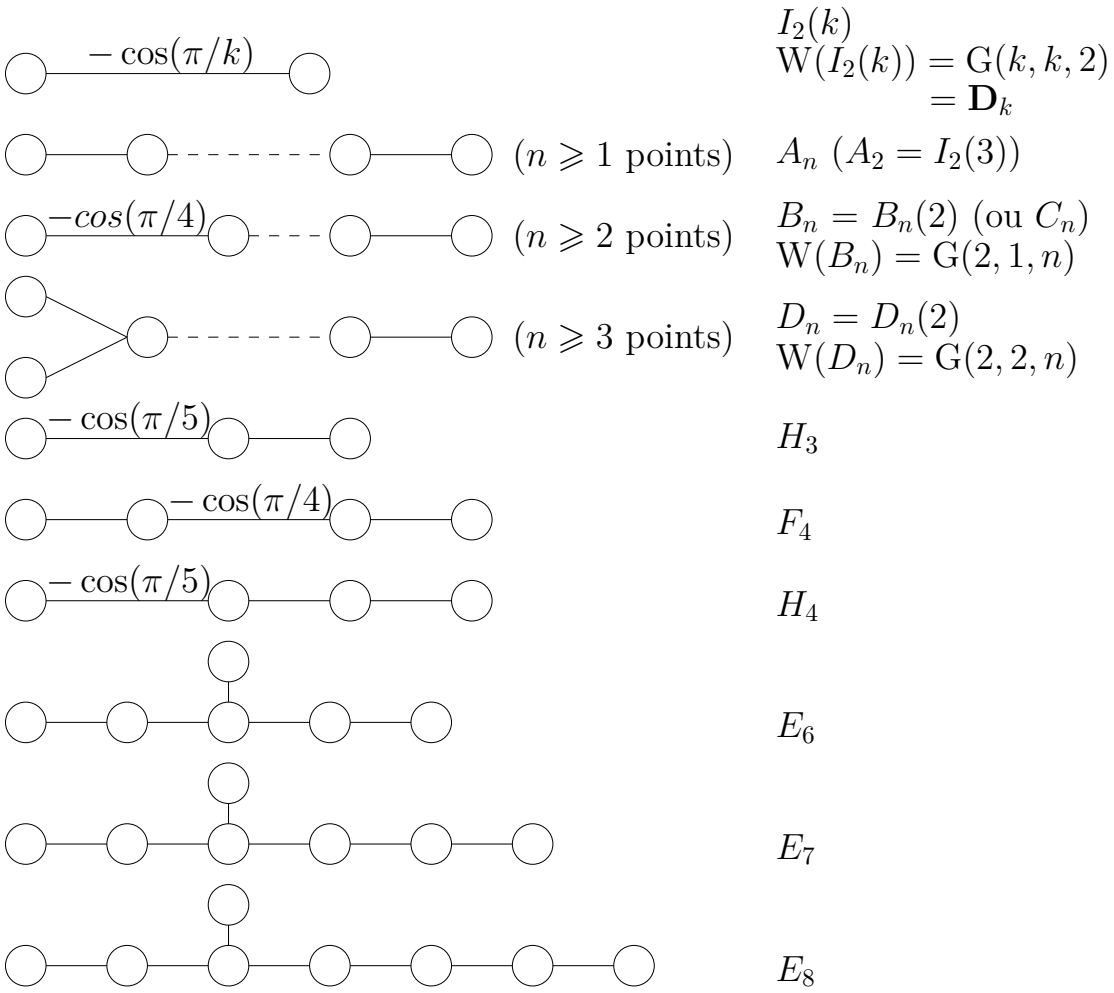


FIG. 4.3 – Les graphes de Coxeter irréductibles

minimal reliant C à $\{a, b\}$ partant de e_1 et arrivant à a. Ainsi si $\{a, b\} \bigcap C \neq \varnothing$, alors $e_1 = a$.

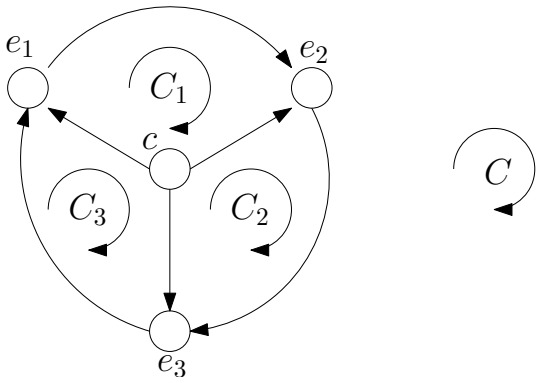
Supposons que $m \geqslant 4$. Si $\{a, b\} \subset C$, alors $a = e_1$ et comme b est lié à a, $b = e_2$ ou $b = e_m$. Quitte à renuméroter, on peut supposer dans tous les cas que $\{a, b\} \bigcap \{e_2, e_3\} = \varnothing$. Alors le sous-graphe Γ_1 engendré par $\{s_{e_2} e_3\} \bigcup B \setminus \{e_2, e_3\}$ convient. En effet il vérifie $d(\Gamma_1) = d(\Gamma)$, et $\dim(\Gamma_1) = \dim(\Gamma)$. Il reste à vérifier que Γ_1 est bien complexe et irréductible. Mais $s_{e_2} e_3 = e_3 - 2\,(e_3\,|e_2\,)\,e_2$, d'où (voir aussi l'Exemple 4.14) :

$$(e_1\,|s_{e_2} e_3\,) = -2\,(e_2\,|e_3\,)\,(e_1\,|e_2\,) \tag{4.1}$$

$$(s_{e_2} e_3\,|e_4\,) = (e_3\,|e_4\,) \tag{4.2}$$

Donc $(e_1\,|s_{e_2} e_3\,) \times (s_{e_2} e_3\,|e_4\,) \times \cdots \times (e_{m-1}\,|e_m\,) \in \mathbf{C} \setminus \mathbf{R}$ (donc en particulier $\neq 0$). Ainsi Γ_1 est bien irréductible, et est complexe par le Lemme 4.15.

On peut donc supposer $m = 3$. Si $\{a, b\} \in C$, $\Gamma_1 = C$ convient. Si $\{a, b\} \bigcap C = \varnothing$, soit c l'unique point vérifiant $(e_1\,|c\,) \neq 0$ dans le chemin minimal reliant e_1 à a. Si $(e_2\,|c\,) \neq 0$ et $(e_3\,|c\,) \neq 0$, on est dans le situation suivante (où l'on ne met pas la valuation des arrêtes) :



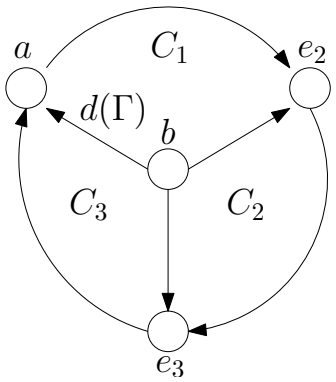
Et l'on vérifie que $\mathrm{Val}(C) = \mathrm{Val}(C_1)\,\mathrm{Val}(C_2)\,\mathrm{Val}(C_3)$ avec l'orientation donnée dans la figure. Donc au moins l'un des cycles C_i est complexe, supposons que ce soit C_1. Le sous-graphe Γ_1 engendré par $B \setminus \{e_3\}$ convient presque, mais il n'est pas forcément irréductible, par contre la composante connexe de Γ_1 qui contient c convient elle, car a et b y apparaissent.

On peut donc supposer $(e_3\,|c\,) = 0$. Si $(e_2\,|c\,) = 0$, l'Exemple 4.14 montre qu'on peut se ramener au cas $(e_2\,|c\,) \neq 0$ en remplaçant e_2 par $s_{e_1} e_2$ (ce qui ne change pas la nature du triangle $\{e_1, e_2, e_3\}$ comme le montre l'Exemple 4.17). Si le triangle $T = \{e_1, e_2, c\}$ est complexe, le graphe Γ_1 engendré par $B \setminus \{e_3\}$ convient (quitte à prendre la composante connexe contenant c). S'il est réel, alors on se ramène au cas précédent en remplaçant e_1 par $s_{e_3} e_1$. En effet $(c\,|s_{e_3} e_1\,) = (c\,|e_1\,)$, $(s_{e_3} e_1\,|e_2\,) = (e_1\,|e_2\,) - 2\,(e_1\,|e_3\,)\,(e_3\,|e_2\,) = (e_1\,|e_2\,) - 2\gamma\,(e_1\,|e_2\,)$ où $\gamma = \mathrm{Val}(C) \in \mathbf{C} \setminus \mathbf{R}$. Alors si $T' = \{s_{e_3} e_1, e_2, c\}$, $\mathrm{Val}(T') = (1 - 2\gamma)\,\mathrm{Val}(T) \in \mathbf{C} \setminus \mathbf{R}$ et T' est bien complexe.

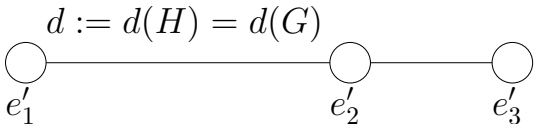
Enfin, il reste le cas $e_1 = a$ et $b \notin C$. On peut raisonner comme dans le cas précédent avec $c = b$: si par exemple $(e_3\,|b\,) = 0$, les transformations décrites dans le paragraphe précédent fonctionnent toujours, il faut juste vérifier

que dans Γ_1 que l'on construit, on a bien $d(\Gamma_1) = d(\Gamma)$ mais c'est le cas car $(s_{e_3} a \,|\, b) = (a \,|\, b)$.

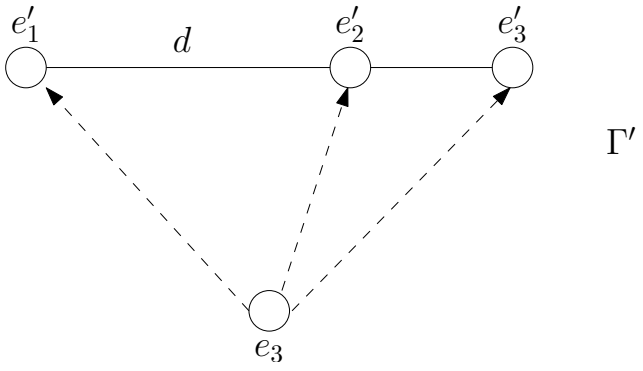
Il ne nous reste plus qu'à traiter le cas $(e_2 \,|\, b) \neq 0$ et $(e_3 \,|\, b) \neq 0$:



Si C_1 ou C_3 sont non réels, on raisonne comme dans le cas précédent : on peut enlever e_3 ou e_2. Si ce n'est pas le cas, C_2 est complexe, mais on ne peut cette fois enlever a sous peine de risquer de diminuer $d(\Gamma_1)$[1]. On peut supposer que $B = \{a, b, e_2, e_3\}$ sinon le graphe Γ_1 engendré par ces éléments convient. Soit $H = \mathrm{W}(C_1)$. $d(G) = d(C_1) \leqslant d(H) \leqslant d(G)$ donc $d(H) = d(G)$. Comme C_1 est réel irréductible, la classification des graphes de Coxeter du Théorème 4.18 montre que C_1 est équivalent à

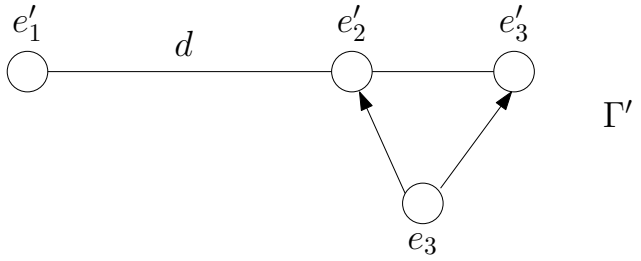


donc Γ est équivalent à Γ' :



Comme G est irréductible et complexe, Γ' contient au moins un triangle complexe. Si ce triangle contient e'_1 et e'_2 ce triangle convient. Sinon on est par exemple dans le cas suivant :

[1] C'est d'ailleurs une erreur que fait [Coh76] dans la preuve du Lemme 4.5, page 401

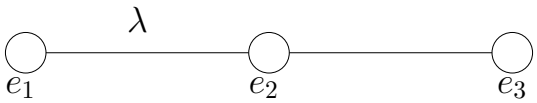


mais ici $(e'_1 \,|e'_3\,) = 0$ et l'on revient à un cas connu ($a = e'_2$, $b = e'_1$), ce qui conclut la preuve. ■

Théorème 4.20: *Soit G un groupe de réflexions complexe irréductible de dimension $n \geqslant 3$ dont toutes les réflexions sont d'ordres 2. Alors il existe un graphe de racines Γ complexe, irréductible et de dimension 3 tel que $\mathrm{W}(\Gamma) \subset G$ et $d(\Gamma) = d(G)$.*

DÉMONSTRATION: On procède par récurrence sur n. Comme les réflexions de G sont d'ordres 2, les graphes de racines que l'on considère auront des racines d'ordres 2.

Soit $\lambda = \cos(\pi/d(G))$. Il existe par définition des racines unitaires e_1 et e_2 de G telles que $(e_1\,|e_2\,) = \lambda$ (cf. la discussion qui précède la Définition 4.10 ainsi que celle qui précède le Théorème 4.18). On ajoute une racine unitaire e_3 de manière à former un graphe de racines irréductible Γ_0 (cf. le Lemme 4.19(i)). Si Γ_0 est complexe, $\Gamma = \Gamma_0$ convient. Sinon Γ_0 est réel, donc par le Théorème 4.18, Γ_0 est équivalent à :



Supposons que $n = \dim G = 3$. Comme (e_1, e_2, e_3) sont libres [1], ils forment une base des racines de G. Si pour tout réflexion s de G il existait une racine a de s telle que $(a\,|e_i\,) \in \mathbf{R}$ pour $i = 1, 2, 3$, G serait réel. Donc il existe une réflexion s de G pour laquelle ce n'est pas le cas, c'est à dire il existe une racine unitaire v de G telle que :

$$\text{pour tout } \alpha \in \mathbf{U}, \text{ il existe un } i \text{ tel que } \alpha\,(v\,|e_i\,) \in \mathbf{C} \setminus \mathbf{R} \tag{4.3}$$

On remarque que $s_{e_i} v$ satisfait aussi à (4.3), en effet si par exemple $v' = s_{e_1} v = v - 2\,(v\,|e_1\,)\,e_1$, on a (cf. l'Exemple 4.14) :

$$\begin{aligned}
(v'\,|e_1\,) &= -\,(v\,|e_1\,) \\
(v'\,|e_2\,) &= (v\,|e_2\,) - 2\,(v\,|e_1\,)\,(e_1\,|e_2\,) \\
(v'\,|e_3\,) &= (v\,|e_3\,)
\end{aligned}$$

donc si $(v'\,|e_1\,)$ et $(v'\,|e_3\,)$ sont réels, $(v\,|e_2\,)$ est complexe, et $(v'\,|e_2\,)$ l'est aussi. Le même raisonnement montre que si on change e_j par $s_{e_i} e_j$, v satisfait toujours (4.3).

Comme v satisfait à (4.3), il est relié à au moins deux (e_i), s'il n'est pas relié à e_1, il est relié à e_2 et quitte à prendre $v' = s_{e_2} v$, on peut supposer que v est lié à

[1] On voit ainsi l'intérêt d'imposer la condition que les racines soient libres dans un graphe de racines

e_1. Quitte à multiplier v par un $\lambda \in \mathbf{U}$, on peut même supposer que $(v\,|e_1\,) \in \mathbf{R}^\star$. Si v, e_1, e_2 sont linéairement dépendants, alors $v = \lambda e_1 + \mu e_2$ car (e_1, e_2) sont libres. Alors $v, e_1, s_{e_3}e_2$ sont libres, sinon on aurait $v = \lambda' e_1 + \mu' s_{e_3}e_2 = \lambda' e_1 + \mu' e_2 - \mu' e_3$, donc par liberté de e_1, e_2, e_3, on aurait $\mu = \mu' = 0$, et v serait proportionnel à e_1 ce qui contredit (4.3). Donc quitte à remplacer e_2 par $s_{e_3}e_2$, ce qui ne change pas la nature de Γ_0 ni celle de v comme on l'a vu, on peut supposer que v, e_1, e_2 sont libres. Soit

$$B_1 = \{e_1, e_2, v\}\,, B_2 = \{e_1, s_{e_2}e_3, v\}\,, B_3 = \{s_{e_2}e_1, e_3, v\}$$
$$B_4 = \{e_2, e_3, v\} \text{ et } B_5 = \{e_2, e_3, s_{e_2}v\}$$

et Γ_i le graphe de vecteur engendré par B_i. Supposons qu'aucun des Γ_i ne soit un graphe de racines irréductible complexe tel que $d(\Gamma_i) = d(G)$.

Comme Γ_1 est un graphe de racines irréductible tel que $d(\Gamma_1) = d(G)$, Γ_1 est réel. Or $(e_1\,|e_2\,)\,, (v\,|e_1\,) \in \mathbf{R}^\star$, donc $(v\,|e_2\,) \in \mathbf{R}$ par le Lemme 4.15(i). Donc $(e_3\,|v\,) \in \mathbf{C}\backslash\mathbf{R}$ (par (4.3)), et $(v\,|s_{e_2}e_1\,) \in \mathbf{R}$.

Si $e_1, s_{e_2}e_3, v$ sont libres, Γ_2 est un graphe de racines tel que $d(\Gamma_2) = d(G)$ car $(e_1\,|s_{e_2}e_3\,) = (e_1\,|e_2\,)$ vu que $s_{e_2}e_3 = e_3 - 2 \times (-1/2)e_2 = e_2 + e_3$. Mais $(e_1\,|v\,) \in \mathbf{R}^\star$, $(s_{e_2}e_3\,|e_1\,) \in \mathbf{R}^\star$ et $(v\,|s_{e_2}e_3\,) \in \mathbf{C} \setminus \mathbf{R}$ vu que $(v\,|e_2\,) \in \mathbf{R}$ et $(v\,|e_3\,) \notin \mathbf{R}$. Donc Γ_2 est complexe, contradiction. Donc

$$v = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_2 e_3 \tag{4.4}$$

On a $(v\,|e_3\,) = \lambda_2/2 \in \mathbf{C} \setminus \mathbf{R}$ donc $\lambda_2 \in \mathbf{C} \setminus \mathbf{R}$ et $\lambda_1 \neq 0$ sinon $\alpha = 1/\lambda_2$ contredirait (4.3).

Notons que $(v\,|s_{e_2}e_1\,) \in \mathbf{R}$ et que $(s_{e_2}e_1\,|e_3\,) = (e_1\,|s_{e_2}e_3\,) = (e_1\,|e_2\,)$. Donc si $(v\,|s_{e_2}e_1\,) \neq 0$, le même raisonnement que pour le graphe Γ_2 s'applique au graphe Γ_3 et on obtient que

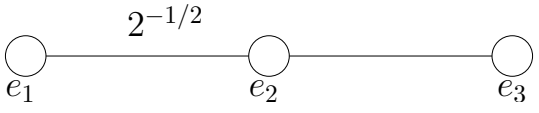
$$v = \lambda_1' e_1 - 2\lambda\lambda_1' e_2 + \lambda_2' e_3 \tag{4.5}$$

Comme e_1, e_2, e_3 sont libres, (4.4) et (4.5) donnent $v = \lambda_1(s_{e_2}e_1 - 2\lambda e_3)$ ce qui contredit (4.3) avec $\alpha = 1/\lambda_1$.

Donc $(v\,|s_{e_2}e_1\,) = \lambda_1(1 - 2\lambda^2) = 0$, or $\lambda_1 \neq 0$ donc $\lambda = 2^{-1/2} = \cos(\pi/4)$. D'où $d(G) = 4$.

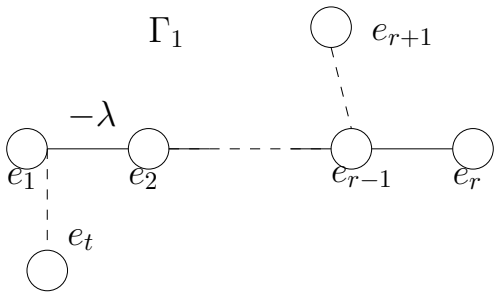
On a $(v\,|e_2\,) \neq 0$ car $(v\,|e_1\,) \neq 0$ et $(v\,|s_{e_2}e_1\,) = 0$, d'où $(v\,|e_2\,) \in \mathbf{R}^\star$. v, e_2, e_3 sont libres par (4.4), donc Γ_4 est un graphe de racines complexe. Si $|(v\,|e_i)| = 2^{-1/2}$ pour $i = 2$ ou 3, on obtient à nouveau une contradiction. Donc on peut supposer (quitte à remplacer v par $-v$) que $(v\,|e_2\,) = |(v\,|e_3)| = \cos(\pi/3) = 1/2$. D'où $2\,(v\,|e_2\,) = \lambda_1\sqrt{2} + \lambda_2 = 1$ et $2\,|(v\,|e_3)| = |\lambda_2| = 1$. Le même raisonnement appliqué au graphe de racines Γ_5 qui est complexe car $(s_{e_2}v\,|e_2\,) \in \mathbf{R}$ et $(s_{e_2}v\,|e_3\,) \in \mathbf{C} \setminus \mathbf{R}$ donne $|(s_{e_2}v\,|e_3\,)| = |(v\,|e_3\,) + (e_2\,|v\,)| = \left|\lambda_1/\sqrt{2} + \lambda_2\right| = 1/2$. En regroupant ces équations, on voit que λ_2 est unitaire et vérifie $|1 + \lambda_2| = 1$. Ceci implique que $\lambda_2 \in \{j, j^2\}$.

Pour résumer, on est dans la situation suivante :



avec $v = 2^{-1/2}(1-\lambda_2)e_1 + \lambda_2 e_2 + \lambda_2 e_3$ où $\lambda_2 \in \{j, j^2\}$. (on rappelle que l'arrête non valuée entre e_2 et e_3 signifie que $(e_2\,|e_3\,) = -1/2$.) On vérifie alors que la transformation linéaire t telle que $te_1 = -\varepsilon_3$, $te_2 = 2^{-1/2}(\varepsilon_2 - \varepsilon_3)$, $te_3 = 2^{-1/2}(\varepsilon_1 - \varepsilon_2)$ est unitaire. De plus $tv = 2^{-1/2}(\lambda_2\varepsilon_1 - \varepsilon_3)$. Donc le groupe $\langle s_v, s_{e_1}, s_{e_2}, s_{e_3}\rangle$ est conjugué à $\mathrm{G}(6,3,3)$ (cf. cf. la Définition 2.6 et la Remarque 2.7 : avec les notations de la preuve du Théorème 2.8, on a $d = 2$, l'ordre de -1 et $m = 6$, l'ordre de $-\lambda_2$). Mais l'Exemple 4.12 donne $d(\mathrm{G}(6,3,3) = 6$ or $d(\mathrm{G}(6,3,3)) \leqslant d(G)$ puisque $\mathrm{G}(6,3,3) \subset G$ alors qu'on a vu que $d(G) = 4$. On obtient une contradiction, et celà fini la preuve du Théorème pour $n = 3$.

Supposons maintenant que $n > 3$. Soit H un sous-groupe de réflexions réel irréductible maximal (pour ces propriétés) de G contenant $\mathrm{W}(\Gamma_0)$ (ainsi $d(H) = d(G)$). H étant réel, le Théorème 4.18, il est représenté par un graphe de Coxeter $\Gamma_1 = (B_1, w_1)$, $B_1 = \{e_1, \ldots, e_r, \ldots, e_t\}$. On suppose que l'on a numéroté les e_i de telle sorte que $(e_1\,|e_2\,) = -\cos(\pi/d(G))$, $(e_{i-1}\,|e_i\,) = -1/2, 3 \leqslant i \leqslant r$ et e_r soit un point terminal de Γ_1 (c'est à dire que seul e_{r-1} est relié à e_r). C'est toujours possible comme le montre la figure 4.3 :



Comme G est complexe, il existe une racine unitaire v telle que $s_v \in G \setminus H$. Si on pose $v' = s_{e_r}v = v - 2\,(e_r\,|v\,)\,e_r$, v' est racine de la réflexion $s_{e_r}s_v s_{e_r} \in G \setminus H$. Supposons que v ou v' soit linéairement dépendant de $e_1, \ldots, e_{r-1}, e_{r+1}, \ldots, e_t$, et soit $H' = \langle \{s_{e_i}, i \neq r\}, s_v\rangle$. Si H' est réel, il existe un multiple λv de v qui appartient à $\mathbf{R}e_1 \oplus \cdots \oplus \mathbf{R}e_{r-1} \oplus \mathbf{R}e_{r+1} \oplus \cdots \oplus \mathbf{R}e_t$, donc $(\lambda v\,|e_r\,) \in \mathbf{R}$ et $\langle H', e_r\rangle$ est réel. Mais $\langle H', e_r\rangle \supsetneq H$ et celà contredit la définition de H. Donc H' est complexe, de dimension $< \dim(G)$, et l'hypothèse de récurrence appliquée à H' permet de conclure.

Donc $v, e_1, \ldots, e_r, e_{r+1}, \ldots, e_t$ engendre un graphe de racines Γ_v, et on peut suupposer que Γ_v est réel grâce au Lemme 4.19(ii). De plus v est relié à l'un des $e_i, i \neq r$ car sinon $e_1, \ldots, e_t, v$ serait un graphe de vecteurs sans cycle, donc réel, ce qui contredit la maximalité de H. Comme e_r est un point terminal de Γ_1, $e_1, \ldots, e_{r-1}, e_{r+1}, \ldots, e_t$ est connexe, donc Γ_v l'est aussi. De même $v', e_1, \ldots, e_r, e_{r+1}$, $\ldots, e_t$ engendre un graphe de racines $\Gamma_{v'}$ réel irréductible.

Ainsi, quitte à remplacer v par un multiple, on peut supposer que $(v\,|e_i\,) \in \mathbf{R}$ si $i \neq r$. De plus il existe un $j \neq r$ tel que $(v\,|e_j\,) \neq 0$. Quitte à changer v par un élément de $\langle s_{e_i}, i \neq r, r-1\rangle$ (cf. le Lemme 4.13), on peut supposer que $(v\,|e_{r-1}\,) \neq 0$. On a donc $(v'\,|e_{r-1}\,) \in \mathbf{C} \setminus \mathbf{R}$ et $(v'\,|e_i\,) \in \mathbf{R}$ si $i < r-1$ (car alors $(e_i\,|e_r\,) = 0$). Donc $(v'\,|e_i\,) = 0$ si $i < r-1$ sinon on aurait un cycle complexe dans $\Gamma_{v'}$ par le Lemme 4.15(i). D'où $(v\,|e_i\,) = 0$ si $i < r-1$.

Posons $u = e_2 + e_3 + \cdots + e_{r-1} = s_{e_2}s_{e_3}\ldots s_{e_{r-2}}e_{r-1}$. u est une racine unitaire de H telle que $(e_1\,|u\,) = -\cos(\pi/d(G))$. Si v est une combinaison linéaire de e_1, u

et e_r, alors $K = \langle v, e_1, u, e_r \rangle$ est un groupe de dimension 3, irréductible (car e_1, u, e_r engendre un graphe de racines irréductible) et complexe (car v, u, e_r est un cycle complexe puisque $(v\,|u) \in \mathbf{R}^\star$, $(u\,|e_r) \in \mathbf{R}^\star$ et $(e_r\,|v) \in \mathbf{C} \setminus \mathbf{R}$). Or $d(K) = d(G)$, donc le cas $n = 3$ précedemment traité nous permet de conclure.

On peut donc supposer que v, e_1, u et e_r sont libres. Posons $v'' = s_{e_r} s_u v = v - 2\,(e_{r-1}\,|v)\,u - 2\,((v\,|e_r) + (e_{r-1}\,|v))\,e_r$. Alors

$$(v''\,|e_1) = -2\,(e_2\,|e_1)\,(v\,|e_{r-1}) \in \mathbf{R}^\star \quad \text{et} \quad (v''\,|u) = (v\,|e_r) \in \mathbf{C} \setminus \mathbf{R}$$

Donc puisque v'', u, e_1 sont libres, ils forment le triangle complexe Γ que l'on cherchait. ■

Corollaire 4.21: *Soit G comme dans le Théorème 4.20. Supposons de plus que G est primitif et vérifie $n \geqslant 8 - d(G) \geqslant 4$. Alors il existe un graphe de racines Γ primitif, complexe, de dimension $8 - d(G)$ tel que $d(\Gamma) = d(G)$ et $\mathrm{W}(\Gamma) \subset G$. (En fait, Γ peut être obtenu comme une extension de n'importe quel graphe de racines Γ_0 qui vérifie les conditions du Théorème 4.20).*

DÉMONSTRATION: Par le Théorème 4.20, il existe un graphe de racines Γ_0 complexe, irréductible de dimension 3 tel que $d(\Gamma_0) = d(G)$ et $\mathrm{W}(\Gamma_0) \subset G$. Le Lemme 4.19(i) nous dit que l'on peut étendre Γ_0 en un graphe de racines Γ_1 complexe de dimension $7 - d(G)$.

Si Γ_1 est primitif, il n'est pas conjugué à $\mathrm{A}_{7-d(G)}$ car il est complexe. Si on étend Γ_1 en un graphe de racines Γ irréductible de dimension $8 - d(G)$ il sera primitif par le Lemme 2.10.

Si Γ_1 est imprimitif, il n'est pas conjugué à $\mathrm{G}(2, 2, 4)$ (qui est réel), ni à $\mathrm{G}(3, 3, 3)$ (car $d(G(3, 3, 3) = 3$, et si $7 - d(G) = 3$, $d(\mathrm{W}(\Gamma_1)) = d(G) = 4$). Donc il a un unique système d'imprimitivité par le Lemme 2.11, et donc la Proposition 2.12 permet de conclure. ■

Remarque 4.22: La même preuve montre que si $n \geqslant 4$ et $d(G) = 5$, il exsite un graphe de racines Γ de dimension 4, primitif et complexe tel que $d(\Gamma) = 5$ et $\mathrm{W}(\Gamma) \subset G$.

4.3 Systèmes de racines

Définition 4.23 (Présystème de racines): Un présystème de racines est la donnée d'un couple $\Sigma = (R, f)$ tel que :

(i) R (l'ensemble des préracines du système) est un ensemble fini d'éléments non nuls de $\mathbf{C}^\infty$.

(ii) f (la valuation) est une application $f : R \to \mathbf{N} \setminus \{0, 1\}$ qui vérifie $\forall a, b \in R$:

$$s_{a,f(a)} R = R, \quad f(s_{a,f(a)}) b = f(b)$$

et $f(a) = f(b)$ si $a, b \in R$ sont proportionnels.

Si R est inclus dans un sous-espace vectoriel V de $\mathbf{C}^\infty$, on dit que Σ est un présystème de racines de V.

On dit que Σ est isomorphe à $\Sigma' = (R', f')$ s'il existe une transformation unitaire qui envoie R sur R' et f sur f'.

Définition 4.24: À un présystème de racines $\Sigma = (R, f)$, on peut associer un groupe de réflexions $\mathrm{W}(\Sigma)$[1] avec :

$$\mathrm{W}(\Sigma) = \langle s_{a,f(a)}, a \in R \rangle$$

Remarque 4.25:

- Si Σ est isomorphe à Σ', alors $\mathrm{W}(\Sigma)$ est isomorphe à $\mathrm{W}(\Sigma')$.
- À cause de la Définition 4.23(ii), on voit que remplacer $v \in R$ par un multiple λv muni de la même valuation donne un système de racines (si on remplace aussi les orbites de v sous l'action de $\mathrm{W}(\Sigma)$ par le même multiple) essentiellement pareil (« congru ») à Σ, et qui donne le même groupe de réflexions. Il en va de même quand on rajoute au système de racines λv (et son orbite sous $\mathrm{W}(\Sigma)$) avec la même valuation. Par la suite on identifiera deux système de racines semblable par ses opérations, autrement dit même on suppose implicitement lorsqu'on parle d'un vecteur non unitaire v du système de racines que l'on considère en réalité $v/|v|$. On ne travaille pas directement sur des vecteurs unitaires pour simplifier les calculs, voir l'Exemple 4.35.

Définition 4.26 (Système de racines): Un présystème de racines $\Sigma = (R, f)$ est un système de racines ssi $\forall a \in R$

$$\alpha a \in R \quad \Leftrightarrow \quad \alpha a \in \mathrm{W}(\Sigma).a \quad (\alpha \in \mathbf{C}) \tag{4.6}$$

Exemple 4.27:

(i) Si $\Gamma = (B, w)$ est un graphe de racines, alors $R = \mathrm{W}(\Gamma).B$ et $f : R \to \mathbf{N}$ induite par la fonction $o_{\mathrm{W}(\Gamma)}$ donnent un système de racines Σ tel que $\mathrm{W}(\Sigma) = \mathrm{W}(\Gamma)$. (Attention: même si $b \in B$, on n'a pas forcément $f(b) = w(b)$).

(ii) Soit G est un groupe de réflexions dans $V \subset \mathbf{C}^\infty$. Pour toute réflexion $s \in G$, on choisit une racine unitaire $a_s \in V$. Soit $R_0 = \{a_s, s \in \mathrm{Ref}(G)\}$, et définissons $f_0 : R_0 \to \mathbf{N}$ par $f_0(a) = o_G(a)$. Alors $R = G.R_0$, muni de $f : R \to N$ qui étend f_0 par $f(g.a) = f_0(a)$ si $a \in R_0$, $g \in G$[2] forme un présystème de racines de V. (Et si on choisit R_0 de manière à ce que si a_s est multiple de $a_{s'}$, alors $a_s = a_{s'}$, on obtient même un système de racines.)

Lemme 4.28: *Soit $\Sigma = (R, f)$ un présystème de racines.*

(i) $\mathrm{Ref}(\mathrm{W}(\Sigma)) = \left\{ s^j_{a,f(a)}, a \in R, 0 < j < f(a) \right\}$. *En particulier, les racines de* $\mathrm{W}(\Sigma)$ *sont* $\mathbf{C}.R$.

(ii) Il existe un système de racines $\Omega = (S, g)$ tel que $\mathrm{W}(\Omega) = \mathrm{W}(\Sigma)$, $S \subset R$ et $g = f|_S$

[1] $\mathrm{W}(\Sigma)$ est fini car il fixe $R^\perp$, donc c'est un groupe de permutation de R

[2] f est bien définie, en fait f est la restriction de o_G à R

(iii) Si $\Delta \subset R$ *est tel que* $\mathrm{W}(\Sigma) = \langle s_{a,f(a)}, a \in \Delta \rangle$*, alors pour toute racine* x *de* $\mathrm{W}(\Sigma)$ *est dans* $\mathbf{C}\,\mathrm{W}(\Sigma).\Delta$*. En particulier, toute réflexion de* $\mathrm{W}(\Sigma)$ *est conjuguée à* $s^j_{a,f(a)}$ *pour certains* $j \in \mathbf{N}$ *et* $a \in \Delta$*, et si* x *et* y *sont des racines unitaires de* $\mathrm{W}(\Sigma)$*, alors* $(x\,|y) \subset \{((u/\,|u|)\,|(v/\,|v|))\,, u, v \in \Delta\}$

Si de plus Σ *est un système de racines, alors* R *est formé des orbites de* Δ *par* $\mathrm{W}(\Sigma)$*. En particulier si* $x, y \in R$ *alors* $(x\,|y) \subset \{(u\,|v)\,, u, v \in \Delta\}$

Démonstration:

(i) Soit $T = \{v \in \mathbf{C}^\infty, \mathbf{C}v \bigcap R \neq 0\}$, et $u \in \mathbf{C}^\infty \setminus T$ une racine de $\mathrm{W}(\Sigma)$ d'ordre $m > 1$. $\mathrm{W}(\Sigma)$ laisse R invariant, et donc T aussi. La Proposition 1.28 nous fournit un caractère linéaire $\chi : \mathrm{W}(\Sigma) \to \mathbf{C}^\star$ tel que pour toute réflexion $r \in \mathrm{W}(\Sigma)$:

$$\chi(r) = \begin{cases} \det(r) & \text{si } r \text{ a une racine dans } T \\ 1 & \text{sinon} \end{cases}$$

Mais comme $\mathrm{W}(\Sigma)$ est engendré par les $s_{a,f(a)}$, $a \in R$, χ coincide avec det, donc $1 = \chi(s_{u,m}) = \det(s_{u,m})$, ce qui est absurde. Ainsi T est bien l'ensemble des racines de $\mathrm{W}(\Sigma)$.

Soit maintenant s une réflexion de $\mathrm{W}(\Sigma)$, de valeur propre $\zeta \neq 1$. On a vu que s a une racine $a \in R$. Il reste à vérifier que l'ordre de s divise $f(a)$. Posons $Q = \mathrm{W}(\Sigma).(\mathbf{C}^\star a)$. La Proposition 1.28 nous donne à nouveau un caractère linéaire $\varphi : \mathrm{W}(\Sigma) \to \mathbf{C}^\star$ tel que pour toute réflexion $r \in \mathrm{W}(\Sigma)$:

$$\chi(r) = \begin{cases} \det(r) & \text{si } r \text{ a une racine dans } Q \\ 1 & \text{sinon} \end{cases}$$

Il existe $a_1, \ldots, a_l \in R$ (avec multiplicités) tels que $s = s_{a_1,f(a_1)} \ldots s_{a_l,f(a_l)}$, d'où $\zeta = \prod_{a_i \in Q} \det s_{a_i,f(a_i)}$. Or si $a_i \in Q$, a_i est dans l'orbite de $\mathbf{C}^\star a$ par $\mathrm{W}(\Sigma)$, donc la Définition 4.23(ii) montre que $f(a_i) = f(a)$. Ainsi l'ordre de ζ est un diviseur de $f(a)$, ce qu'on voulait.

(ii) Soit $U = \{\mathbf{C}^\star u, u \text{ racine de } \mathrm{W}(\Sigma)\}$, et $u_1, \ldots, u_l \in R$ des éléments tels que $\{\mathbf{C}^\star u_i\}$ est un système de représentants des orbites de $\mathrm{W}(\Sigma)$ dans U. Posons $\Omega = (S, g)$ où $S = \bigcup_{i=1}^{l} \mathrm{W}(\Sigma)u_i$ et $g = f|_S$. On vérifie immédiatement que $S \subset R$, $\mathrm{W}(\Sigma)$ stabilise S donc S est un présystème de racines, $\mathrm{W}(\Omega) = \mathrm{W}(\Sigma)$ et S est un système de racines par le choix des (u_i).

(iii) On définit un présystème de racines $\Sigma_1 = (R_1, f_1)$ avec $R_1 = \mathrm{W}(\Sigma).\Delta$ et $f_1 = f|_{R_1}$ (ce qui garantit que Σ_1 est bien un présystème de racines ; f_1 est l'unique extension à R_1 de $f|_\Delta$ stable par l'action de $\mathrm{W}(\Sigma)$). Par définition de Δ, $\mathrm{W}(\Sigma_1) = \mathrm{W}(\Sigma)$, donc on peut appliquer (i) : si x est une racine, il existe $\alpha \in \mathbf{C}^\star$ tel que $\alpha x \in R_1 = \mathrm{W}(\Sigma).\Delta$, donc il existe $a \in \Delta$ tel que $\alpha x \in \mathrm{W}(\Sigma).a$. Si Σ est un système de racines et $x \in R$ on peut prendre $\alpha = 1$, donc R est bien une réunion d'orbites de Δ par $\mathrm{W}(\Sigma)$.

Les cas particuliers s'en déduisent immédiatement, car quitte à changer x par un multiple, on peut supposer que $x \in R$, dans ce cas $\alpha x \in R_1 \subset R$ donc $f(x) = f(\alpha x) = f(a)$ et $s_{x,f(x)}$ est conjugué à $s_{a,f(a)}$ (ce qui donne bien le cas

général puisque toute réflexion est de la forme $s^j_{x,f(x)}, x \in R$ d'après (i)). De plus $\mathrm{W}(\Sigma)$ est formé d'automorphismes unitaires, donc son action ne change pas le produit scalaire. ■

Comme tout ce qui concerne les éléments réguliers, la deuxième partie du lemme suivant sert à calculer les invariants associés à un groupe de réflexions donné. Nous ne nous en servirons pas (nous renvoyons à [Coh76] pour quelques exemples de calculs effectifs à la main, et à [GAP06] pour les calculs automatiques). Nous la montrons juste par souci de complétude et pour donner une idée de l'intérêt des système de racines.

Lemme 4.29: *Soit $\Sigma = (R, f)$ un système de racines.*

(i) Soit Δ comme dans le Lemme 4.28(iii) et soit A un sous-anneau de $\mathbf{C}$ tel que $\exp(2\pi i/m) \in A$ pour tout $m \in f(\Delta)$, et $(a\,|a) \in A, (b\,|a)\,(a\,|a)^{-1} \in A$ pour tous $a, b \in \Delta$. Alors $(b\,|a)\,(a\,|a)^{-1} \in A$ pour tous $a, b \in R$ et $\mathrm{W}(\Sigma)$ est défini sur le corps des fractions de A.

(ii) Si g est un élément régulier de $\mathrm{W}(\Sigma)$, l'ordre de g est un diviseur de $|R|$.

Démonstration:

(i) On a

$$\left(s^k_{a,f(a)} b\,|c\right) = (b\,|c) - (1 - \exp(2\pi i k f(a)^{-1})\,(b\,|a)\,(a\,|c)\,(a\,|a)^{-1} \in A$$

(pour tout $a, b, c \in \Delta$ et $k \in \mathbf{N}$), une induction immédiate nous permet de conclure vu que $R = \mathrm{W}(\Sigma)\Delta$.

(ii) Si $g \in \mathrm{W}(\Sigma)$ est régulier, il permute les éléments de R. De plus s'il est non trivial, il ne fixe pas d'éléments de R, en effet v est un vecteur régulier de g, de valeur propre ζ, alors $\zeta \neq 1$ par le Théorème 1.26. D'où s'il $a \in R$ est fixé par g, $(v\,|a) = (g.v\,|g.a) = \zeta\,(v\,|a)$, absurde. Ainsi les orbites de g dans R ont toutes la même longueur : l'ordre de g (car c'est l'ordre par $\langle g \rangle$ de v, cf. le Théorème 1.26). ■

Corollaire 4.30: *Soit $\Gamma = (B, w)$ un graphe de racines tel que $w(B) = \{2\}$. Alors $d(\Gamma) = d(\mathrm{W}(\Gamma))$.*

Démonstration: En effet, si l'on note $\Sigma = (R, f)$ le système de racines associé à Γ par l'Exemple 4.27, alors comme $G = \mathrm{W}(\Gamma)$ n'a que des réflexions d'ordres 2, $f(R) = \{2\}$. Et B vérifie la condition du Lemme 4.28(iii). Comme les éléments de B sont unitaires, $A = \mathbf{Z}[\exp(2i\pi/d(\Gamma))]$ vérifie la conditon du Lemme 4.29(i). Donc les produits scalaires des éléments de R sont dans A, et comme chaque réflexion a une racine dans R, on voit que $d(G) = d(\mathrm{W}(\Gamma))$. ■

Exemple 4.31:

(i) Posons

$$R(m,m,n) = \mu_2\mu_m \left\{ e^{2\pi il/m}\varepsilon_i - \varepsilon_j, i,j,l \in \mathbf{N}, i \neq j, 1 \leqslant i,j \leqslant n \right\}$$

et soit $f_{m,m,n} : R(m,m,n) \to \mathbf{N}$ la fonction constante 2. Alors $\Sigma(m,m,n) = (R(m,m,n), f_{m,m,n})$ est un système de racines qui vérifie $\mathrm{W}(\Sigma(m,m,n)) = \mathrm{G}(m,m,n)$ et $|R(m,m,n)| = m^2n(n-1)\,\mathrm{pgcd}(m,2)^{-1}$

(ii) Posons $m = de$. Soit $R(de,e,n) = R(m,m,n) \bigcup \mu_d \{\varepsilon_k, 1 \leqslant k \leqslant n\}$ et $f_{de,e,n} : R(de,e,n) \to \mathbf{N}$ l'extension de $f_{m,m,n}$ qui envoie ε_i sur d. Alors $\Sigma(de,e,n) = (R(de,e,n), f_{de,e,n})$ est un système de racines tel que $\mathrm{W}(\Sigma(de,e,n)) = G(de,e,n)$.

(iii) Soit $R = \mu_6 \{\varepsilon_1, 1/3(2\omega+1)(w^j\varepsilon_1 + \varepsilon_2 + \varepsilon_3, j = 0,1,2\}$ et $f : R \to \mathbf{N}$ la fonction constante 3. Alors $\Sigma = (R,f)$ est un système de racines et $\mathrm{W}(\Sigma) = \mathrm{W}(L_2)$ (cf. l'Exemple 4.9).

Définition 4.32: Soit $\Sigma = (R,f)$ un présystème de racines. Une extension propre de Σ est un système de racines $\Omega = (S,g)$ tel que $S \supsetneq R$, $g|_R = f$ et

(i) $g(S) = f(R)$

(ii)

$$\left\{ |(a\,|b)|\,|a|^{-1}\,|b|^{-1}\,; a,b \in S \bigcap g^{-1}(2) \right\} \subset \{|\cos(\pi k/m)|; k \in \mathbf{Z}, 0 < m \leqslant d(\mathrm{W}(\Sigma))\}$$

Remarque 4.33: La condition (i) de la Définition 4.32 signifie que $\mathrm{Im}\, o_{\mathrm{W}(\Sigma)} = \mathrm{Im}\, o_{\mathrm{W}(\Omega)}$ et la condition (ii) signifie que $d(\mathrm{W}(\Sigma)) = d(\mathrm{W}(\Omega))$ (cf. le Lemme 4.28(i)).

Lemme 4.34: *Si G est un groupe de réflexions, et Σ un système de racines tel que $\mathrm{W}(\Sigma) \subsetneq G$ avec $\mathrm{Im}\, o_{\mathrm{W}(\Sigma)} = \mathrm{Im}\, o_G$ et $d(\mathrm{W}(\Sigma)) = d(G)$, alors il existe un système de racines Σ' tel que $G = \mathrm{W}(\Sigma')$ et Σ' est (isomorphe à) une extension propre de Σ.*

DÉMONSTRATION: On étend Σ en un système de racines Σ' qui représente G (cf. l'Exemple 4.27 et le Lemme 4.28(i)). La Remarque 4.33 montre que Σ' est une extension propre de Σ. ■

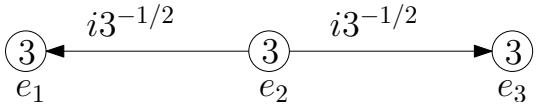
Exemple 4.35: Il n'y a pas d'extension propre dans $\mathbf{C}^3$ de $\Sigma(3,3,3)$. (En effet, si $x \in \mathbf{C}^3 \setminus \Sigma(3,3,3)$ appartient à une extension propre, alors quitte à changer la longueur de x on peut supposer que $|x| = \sqrt{2}$ et la condition (ii) de la Définition 4.32 implique que $\left|\left(x\,|\varepsilon_i - e^{2i\pi/3}\varepsilon_j\right)\right| = 0,1$ pour tout $1 \leqslant i \neq j \leqslant 3$, et un calcul rapide montre que c'est impossible.)

4.4 Les graphes de racines primitifs complexes de rang $\geqslant 3$

On a vu dans le Chapitre 3 qu'il y avait 15 groupes de réflexions complexes primitifs rang $\geqslant 3$, et le Théorème 4.18 montre qu'il y en a 9 qui sont complexes. On va les exhiber en donnant la description des graphes de racines qui les représentent (ils sont tous représentables par un graphe de racines, sauf un). On conclura au Chapitre 5 en montrant que ce sont bien les seuls.

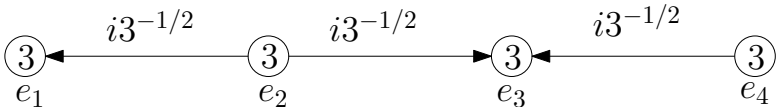
Définition 4.36:

(i) On appelle L_3 le graphe de vecteurs



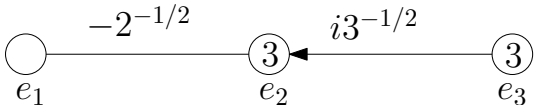
où $e_1 = \varepsilon_3$, $e_2 = i3^{-1/2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)$ et $e_3 = \varepsilon_2$.

(ii) On appelle L_4 le graphe de vecteurs



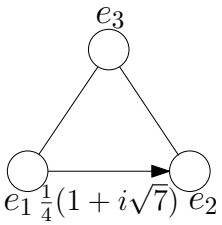
où $e_1 = \varepsilon_3$, $e_2 = i3^{-1/2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)$, $e_3 = \varepsilon_2$ et $e_4 = i3^{-1/2}(-\varepsilon_1 + \varepsilon_2 + \varepsilon_4)$.

(iii) On appelle M_3 le graphe de vecteurs



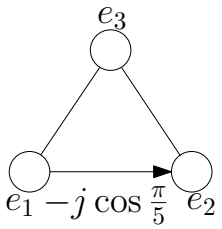
où $e_1 = 2^{-1/2}(\varepsilon_2 - \varepsilon_3)$, $e_2 = \varepsilon_3$ et $e_3 = i3^{-1/2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)$.

(iv) On appelle $J_3(4)$ le graphe de vecteurs



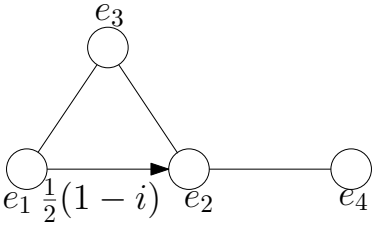
où $1/4(1 + i\sqrt{7}) = 2\alpha$, avec α une racine de $X^2 - X + 2$, $e_1 = \varepsilon_2$, $e_2 = 1/2\overline{\alpha}(\varepsilon_2 + \varepsilon_3)$ et $e_3 = -1/2(\varepsilon_1 + \varepsilon_2 - \alpha\varepsilon_3)$.

(v) On appelle $J_3(5)$ le graphe de vecteurs



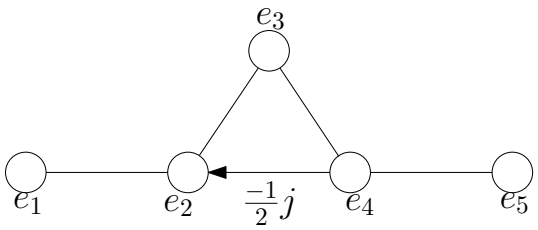
où $e_1 = \varepsilon_1$, $e_2 = -(j^2\cos(\pi/5)\varepsilon_1 - \cos(3\pi/5)\varepsilon_2 + 1/2j\varepsilon_3)$ et $e_3 = -(1/2\varepsilon_1 + \cos(3\pi/5)\varepsilon_2 + \cos(\pi/5)\varepsilon_3)$.

(vi) On appelle N_4 le graphe de vecteurs



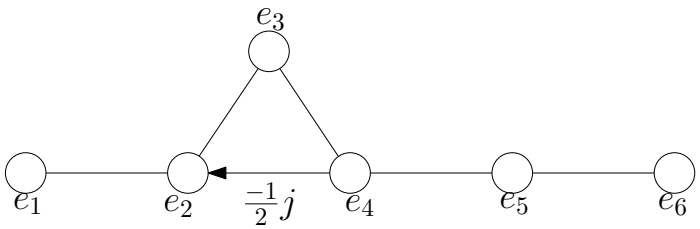
où $e_1 = 1/2(1+i)(\varepsilon_2+\varepsilon_4)$, $e_2 = 1/2(1+i)(\varepsilon_3-\varepsilon_2)$, $e_3 = 1/2(-\varepsilon_1+i\varepsilon_2-\varepsilon_3+i\varepsilon_4)$ et $e_4 = \varepsilon_1$.

(vii) On appelle K_5 le graphe de vecteurs



où $e_1 = j2^{-1/2}(\varepsilon_5+\varepsilon_6)$, $e_2 = -j2^{-3/2}(-\varepsilon_1+(1+2j)\varepsilon_2+\varepsilon_3+\varepsilon_4+\varepsilon_5+\varepsilon_6)$, $e_3 = 2^{-1/2}(\varepsilon_1-\varepsilon_2)$, $e_4 = 2^{-1/2}(\varepsilon_2-\varepsilon_3)$ et $e_5 = 2^{-1/2}(\varepsilon_3-\varepsilon_4)$.

(viii) On appelle K_6 le graphe de vecteurs



où $e_1 = j2^{-1/2}(\varepsilon_5+\varepsilon_6)$, $e_2 = -j2^{-3/2}(-\varepsilon_1+(1+2j)\varepsilon_2+\varepsilon_3+\varepsilon_4+\varepsilon_5+\varepsilon_6)$, $e_3 = 2^{-1/2}(\varepsilon_1-\varepsilon_2)$, $e_4 = 2^{-1/2}(\varepsilon_2-\varepsilon_3)$, $e_5 = 2^{-1/2}(\varepsilon_3-\varepsilon_4)$ et $e_6 = -2^{-3/2}j^2(\varepsilon_1+\varepsilon_2+\varepsilon_3+(1+2j)\varepsilon_4+\varepsilon_5-\varepsilon_6$ ♢

Théorème 4.37: *Soit $\Gamma = (B, w)$ l'un des graphes de vecteurs de la Définition 4.36, disons de dimension n. Alors Γ est un graphe de racines. De plus, soit $\Sigma = (R, f)$ le système de racines associé à Γ (cf. l'Exemple 4.27) et posons $G = \mathrm{W}(\Gamma) = \mathrm{W}(\Sigma)$. Alors :*

(i) G est un groupe de réflexions complexe primitif de $\mathbf{C}^n$, $d(G) = d(\Gamma)$ et si $v \in R \bigcap B$, $f(v) = w(v)$ (autrement dit f est déterminé par w, f est l'unique extension de w compatible avec l'action de G).

(ii) Σ n'admet pas d'extension propre dans $\mathbf{C}^n$, sauf si $\Gamma = N_4$. Dans ce dernier cas, Σ n'admet qu'une seule extension propre : $\Delta = (S, g)$ où $S = G.B \bigcup G.(\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4)$ et g est la fonction constante 2. On notera $\mathrm{EW}(N_4)$ le groupe engendré par Δ.

(iii) G est conjugué à son conjugué complexe $\overline{G}$.

On trouvera dans le Tableau 4.1 un récapitulatif des groupes primitifs de rang $\geqslant 3$, avec leurs numéros de Shephard et Todd, leurs degrés caractéristiques, leurs ordres, et l'ordre de leurs centres.

Démonstration (idée): On fait une preuve au cas par cas, voir [Coh76], Théorème 4.15 page 409 pour plus de détails. On vérifie que Γ est un graphe de racines en vérifiant que R est fini, donc $G = \mathrm{W}(\Sigma)$ l'est aussi (on n'a pas besoin de connaître f ici pour savoir que G est fini). On vérifie ensuite que si on note f' l'unique extension

de w compatible avec l'action de G (c'est à dire avec l'action des réflections données par Γ), (R, f') vérifie la condition (ii) de la Définition 4.23, donc $\Sigma' = (R, f')$ est un système de racines. Comme $G = \mathrm{W}(\Gamma)$, $G = \mathrm{W}(\Sigma')$ et le Lemme 4.28 montre que si $v \in R$, $f'(v) = o_G(v)$ d'où $f = f'$. G est complexe car pour chacun des cas, soit Γ contient une réflexion d'ordre $\geqslant 2$, soit Γ contient un cycle complexe. Pour montrer que G est primitif, il suffit d'exhiber un sous-groupe de réflexions de G primitif de même dimension. Par exemple pour $\Gamma = K_5$, on vérifie que Σ est une extension propre d'un système de racines associé à $\mathrm{W}(A_5)$, qui est primitif en dimension 5. De plus, $d(G) = d(\Gamma)$, en effet on peut calculer $d(G)$ grâce à Σ d'après la Remarque 4.33.

Pour montrer que Σ n'admet pas d'extension propre (ou une seule dans le cas $\Gamma = N_4$), on procède comme dans l'Exemple 4.35. Par exemple, pour $\Gamma = N_4$, supposons que $x \in \mathbf{C}^4 \setminus \mathbf{U}.R$ est un élément d'une extension propre de Σ. Quitte à changer la longueur de x, on peut supposer que $|x| = 2$. Comme $d(\mathrm{W}(N_4)) = 4$, le produit scalaire de x avec un élément v de R est dans $\left\{0, 2\,|v| \times 1/2, 2\,|v| \times \sqrt{(2)}/2\right\}$. Comme $\varepsilon_i \pm \varepsilon_j \in R$ (si $1 \leqslant i, j \leqslant 4$), et on vérifie facilement en faisant les calculs que $x \in \mathbf{C}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4)$ (quitte à remplacer x par un conjugué de x sous l'action de $\mathrm{W}(N_4)$). Donc Δ est bien l'unique extension propre de Σ.

Enfin, on vérifie aussi au cas par cas que G est conjugué à $\overline{G}$, ceci ne nous servira pas pour la suite, celà montre juste que la conjugaison complexe ne donne pas de nouveaux groupes primitifs (en rang $\geqslant 3$). ■

Numéro	Groupe	Degrés	Ordre	Ordre du centre	Nombre de réflexions d'ordres	
					2	3
24	$\mathrm{W}(J_3(4))$	$4, 6, 14$	336	2	21	-
25	$\mathrm{W}(L_3)$	$6, 9, 12$	648	3	-	24
26	$\mathrm{W}(M_3)$	$6, 12, 18$	1296	6	9	24
27	$\mathrm{W}(J_3(5))$	$6, 12, 30$	2160	6	45	-
29	$\mathrm{W}(N_4)$	$4, 8, 12, 20$	7680	4	40	-
31	$\mathrm{EW}(N_4)$	$8, 12, 20, 24$	46080	4	60	-
32	$\mathrm{W}(L_4)$	$12, 18, 24, 30$	155520	6	-	80
33	$\mathrm{W}(K_5)$	$4, 6, 10, 12, 18$	51840	2	45	-
34	$\mathrm{W}(K_6)$	$4, 12, 18, 24, 30, 42$	26127360	2	126	-

TAB. 4.1 – Les groupes primitifs de rang $\geqslant 3$

Chapitre 5

Classification des groupes de réflexions primitifs

5.1 Introduction

Notre but dans ce Chapitre est de terminer la liste des groupes de réflexions irréductibles. On a déjà classifié les groupes de réflexions imprimitifs dans le Chapitre 2, et on a rappelé quels sont les groupes de réflexions réels primitifs dans le Théorème 4.18. Il ne reste plus qu'à montrer que les 9 groupes de réflexions complexes que l'on a exhibés dans la section 4.4 sont bien les seuls.

L'idée est de partir d'un groupe de réflexions complexe primitif G de dimension n, et de montrer que son système de racines associé est une extension propre d'un des systèmes de racines du Théorème 4.37. Le Théorème 4.37(ii) montrera alors que G est bien l'un des groupes de la liste. Une méthode possible, si G est engendré par des réflexions d'ordre 2, c'est d'utiliser le Théorème 4.20 pour obtenir un graphe de racines Γ qui engendre un groupe $\mathrm{W}(\Gamma) \subset G$ et tel que $d(\Gamma) = d(G)$ (une condition dont on a besoin pour montrer que le système de racines associé à G est une extension propre du système de racines associé à une extension de Γ). On pourra étendre Γ en un graphe de racines de dimension n grâce au Lemme 4.19(i), mais en fait on préférera utiliser le Corollaire 4.21 pour avoir un sous-groupe primitif, on verra pourquoi plus tard. Le problème du Corollaire 4.21 est qu'il donne un graphe de racines Γ de dimension $8 - d(G)$, donc plus $d(G)$ est grand, plus Γ sera petit, et plus il y aura de possibilités pour le compléter en un groupe de dimension n. Enfin, si G contient une réflexion d'ordre $\geqslant 3$, la méthode précédente ne marche pas (on peut cependant utiliser la Proposition 2.12 pour obtenir un sous-groupe primitif).

Ainsi il nous faut une méthode pour montrer que G n'a pas de réflexions d'ordres trop important, et que $d(G)$ est assez petit. On obtiendra ce résultat grâce à un théorème de Blichfeldt, qui s'applique à n'importe quel groupe primitif. On voit que l'on est obligé d'utiliser un résultat qui sort du cadre des groupes de réflexions, c'est pourquoi l'on peut dire que la preuve de la classification des groupes de réflexions réalisée dans ce mémoire n'est pas totalement satisfaisante : les constructions combinatoires (graphes de racines et systèmes de racines) introduites dans le Chapitre 4 ne sont pas assez puissantes pour parvenir à elles seules à la classification (à la différence des graphes de Coxeter pour la classification des groupes de réflexions

réels).

Une fois énoncé ce théorème, il ne nous restera plus qu'à étudier au cas par cas chacune des possibilités laissée. Comme ce n'est pas vraiment la partie la plus intéressante de la preuve, on donnera juste quelques exemples pour montrer comment se servir des outils que l'on a construits jusqu'ici, et l'on renvoie à [Coh76] pour la preuve en détail des cas restant.

5.2 Le théorème de Blichfeldt

Théorème 5.1 (Blichfeldt): *Soit V un espace vectoriel complexe et G un groupe fini et primitif de morphismes unitaires de V. Soit $g \in G$, et notons $\{\zeta_1, \dots, \zeta_m\}$ l'ensemble des valeurs propres distinctes de g. On suppose que $\left|\arg \zeta_j \zeta_1^{-1}\right| \leqslant \pi/3$ pour tout $1 \leqslant j \leqslant m$. Alors $g \in \mathcal{Z}(G)$.*

DÉMONSTRATION: Voir l'Appendice A. ■

Ce théorème a les conséquences suivantes pour un groupe de réflexions primitif, ce qui va nous permettre d'élaguer considérablement les groupes que l'on a à considérer pour terminer la classification :

Corollaire 5.2: *Soit V un espace vectoriel complexe de dimension $n \geqslant 3$, et $G \subset \mathrm{U}(V)$ un groupe de réflexions primitif fini. Alors :*

(i) G ne contient pas de réflexions d'ordres $\geqslant 4$. Si G contient une réflexion d'ordre 3, alors G contient un sous-groupe conjugué à $\mathrm{W}(L_2)$.

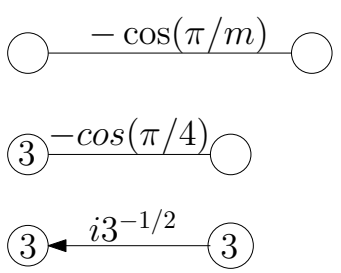
(ii) Si H est un sous-groupe de réflexions de G irréductible de dimension r, et que $1 < r < n$; alors $\mathcal{Z}(H) < 6$. Si de plus $r = n - 1$, alors $\mathcal{Z}(H) < 4$. Dans ce dernier cas, si $\mathcal{Z}(H) = 3$, alors $\langle G, j\,\mathrm{Id}_n \rangle$ contient un sous-groupe de réflexions conjugué à $\mathrm{W}(L_2)$.

(iii) Si H est un sous-groupe de réflexions de G primitif de dimension r, avec $r < n$, alors $|\mathcal{Z}(H)| < 4$.

(iv) Si H est un sous-groupe de réflexions de G primitif de dimension 2, alors H est conjugué à $\mathrm{W}(L_2)$ (i.e. à $(\mu_6\,|\mu_2\,;\mathbf{T}\,|\mathbf{D}_2)$)

(v) Si $\mathrm{G}(de, e, r)$ est un sous-groupe de réflexions de G avec $r \geqslant 2$, alors $de \leqslant 5$ et $d \leqslant 3$. En particulier, $d(G) \leqslant 5$.

(vi) Tout graphe de racines Γ irréductible de dimension 2 et tel que $\mathrm{W}(\Gamma) \subset G$ est équivalent à $I_2(m)$ $(3 \leqslant m \leqslant 5)$, $B_2(3)$ ou L_2 :



$I_2(m)$, $(3 \leqslant m \leqslant 5)$
$\mathrm{W}(I_2(m)) = \mathrm{G}(m, m, 2) = \mathbf{D}_m$

$B_2(3)$
$\mathrm{W}(B_2(3)) = \mathrm{G}(3, 1, 2)$

L_2
$\mathrm{W}(L_2) = (\mu_6|\mu_2; \mathbf{T}|\mathbf{D}_2)$

DÉMONSTRATION: Rappelons que si H est un sous-groupe irréductible de $\mathrm{GL}(V)$ et que $h \in \mathcal{Z}(H)$, alors $v \in V \mapsto h.v$ est un H-morphisme, donc h est scalaire (car $\mathbf{C}$ est algébriquement clos).

Si $g \in G$ a pour valeurs propres distinctes $\{1, \zeta\}$, ζ ne peut pas être une racine de l'unité d'ordre $\geqslant 6$ d'après le Théorème 5.1, sinon g serait dans le centre de G, donc scalaire (on note que la preuve marche ici aussi pour $n = 2$, ce qui explique l'absence de réflexions d'ordres $\geqslant 6$ dans le Tableau 3.1). Ainsi les réflexions dans G sont d'ordres < 6, et si H est comme dans (ii), et $h \in \mathcal{Z}(H)$, alors $h|_{(V^H)^\perp}$ est scalaire (car H est irréductible), et h a pour uniques valeur propres $\{1, \zeta\}$ (car $r < n$ donc $V^H \neq \{0\}$), avec ζ d'ordre < 6. D'où comme $\mathcal{Z}(H)$ est cyclique (c'est $\mathcal{Z}(\mathrm{GL}((V^H)^\perp) \bigcap H)$), $|\mathcal{Z}(H)| < 6$[1], ce qui prouve la première partie de (ii). Le Tableau 3.1 montre alors que si H est un sous-groupe de réflexions de G primitif de dimension 2, alors H est conjugué à $(\mu_6 \,|\mu_2\,; \mathbf{T}\,|\mathbf{D}_2)$, $(\mu_{12}\,|\mu_4\,; \mathbf{T}\,|\mathbf{D}_2)$, $(\mu_8\,|\mu_4\,; \mathbf{O}\,|\mathbf{T}_2)$, $(\mu_4\,|\mu_2\,; \mathbf{O}\,|\mathbf{T}_2)$, $\mu_4\mathbf{O}$ ou $\mu_4\mathbf{I}$.

Mais puisque $(\mu_8\,|\mu_4\,; \mathbf{O}\,|\mathbf{T}_2)$, $(\mu_4\,|\mu_2\,; \mathbf{O}\,|\mathbf{T}_2)$ et $\mu_4\mathbf{O}$ contiennent l'élément

$$2^{-1/2}\exp(\frac{\pi i}{4})\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix} \in \mathbf{T}$$

(voir la Remarque 3.1) et $\mu_4\mathbf{I}$ contient l'élément

$$\frac{-1}{\sqrt{5}}\begin{pmatrix}\eta^2-\eta^4 & \eta^4-1\\ 1-\eta & \eta^3-\eta\end{pmatrix} \in \mathbf{I}$$

chacun de ces quatre groupes contient un élément qui a $\{-j, -j^2\}$ comme valeurs propres. Le Théorème 5.1 montre à nouveau qu'aucun de ces quatre groupes n'est inclus dans G (car $n \geqslant 3$, donc un élément d'un de ces groupes ne peut être scalaire).

Supposons maintenant que G contient une réflexion s d'ordre $\geqslant 3$. Soit B l'orbite par G d'une racine de s. Si $(x\,|y) = 0$ pour tout couple $(x, y) \in B^2$ de vecteurs linéairement indépendants, alors B donne lieu à un système d'imprimitivité de G (en effet, $\{\mathbf{C}b, b \in B\}$ engendre V car G est irréductible (puisque primitif) et est formé de sous-espace vectoriel libres car les vecteurs sont deux à deux orthogonaux). C'est absurde, et donc il existe $x, y \in B$ avec $(x\,|y) \neq 0$ et $\mathbf{C}x \neq \mathbf{C}y$. Soit H le sous-groupe de G engendré par les réflexions ayant x ou y pour racines. H est irréductible de dimension 2 (si $W = \langle x, y\rangle$, H stabilise $W^\perp$ et x, y sont des racines non orthogonales de H dans W, donc H est irréductible dans W par la Proposition 1.22). De plus il est primitif, car s'il avait pour système d'imprimitivité W_1, W_2, on aurait par exemple $x \in W_1$ et $y \in W_2$ puisque x et y sont racines d'une réflexion de H d'ordre > 2 (cf. la Proposition 2.4(ii)) mais comme $(x\,|y) \neq 0$, on contredirait la Proposition 2.4(iv). H est primitif de dimension 2, il est donc conjugué à $(\mu_6\,|\mu_2\,; \mathbf{T}\,|\mathbf{D}_2)$ ou à $(\mu_{12}\,|\mu_4\,; \mathbf{T}\,|\mathbf{D}_2)$ par ce qui précède. Mais comme ces deux groupes ne contiennent pas des réflexions d'ordres $\geqslant 4$, G n'en contient pas non plus.

Si H est un sous-groupe de réflexions de G irréductible de dimension $n-1$, et

[1] ici on ne s'est pas servi que H est un sous-groupe de réflexions de G, la même preuve marche pour n'importe quel sous-groupe irréductible de G

$\mathcal{Z}(H) = m$, il existe $h \in \mathcal{Z}(H)$ tel que (quitte à changer de base),

$$h = \begin{pmatrix} e^{-2i\pi/m} & & & \\ & \ddots & & \\ & & e^{-2i\pi/m} & \\ & & & 1 \end{pmatrix}$$

et $\langle G, e^{2i\pi/m}\,\mathrm{Id}_n\rangle$ est un groupe primitif qui contient des réflexions d'ordre m. D'où $m < 4$. Si H est comme dans (iii), on peut supposer que $r > 1$ (on a déjà vu qu'une réflexion est d'ordre < 4). Si H est conjugué à $\mathrm{W}(A_r)$, $\mathcal{Z}(H) = 1 < 4$. Si ce n'est pas le cas, on choisit un sous-groupe de réflexions H' de G qui contient H et est irréductible de dimension $r + 1$: un tel groupe existe car G étant irréductible il existe une réflexion s de G qui ne stabilise pas V^H, alors $\langle H, s\rangle$ convient par le Corollaire 1.24. La Lemme 2.10 montre alors que H' est primitif de dimension $r+1$, on peut appliquer ce que l'on vient de démontrer en remplaçant G par H' pour obtenir $\mathcal{Z}(H) < 4$. On a donc montré (iii).

Comme $\mathcal{Z}((\mu_{12}\,|\mu_4\,;\mathbf{T}\,|\mathbf{D}_2)) = 4$, (iii) montre que ni G, ni $\langle G, j\,\mathrm{Id}_n\rangle$ ne contiennent ce groupe, ce qui fini la preuve de (i) et de (iv). Si H est comme dans (ii) et $r = n - 1$, $\mathcal{Z}(H) = 3$ alors $\langle G, j\,\mathrm{Id}_n\rangle$ contient une réflexion d'ordre 3, donc contient $\mathrm{W}(L_2)$ par (i), ce qui finit la preuve de (ii).

$\mathrm{G}(de, e, n) = \mathrm{G}(d, 1, n).\,\mathrm{G}(de, de, n)$ contient des réflexions d'ordres d. Donc s'il est inclus dans G, $d \leqslant 3$, et dans ce cas G contient (quitte à changer de base) l'élément :

$$\begin{pmatrix} e^{2i\pi/m} & & \\ & e^{-2i\pi/m} & \\ & & \mathrm{Id}_{n-2} \end{pmatrix} \in \mathrm{G}(m, m, n) \quad \text{où l'on a posé } m = de$$

Si $m \geqslant 6$, le Théorème 5.1 (avec $\zeta_1 = 1$) montre que cet élément est dans le centre de G, donc est scalaire, c'est absurde, d'où $m < 6$. En particulier, si $d(G) = m$, G contient $\mathrm{W}(I_2(m))$ par définition, or $\mathrm{W}(I_2(m)) = \mathrm{G}(m, m, 2)$, donc $m \leqslant 5$, ce qui fini de prouver (v).

Si Γ est un graphe de racines irréductible de dimension 2, alors si $\mathrm{W}(\Gamma)$ est primitif, Γ est équivalent à $\mathrm{W}(L_2)$ par (iii). Sinon $\mathrm{W}(\Gamma) = \mathrm{G}(de, e, 2)$, avec $de \leqslant 5$, $d \leqslant 3$. Or $\mathrm{G}(2, 2, 2)$ n'est pas irréductible, $\mathrm{G}(4, 2, 2)$ n'est pas généré par 2 réflexions, et $\mathrm{G}(2, 1, 2)$ non plus (car il est conjugué à $\mathrm{G}(4, 2, 2)$). Il reste donc $\mathrm{G}(3, 3, 2)$, $\mathrm{G}(4, 4, 2)$, $\mathrm{G}(5, 5, 2)$ qui sont représentables par $I_2(m)$ et $\mathrm{G}(3, 1, 2)$ qui est représentable par $B_2(3)$, ce qui conclu la preuve de (vi) et donc le corollaire. ■

Remarque 5.3: Le Corollaire 5.2 marche également pour n'importe quel groupe $G \subset \mathrm{U}(V)$ d'automorphismes unitaires fini. En effet, on ne se sert nulle part du fait que G est un groupe de réflexions dans la preuve du corollaire, sauf pour prouver (iii). Mais si on considère K le sous-groupe de G engendré par les réflexions de G, il est normal (car le conjugué d'une réflexion est une réflexion), et irréductible de dimension n (on peut aussi le supposer non trivial car sinon $H \subset K$ serait également trivial, et on aurait immédiatement (iii)). Il suffit alors de remplacer K par G dans la preuve de (iii) pour obtenir un groupe de réflexions $H' \supset H$ de dimension $r + 1$ et conclure

de la même manière. Le seul point délicat est de voir que K est bien irréductible dans V, mais G étant primitif, le Théorème de Clifford (Théorème A.1) montre qu'en tant que $\mathbf{C}[K]$-module, V n'a qu'une seule composante isotypique. Il existe donc un sous-module irréductible W de V tel que $V \simeq W \oplus W \cdots \oplus W$. Mais si $s \in K$ est une réflexion, et que la multiplicité de W dans V est ≥ 2, il existe un W tel que s agisse trivialement dessus. Comme s agit de la même manière sur tous les W, s agit trivialement sur V, ce qui est absurde. Donc $V = W$ est bien un $\mathbf{C}[K]$-module irréductible.

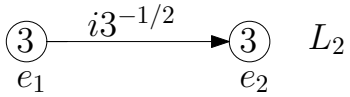
On ne se servira pas de cet énoncé plus général, ce qui explique pourquoi on a énoncé le Corollaire 5.2 directement pour un groupe de réflexions.

À partir de maintenant, si on a un graphe de racines $\Gamma = (B, w)$, on notera r_i la réflexion $s_{e_i, w(e_i)}$.

5.3 Cas des groupes contenant une réflexion d'ordre 3

5.3.1 Cas des groupes ne contenant que des réflexions d'ordres 3

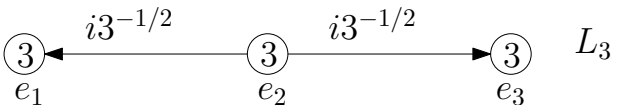
Soit G un groupe de réflexions primitif complexe de dimension 3 engendré par des réflexions d'ordres 3, toutes les réflexions de G sont d'ordres 3 par le Lemme 4.28. Si v et w sont des racines de deux réflexions distinctes de G, alors $|(v\,|w)| \in \{0, 3^{-1/2}\}$. En effet par le Corollaire 5.2(vi), v et w engendrent un graphe équivalent à L_2 et l'Exemple 4.31(ii) et le Lemme 4.28(iii) permettent de conclure. Et G contient $\mathrm{W}(L_2)$ (par le Corollaire 5.2(i)) :



Comme G est irréductible de dimension 3, il existe une racine unitaire e_3 de G non contenue dans $(\mathbf{C}e_1 + \mathbf{C}e_2) \bigcup (\mathbf{C}e_1 + \mathbf{C}e_2)^{\perp}$. Si $(e_3\,|e_2) = 0$, alors $(e_3\,|e_1) \neq 0$ et quitte à remplacer e_3 par $r_1 e_2$, on peut supposer que $(e_3\,|e_2) \neq 0$. Soit Γ le graphe de racines engendré par e_1, e_2 et e_3, i.e. $\Gamma = (B, w)$ avec $B = \{e_1, e_2, e_3\}$ et $w(B) = \{3\}$.

Proposition 5.4:

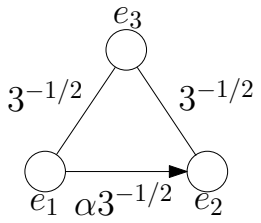
(i) Γ *est équivalent à* L_3 *:*



(ii) G *est conjugué à* $\mathrm{W}(L_3)$ *:*

Démonstration:

(i) Si Γ est sans cycles, Γ est clairement congruent à L_3 par la discussion qui précède la proposition. Si Γ est un triangle, alors Γ est de la forme (à congruence près) :



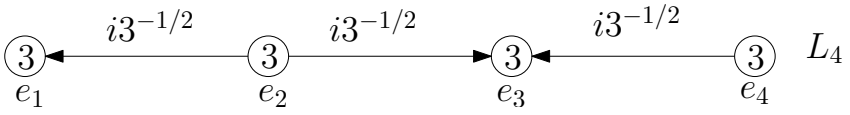
où $\alpha \in \mathbf{U}$.
Si $\left(r_3^l e_1 \,|e_2\right) = 0$ pour un $l = 1, 2$, alors Γ est équivalent au graphe de racines engendré par $r_3^l e_1, e_2, e_3$, mais ce dernier n'a pas de cycles (cf. le Lemme 4.13 qui marche évidemment si au lieu de remplacer b par $r_a b$, on remplace b par $r_a^k b$ du moment que k est premier avec $w(a)$ et l'Exemple 4.14), mais ce dernier graphe est sans cycles donc on revient au cas précédent. Sinon $\left(r_3^l e_1 \,|e_2\right) = 3^{-1/2}$ pour $l = 1, 2$ d'après la discussion qui précède la proposition, soit encore $\left|\alpha - 3^{-1/2}(1 - j^l)\right| = 1$ pour $l = 1, 2$ ce qui est absurde.

(ii) Comme G contient le $\mathrm{W}(L_3)$, le système de racines associé à G contient le système de racines associé à L_3. Or ce dernier n'ayant pas d'extension propre (Théorème 4.37(ii)), et puisque $d(G) = d(L_3) = -\infty$, ces deux systèmes de racines sont égaux et $G = \mathrm{W}(L_3)$. ■

Soit G un groupe de réflexions primitif complexe de dimension 4 engendré par des réflexions d'ordres 3.

Proposition 5.5:

(i) Il existe un graphe de racines Γ équivalent à L_4 tel que $\mathrm{W}(\Gamma) \subset G$:

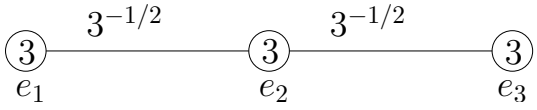


(ii) G est conjugué à $\mathrm{W}(L_4)$:

(iii) Il n'existe pas de groupe de réflexions primitif complexe de dimension $\geqslant 5$ engendré par des réflexions d'ordres 3.

Démonstration:

(i) Si v et w sont des racines de deux réflexions distinctes de G, alors $|(v\,|w)| \in \left\{0, 3^{-1/2}\right\}$ par le même raisonnement que précédemment. De plus G contient $\mathrm{W}(L_2)$ que l'on peut étendre en un graphe de racines irréductible de dimension 3 qui engendre un sous-groupe G' de G. Comme $\mathrm{W}(L_2)$ est primitif, le Lemme 2.10 nous dit que G' est primitif, donc on peut appliquer la Proposition 5.4. Ainsi G contient $\mathrm{W}(L_3)$, or L_3 est congru au graphe Γ_0 suivant :



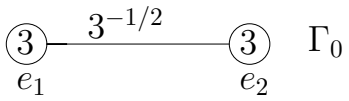
Comme G est primitif, il existe une racine e_4 de G tel que le graphe engendré par e_1, e_2, e_3, e_4 soit irréductible. Si seul $(e_1 \,|e_4\,) \neq 0$, ou seul $(e_3 \,|e_4\,) \neq 0$, alors on tombe bien sur un graphe équivalent (et même congru) à L_4. Si $(e_2 \,|e_4\,) = 0$ mais $(e_1 \,|e_4\,) \neq 0$ et $(e_3 \,|e_4\,) \neq 0$, on se trouve dans la même situation que dans la preuve de la Proposition 5.4(i), et l'on sait qu'il existe $l \in \{1, 2\}$ tel que $\left(e_1 \left| r_3^l e_4 \right.\right) = 0$ ce qui nous ramène au cas précédent. Si $(e_2 \,|e_4\,) \neq 0$, alors encore une fois on peut supposer que $(e_1 \,|e_4\,) = 0$ quitte à remplacer e_4 par $r_2^l e_4$. De plus dans ce cas $(e_3 \,|e_4\,) \neq 0$ sinon on aurait $\det((e_i \,|e_j\,)) = 0$, ce qui contredirait le Lemme 4.6. Encore une fois on obtient un graphe congru à L_4 en remplaçant e_4 par $r_3^l e_4$.

(ii) On applique (i) et le Théorème 4.37(ii).

(iii) Si G est un groupe primitif complexe de dimension $\geqslant 5$ engendré par des réflexions d'ordres 3, le même raisonnement qu'en (i) montre qu'il existe un sous-groupe de réflexions G' de G primitif et de dimension 4. (ii) nous donne alors que G est conjugué à $\mathrm{W}(L_4)$, mais $|\mathcal{Z}(\mathrm{W}(L_4))| = 6$, ce qui contredit le Corollaire 5.2(ii). ■

5.3.2 Cas des groupes contenant des réflexions d'ordres 3 et 2

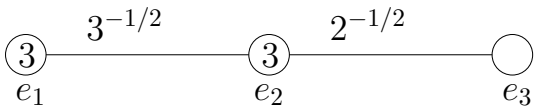
Soit G un groupe de réflexions complexe primitif de dimension 3 contenant des réflexions d'ordres 2 ainsi que d'ordres 3. Comme on l'a vu dans la section 5.3.1, par le Corollaire 5.2(i) G contient le sous-groupe $\mathrm{W}(\Gamma_0)$ où Γ_0 est le graphe (congru à L_2) suivant :



Le Corollaire 5.2(vi) montre que si v est une racine unitaire d'ordre 2 et w une racine unitaire d'ordre 3, ils engendrent un graphe de racines équivalent à $B_2(3)$ et la Proposition 2.4(v) donne alors $|(v \,|w\,)| \in \left\{0, 2^{-1/2}\right\}$. Il existe une racine unitaire e_3 d'ordre 2 non orthogonale à e_1 et e_2 (en effet, si $g \in G$, g envoie une racine d'ordre k de G sur une racine de même ordre, donc si toutes les racines d'ordres 2 de G étaient orthogonales à e_1 et e_2, elles engendreraient un sous-espace stable par G). Quitte à permuter e_1 et e_2, on peut supposer que $(e_2 \,|e_3\,) \neq 0$. Soit Γ le graphe engendré par e_1, e_2, e_3.

Proposition 5.6:

(i) Γ *est équivalent à* M_3*, où* M_3 *est congru au graphe suivant :*

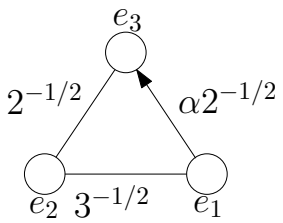


(ii) G *est conjugué à* $\mathrm{W}(M_3)$ *:*

(iii) Si H est un groupe de réflexions primitif de dimension $n > 3$, H ne contient pas un sous-groupe de réflexions conjugué à $\mathrm{W}(M_3)$. En particulier, H ne contient pas à la fois de réflexions d'ordres 2 et 3.

Démonstration:

(i) Si $(e_1 \,|e_3\,) = 0$, Γ est bien congru à M_3. Sinon Γ est congru au graphe suivant :



Et comme dans la preuve de la Proposition 5.4(i) on se ramène au cas précédent si $\left(r_2^l e_1 \,|e_3\right) \neq 0$ pour un $l \in \{1, 2\}$, ce qui est le cas car sinon on a $\left|\left(r_2^j e_1 \,|e_3\right)\right| = 2^{-1/2}$ pour $l = 1, 2$ ce qui est absurde.

(ii) On applique le Théorème 4.37(ii), puisque $d(G) = d(M_3) = -\infty$ (en effet G est de dimension 3 et contient déjà deux racines libres d'ordres 3, e_1 et e_2, donc ne peut contenir deux racines libres d'ordres 2).

(iii) Si G est un groupe primitif complexe de dimension $\geqslant 3$, il ne peut contenir $\mathrm{W}(M_3)$ car $|\mathcal{Z}(\mathrm{W}(M_3))| = 6$ (Corollaire 5.2(ii)).
Or si G contient à la fois des réflexions d'ordres 2 et 3, le même raisonnement qu'avant la proposition nous montre qu'il contient $\mathrm{W}(L_2)$ et qu'on peut étendre L_2 en un graphe Γ irréductible en ajoutant une réflexion d'ordre 2, tel que $G' = \mathrm{W}(\Gamma)$ soit un sous-groupe de G. Mais G' est primitif par le Lemme 2.10, de dimension 3, donc par (ii) G' est $\mathrm{W}(M_3)$, mais on vient de voir que ce n'est pas possible. ■

On note que le Corollaire 5.2(i), la Proposition 5.5(iii) et la Proposition 5.6(iii) montrent que l'on a classifié tous les groupes de réflexions primitifs de rang > 3 contenant une réflexion d'ordre > 2.

5.4 Cas des groupes ne contenant que des réflexions d'ordres 2

(On s'intéresse ici aux groupes de réflexions complexes primitifs, vu que l'on connaît déjà tous les groupes de réflexions réels primitifs.)

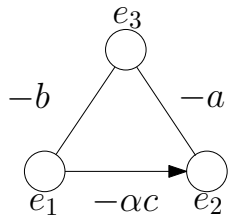
La méthode employée dans cette section est exactement la même que dans la section précédente. Soit G un groupe de réflexions complexe engendré par des réflexions d'ordres 2. On part d'un triangle complexe donné par le Théorème 4.20, et on l'étend en un graphe de racines primitif complexe en se servant du Corollaire 4.21, de la Proposition 2.12 ou du Lemme 4.19(i) conjugué au Lemme 2.10. On obtient ainsi un sous-groupe primitif complexe G' de G de dimension inférieure à celle de G, avec $d(G') = d(G)$. En supposant que l'on a déjà effectué la classification pour les groupes de dimension inférieure à celle de G, on obtient ainsi que G contient l'un

des graphes de racines Γ_0 donné dans la Section 4.4. On étend Γ_0 en un graphe de racines irréductible Γ de même dimension que celle de G (en se servant à nouveau Lemme 4.19(i)), et il ne nous reste plus qu'à montrer que Γ est équivalent à l'un des graphes de racines donné dans la Section 4.4 pour conclure que $G = \mathrm{W}(\Gamma)$ (ou $G = \mathrm{EW}(\Gamma)$ si $\Gamma = N_4$) grâce au Théorème 4.37(ii).

Le plus difficile est donc de montrer que Γ est bien l'un des graphes de racines de la Section 4.4. Pour cela on se sert évidemment du Lemme 4.13 pour aplatir le plus possible Γ (i.e. enlever le plus de cycles possibles). On fait ensuite du cas par cas en fonction des triangles complexes ou réels qui restent grâce au Lemme 5.7.

Comme annoncé dans l'introduction, ceci n'est pas la partie la plus intéressante de la preuve, et donc une fois énoncé le Lemme 5.7 on donnera juste un exemple pour montrer comment l'utiliser, et pour les cas restants, on renverra à [Coh76].

Lemme 5.7: *Soit Γ un triangle complexe formé d'éléments de valuations 2 et $G = \mathrm{W}(\Gamma)$. Notons $m = d(G) = d(\Gamma)$ (par le Corollaire 4.30). Quitte à prendre un graphe congruent, on peut supposer que Γ est de la forme :*



avec $a, b, c \in \mathbf{R}^+$, $\alpha \in \mathbf{U} \setminus \mathbf{R}$, $c = \cos(\pi/m)$. On note $p = |(r_1 e_2 \,|e_3)|$,$q = |(r_2 e_1 \,|e_3)|$ et $r = |(r_3 e_1 \,|e_2)|$. Alors on a

$$p, q, r, a, b, c \in \{|\cos(\pi k/l)\,, k \in \mathbf{Z}, 1 \leqslant l \leqslant m\} \tag{5.1}$$

$$\begin{aligned} p^2 &= a^2 + 4b^2c^2 + 4\,\mathrm{Re}(\alpha)abc \\ q^2 &= b^2 + 4a^2c^2 + 4\,\mathrm{Re}(\alpha)abc \\ r^2 &= c^2 + 4a^2b^2 + 4\,\mathrm{Re}(\alpha)abc \end{aligned} \tag{5.2}$$

$$\begin{aligned} p^2 - q^2 &= (a^2 - b^2)(1 - 4c^2) \\ p^2 - r^2 &= (a^2 - c^2)(1 - 4b^2) \\ q^2 - r^2 &= (b^2 - c^2)(1 - 4a^2) \end{aligned} \tag{5.3}$$

$$1 - a^2 - b^2 - c^2 - 2\,\mathrm{Re}(\alpha)abc > 0 \tag{5.4}$$

$$\begin{aligned} p^2 + a^2 &< 1 + (1 - 2b^2)(1 - 2c^2) \\ q^2 + b^2 &< 1 + (1 - 2a^2)(1 - 2c^2) \\ r^2 + c^2 &< 1 + (1 - 2a^2)(1 - 2b^2) \end{aligned} \tag{5.5}$$

$$pqr \neq 0 \tag{5.6}$$

Si Γ est un triangle réel, Γ est de la même forme que précédemment, mais cette fois $\alpha \in \{-1, 1\}$. Alors on a toujours (5.1), (5.2), (5.3), (5.4) *et* (5.5). ♢

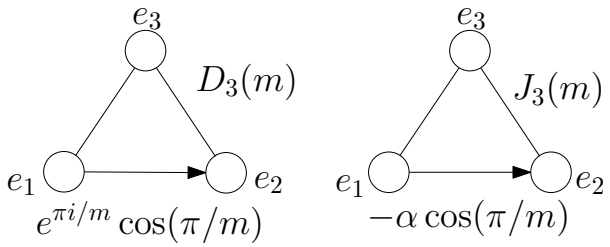
Démonstration:

- (5.1) vient de ce que p, q, r, a, b, c sont des produits scalaires de deux racines non linéairement indépendantes et d'ordres 2.
- $p^2 = |(e_2 \,|r_1 e_3)|^2 = |(e_2 \,|e_3 + 2be_1)|^2 = a^2 + 4b^2c^2 + 4\,\mathrm{Re}(\alpha)abc$ d'où (5.2).
- Si on soustrait les équations dans (5.2), on obtient (5.3).
- $\det((e_i \,|e_j)) > 0$ (Lemme 4.6) donne (5.4).
- (5.4) et (5.2) donnent (5.5).
- Comme α est unitaire non réel pur, $\mathrm{Re}(\alpha) > -1$, donc $p^2 > (a - 2bc)^2 > 0$ d'où (5.6). ■

Le Lemme 5.7 va nous permettre de déterminer à quoi ressemble le triangle (complexe ou réel) Γ lorsque $m \leqslant 5$.

Proposition 5.8:

(i) Si Γ est un triangle complexe comme dans le Lemme 5.7, et que $m = d(\Gamma) \leqslant 5$, alors Γ est conjugué à $D_3(m)$ ($m \geqslant 3$) ou à $J_3(m)$ ($m \geqslant 4$) :



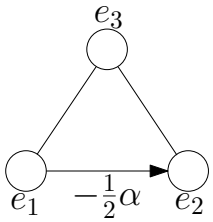
($\alpha = -2^{-3/2}(1 + i\sqrt{7})$ si $m = 4$ et $\alpha = j$ si $m = 5$).

(ii) Si Γ est un triangle réel comme dans le Lemme 5.7, alors

- *si $m \leqslant 4$: $p, q = 0$ ou $p, r = 0$ ou $q, r = 0$.*
- *si $m = 5$: $p = 0$ ou $q = 0$ et il existe $v \in \langle r_1, r_2\rangle.e_3$ tel que $(v \,|e_1) = 0$.*

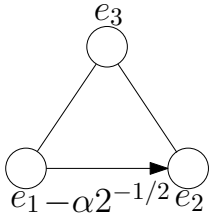
Démonstration:

(i) Si $m = 3$, le Lemme 5.7 nous donne immédiatement que $a = b = c = p = q = r = 1/2$ et $\mathrm{Re}(\alpha) = -1/2$, ainsi Γ est le graphe de racines



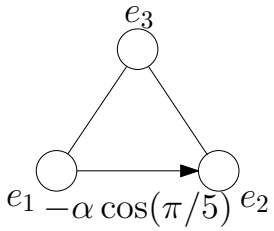
avec $\alpha \in \{j, j^2\}$ donc Γ est équivalent à $D_3(3)$.

Si $m = 4$, une étude au cas par cas en se servant du Lemme 5.7 montre que quitte à remplacer e_3 par un élément de $\langle r_1, r_2\rangle.e_3$ Γ est équivalent à



Si $p = 1/2$ alors $\mathrm{Re}(\alpha) = -2^{-1/2}$ et Γ est équivalent à $D_3(4)$, sinon $p = 2^{-1/2}$, $\mathrm{Re}(\alpha) = -2^{-3/2}$ et Γ est équivalent à $J_3(4)$.

Si $m = 5$, une étude au cas par cas montre à nouveau que Γ est équivalent à



Si $p = 1/2$ alors $\mathrm{Re}(\alpha) = -\cos(\pi/5)$ et Γ est équivalent à $D_3(5)$. Si $p = 2^{-1/2}$ alors $\mathrm{Re}(\alpha) = -1/2$ et Γ est équivalent à $J_3(5)$. Si $p \in \{\cos(\pi/5), \cos(2\pi/5)\}$, on obtient une contradiction.

(ii) La preuve se fait à nouveau au cas par cas en utilisant le Lemme 5.7. ■

5.4.1 Cas des groupes de dimensions 3

Proposition 5.9:

(i) Soit G un groupe de réflexions complexe primitif de dimension 3 engendré par des réflexions d'ordres 2, et notons $m = d(G)$. Alors G est conjugué à $\mathrm{W}(J_3(m))$.

(ii) Il n'existe pas de groupes de réflexions irréductibles de dimensions > 3 contenant un sous-groupe de réflexions conjugué à $\mathrm{W}(J_3(5))$.

Démonstration:

(i) Le Théorème 4.20 nous donne un triangle complexe Γ comme dans la Proposition 5.8, avec $\mathrm{W}(\Gamma) \subset G$. Ce triangle est conjugué à $D_3(m)$ ou $J_3(m)$. Mais si G contient $D_3(m)$, $\langle G, i\,\mathrm{Id}_3\rangle$ qui est primitif contient un conjugué de la réflexion

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & i \end{pmatrix}$$

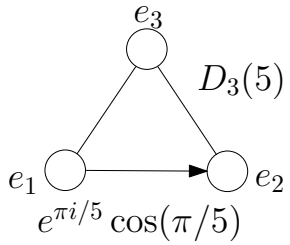
qui est d'ordre 4, ce qui contredit le Corollaire 5.2(i). Donc $G \supset \mathrm{W}(J_3(m))$ donc lui est égal par le Théorème 4.37(ii).

(ii) Si G est un tel groupe, il est primitif par le Lemme 2.10, or $\mathcal{Z}(J_3(5) = 6$ et le Corollaire 5.2(ii) permet de conclure. ■

Si G est un groupe de réflexions primitif, alors $d(G) \leqslant 5$ par le Corollaire 5.2(v).

Proposition 5.10: *Soit G un groupe de réflexions complexe primitif de dimension $n \geqslant 3$ engendré par des réflexions d'ordres 2 et tel que $d(G) = 5$. Alors $n = 3$ et G est conjugué à $\mathrm{W}(J_3(5))$.*

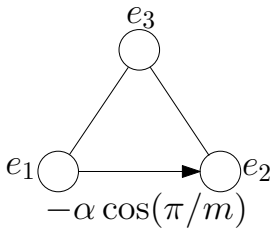
DÉMONSTRATION: Par la Proposition 5.9, il suffit de montrer que G contient un sous-groupe de réflexions complexe G_0 primitif de dimension 3 avec $d(G_0) = 5$. Le Théorème 4.20 nous donne un triangle complexe Γ qui génère un sous-groupe de G et tel que $d(\Gamma) = 5$. Si Γ est primitif, on a gagné, sinon Γ est équivalent à $D_3(5)$:



La Proposition 2.12 nous donne une racine unitaire $e_4 \in G$ telle que e_1, e_2, e_4 engendrent un graphe de racines Γ' primitif. Si Γ' est complexe, on a encore gagné, sinon Γ est réel on utilise la Proposition 5.9(ii) et une étude au cas par cas nous fournit le graphe de racines cherché. ■

5.4.2 Cas des groupes de dimensions 4

Soit G un groupe de réflexions complexe primitif de dimension 4 engendré par des réflexions d'ordres 2. Posons $m = d(G)$, $m \leqslant 4$ par la Proposition 5.10. Par le Théorème 4.20 et la Proposition 5.8(i) il existe un graphe de racines Γ_0 :

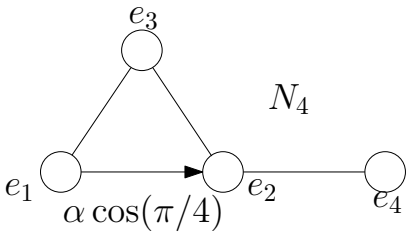


avec $\alpha \in \mathbf{U} \setminus \mathbf{R}$ et $\mathrm{W}(\Gamma_0) \subset G$.

Le Lemme 4.19(i) et le Corollaire 4.21 nous donnent une racine unitaire $e_4 \in G$ telle que le graphe Γ engendré par e_1, e_2, e_3, e_4 est irréductible, et même primitif si $m = 4$.

Proposition 5.11:

(i) $m = 4$ *et* Γ *est équivalent à* N_4 *:*



($\alpha = \frac{\sqrt{2}}{2}(1-i)$*)*

(ii) G est conjugué à $\mathrm{W}(N_4)$ *ou à* $\mathrm{EW}(N_4)$.

(iii) Il n'existe pas de groupe de réflexions irréductible de dimension $\geqslant 5$ *contenant un sous-groupe conjugué à* $\mathrm{W}(N_4)$ *ou* $\mathrm{EW}(N_4)$.

(iv) Si H *est un groupe de réflexions primitif de dimension* $\geqslant 5$, *alors* $d(H) = 3$.

Démonstration:

(i) La Proposition 5.8(i) et la Proposition 5.9 montrent qu'il suffit d'étudier les cas
- $m = 3$, $\Gamma_0 = D_3(3)$.
- $m = 4$, $\Gamma_0 = D_3(4)$ et G ne contient pas de sous-groupe de réflexions complexe primitif de dimension 3.
- $m = 4$, $\Gamma_0 = J_3(4)$.

Une étude détaillée montre alors que dans le premier cas ($m = 3$), G contient un sous-groupe de réflexions conjugué à $\mathrm{W}(D_4(3)) = \mathrm{G}(3, 3, 4)$. Mais alors $\langle G, j\,\mathrm{Id}_4\rangle$ est un groupe primitif qui contient à la fois des réflexions d'ordres 2 et 3, ce qui contredit la Proposition 5.6(iii).

Donc $m = 4$, et une nouvelle étude montre que Γ est équivalent soit à $D_4(4)$, soit à N_4. La première possibilité étant impossible puisque $D_4(4)$ est imprimitif, Γ est bien équivalent à N_4.

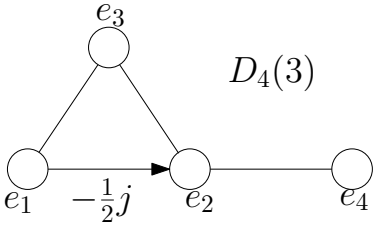
(ii) C'est immédiat par (i) et le Théorème 4.37(ii).

(iii) Si H est un groupe de réflexions irréductible qui contient $\mathrm{EW}(N_4)$, il contient $\mathrm{W}(N_4)$. Si $H \supset \mathrm{W}(N_4)$, comme $\mathrm{W}(N_4)$ est primitif, H l'est aussi par le Lemme 2.10, or $\mathcal{Z}(\mathrm{W}(N_4)) = 4$ donc cela contredit le Corollaire 5.2(iii).

(iv) Si H est un groupe de réflexions primitif de dimension $\geqslant 5$, on a vu qu'il ne contient que des réflexions d'ordres 2. Si H est réel, $d(H) = 3$. Si H est complexe, la Proposition 5.10 montre déjà que $d(H) \leqslant 4$. Si $d(H) = 4$, alors le Corollaire 4.21 nous fournit un sous-groupe de réflexions de H primitif de dimension 4, donc conjugué à $\mathrm{W}(N_4)$ ou $\mathrm{EW}(N_4)$ par (ii), ce qui contredit (iii).■

5.4.3 Cas des groupes de dimensions $\geqslant 5$

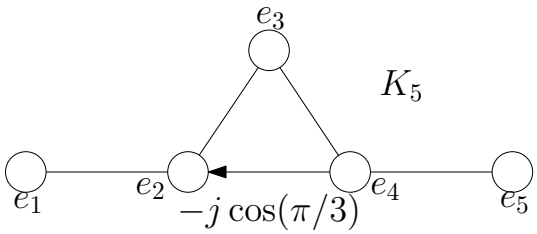
Soit G un groupe de réflexions complexe primitif de dimension 5. On sait que G ne contient que des réflexions d'ordres 2 (cf. la Section 5.3), et que $d(G) = 3$ (Proposition 5.11(iv)). G contient un sous-groupe de réflexions G_0 complexe irréductible de dimension 4 (par le Théorème 4.20 et le Lemme 4.19(i)). G_0 n'est pas primitif par la Proposition 5.11 (ii) et (iii). D'où $G_0 = \mathrm{G}(3, 3, 4)$ ($G_0 \neq \mathrm{G}(3, 1, 4)$ car G ne contient que des réflexions d'ordres 2), qui est représenté par le graphe de racines $D_4(3)$:



Il existe une racine unitaire e_5 de G telle que e_1, e_2, e_3, e_4, e_5 engendrent un graphe de racines Γ primitif par la Proposition 2.12.

Proposition 5.12:

(i) Γ *est équivalent à* K_5 *:*



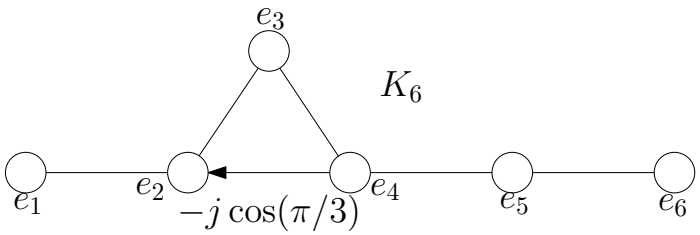
(ii) G *est conjugué à* $\mathrm{W}(K_5)$*.*

Démonstration: Comme d'habitude (i) est une étude au cas par cas et (ii) vient du Théorème 4.37(ii). ■

Soit G un groupe de réflexions complexe primitif de dimension 6. Alors G ne contient à nouveau que des réflexions d'ordres 2 et $d(G) = 3$. Le Corollaire 4.21 nous fournit un graphe de racines Γ_0 primitif de dimension 5 tel que $\mathrm{W}(\Gamma_0) \subset G$. Γ_0 est équivalent à K_5 d'après la Proposition 5.12(ii). Encore une fois, il existe une racine unitaire $e_6 \in G$ telle que Γ et e_6 engendrent un graphe de racines Γ primitif (Lemme 2.10).

Proposition 5.13:

(i) Γ *est équivalent à* K_6*.*



(ii) G *est conjugué à* $\mathrm{W}(K_6)$*.*

(iii) Il n'existe pas de groupe de réflexions primitif de dimension $\geqslant 7$*.*

Démonstration: On procède encore une fois comme dans la Proposition 5.12 pour (i) et (ii). Maintenant, si H est primitif de dimension > 6, G est engendré par des réflexions d'ordres 2 et $d(G) = 3$. Le Corollaire 4.21 montre que H contient $\mathrm{W}(K_5)$. On étend K_5 en un graphe de racines de dimension 6, il sera primitif par le Lemme 2.10, donc équivalent à K_6 par (ii). Donc H contient $\mathrm{W}(K_6)$, mais $|\mathcal{Z}(\mathrm{W}(K_6)) = 6|$ et cela contredit le Corollaire 5.2(ii). ■

On a ainsi terminé la classification.

5.5 Récapitulatif des groupes de réflexions irréductibles

On récapitule l'ensemble des groupes de réflexions irréductibles dans le Tableau 5.1. On note qu'il existe deux familles infinies, $\mathrm{W}(A_n)$ qui est primitive, et $\mathrm{G}(de, e, n)$ qui est imprimitive (en effet, on peut voir $\mathbf{C}_m$ comme $\mathrm{G}(m, 1, 1)$). On rappelle que l'on pose $m = de$. Les 34 groupes sporadiques restants sont primitifs.

Les groupes réels sont ceux qui ont un degré caractéristique égal à 2, il y a $\mathrm{W}(A_n)$, $\mathrm{W}(B_n) = \mathrm{G}(2, 1, n)$, $\mathrm{W}(D_n) = \mathrm{G}(2, 2, n)$, $\mathrm{W}(H_3)$, $\mathrm{W}(F_4)$, $\mathrm{W}(H_4)$, $\mathrm{W}(E_6)$, $\mathrm{W}(E_7)$ et $\mathrm{W}(E_8)$.

Ces groupes sont tous engendrés par n réflexions où n est leur dimension (et donc représentables par des graphes de racines) sauf $G(de, e, n)$ lorsque $e \neq 1$ et $d \neq 1$, $\mathrm{EW}(N_4)$ et les groupes de dimensions 2 de numéro $7, 11, 12, 13, 15, 19, 22$. On rappelle que $\mathrm{G}(m, 1, n)$ est représenté par $B_n(m)$, $\mathrm{G}(m, m, n)$ est représenté par $D_n(m)$ et que $(\mu_6 \,|\mu_2 \,; \mathbf{T} \,|\mathbf{D}_2)$ est représenté par L_2.

N°	Dim.	Groupe	Degrés	Ordre	Ordre du centre
1	n	$\mathrm{W}(A_n)$	$2, 3, \ldots, n+1$	$(n+1)!$	1
2	n	$\mathrm{G}(de, e, n)$	$m, 2m, \ldots, (n-1)m, dn$	$dm^{n-1}n!$	$d(e \wedge n)$
3	1	$\mathbf{C}_m$	m	m	m
4	2	$(\mu_6 \,\vert \mu_2 \,; \mathbf{T} \,\vert \mathbf{D}_2)$	4,6	24	2
5	2	$\mu_6\mathbf{T}$	6,12	72	6
6	2	$(\mu_{12} \,\vert \mu_4 \,; \mathbf{T} \,\vert \mathbf{D}_2)$	4,12	48	4
7	2	$\mu_{12}\mathbf{T}$	12,12	144	12
8	2	$(\mu_8 \,\vert \mu_4 \,; \mathbf{O} \,\vert \mathbf{T}_2)$	8,12	96	4
9	2	$\mu_8\mathbf{O}$	8,24	192	8
10	2	$(\mu_{24} \,\vert \mu_{12} \,; \mathbf{O} \,\vert \mathbf{T}_2)$	24,12	288	12
11	2	$\mu_{24}\mathbf{O}$	24,24	576	24
12	2	$(\mu_4 \,\vert \mu_2 \,; \mathbf{O} \,\vert \mathbf{T}_2)$	6,8	48	2
13	2	$\mu_4\mathbf{O}$	8,12	96	4
14	2	$(\mu_{12} \,\vert \mu_6 \,; \mathbf{O} \,\vert \mathbf{T}_2)$	6,24	144	6
15	2	$\mu_{12}\mathbf{O}$	12,24	288	12
16	2	$\mu_{10}\mathbf{I}$	20,30	600	10
17	2	$\mu_{20}\mathbf{I}$	20,60	1200	20
18	2	$\mu_{30}\mathbf{I}$	30,60	1800	30
19	2	$\mu_{60}\mathbf{I}$	60,60	3600	60
20	2	$\mu_6\mathbf{I}$	12,30	360	6
21	2	$\mu_{12}\mathbf{I}$	12,60	720	12
22	2	$\mu_4\mathbf{I}$	12,20	240	4
23	3	$\mathrm{W}(H_3)$	$2, 6, 10$	120	2
24	3	$\mathrm{W}(J_3(4))$	$4, 6, 14$	336	2
25	3	$\mathrm{W}(L_3)$	$6, 9, 12$	648	3
26	3	$\mathrm{W}(M_3)$	$6, 12, 18$	1296	6
27	3	$\mathrm{W}(J_3(5))$	$6, 12, 30$	2160	6
28	4	$\mathrm{W}(F_4)$	$2, 6, 8, 12$	1152	2
29	4	$\mathrm{W}(N_4)$	$4, 8, 12, 20$	7680	4
30	4	$\mathrm{W}(H_4)$	$2, 12, 20, 30$	14400	2
31	4	$\mathrm{EW}(N_4)$	$8, 12, 20, 24$	64.6 !	4
32	4	$\mathrm{W}(L_4)$	$12, 18, 24, 30$	216.6 !	6
33	5	$\mathrm{W}(K_5)$	$4, 6, 10, 12, 18$	72.6 !	2
34	6	$\mathrm{W}(K_6)$	$4, 12, 18, 24, 30, 42$	108.9 !	2
35	6	$\mathrm{W}(E_6)$	$2, 5, 6, 8, 9, 12$	72.6 !	1
36	7	$\mathrm{W}(E_7)$	$2, 6, 8, 10, 12, 14, 18$	8.9 !	2
37	8	$\mathrm{W}(E_8)$	$2, 8, 12, 14, 18, 20, 24, 30$	192.10 !	2

TAB. 5.1 – Groupes de réflexions irréductibles

Annexe A

Le théorème de Blichfeldt

.

Nous prouvons ici le Théorème 5.1. Pour cela, nous avons d'abord besoin d'énoncer le théorème de Clifford, qui nous fournira au passage la reformulation de la notion d'imprimitivité énoncée dans la Remarque 2.2. Si G est un groupe, et $x, g \in G$, on utilise la notation habituelle $x^g := gxg^{-1}$.

A.1 Le théorème de Clifford

Théorème A.1 (Théorème de Clifford): *Soit k un corps, G un groupe, V un $k[G]$-module irréductible et N un sous-groupe normal de G. Soit W un $k[N]$-sous-module de V. Alors :*

(i) Si $W \neq 0$, alors $V = \sum_{g\in G} gW$. Si W est irréductible, chaque gW l'est aussi, ce qui montre que V est complètement réductible (semi-simple) en tant que $k[N]$-module.

(ii) Soit $W_1, \ldots, W_m$ des représentants des classes d'isomorphismes des $k[N]$-sous-modules irréductibles de V. Soit V_i la somme de tous les $k[N]$-sous-modules de V isomorphes à W. Alors $V = V_1 \oplus \cdots \oplus V_m$.

(iii) Si $g \in G$, pour tout i il existe j tel que $gV_i = V_j$. G agit comme un groupe de permutation transitif sur $\{V_1, \ldots, V_m\}$.

(iv) Si $H_1 = \{g \in G, gV_1 = V_1\}$, alors V_1 est un $k[H_1]$-module irréductible et $V \simeq \mathrm{Ind}_{H_1}^G V_1 = k[G] \otimes_{k[H_1]} V_1$.

(v) Il existe $e \in \mathbf{N}$ tel que $V \simeq e(W_1 \oplus \cdots \oplus W_n)$ (en tant que $k[N]$-module).

(vi) Si on note χ_i le caractère χ_{W_i}, alors

$$\chi_V = e(\chi_1 + \cdots + \chi_m)$$

et si $W_i = g_i W_1$ ($g_i \in G$), $\chi_i(x) = \chi_1(x^{g_i})$ pour tout $x \in N$.

Démonstration:

(i) $V_0 = \sum_{g\in G} gW$ est stable par G donc est égal à V puisque V est irréductible. Comme N est normal dans G, les gW sont aussi des $k[N]$-modules (car ce sont des $k[N^g]$-modules). Si W est irréductible, gW l'est aussi car s'il contenait un sous-module stable W_0, $g^{-1}W_0$ serait un sous-module stable de W, contradiction. Ainsi V est somme directe de sous-modules irréductibles[1], donc est complètement réductible.

(ii) $V = V_1 + \cdots + V_m$ par (i), il reste à voir que la somme est directe. Mais si L est un sous-module irréductible de V_i, $L \simeq W_i$. En effet, par définition $V_i = W_i \oplus \cdots \oplus W_i$, si l'on note π_j la projection sur le j^{eme} facteur, il existe j_0 tel que $\pi_{j_0}(L) \neq 0$, donc $\pi_{j_0}|_L$ est un isomorphisme de L sur W_i. Comme $V_1 + \cdots + V_{i-1}$ est une somme directe (avec multiplicités) de W_j, $j < i$, le même raisonnement nous montre que si $L \bigcap (V_1 + \cdots + V_{i-1}) \neq 0$, L est isomorphe à l'un des W_j, ce qui est absurde car on a vu que $L \simeq W_i$. Donc $V_i \bigcap (V_1 + \cdots + V_{i-1}) = 0$, ce qui montre que la somme est bien directe.

(iii) – $V_i = \sum \{xW_1, x \in G \text{ et } xW_1 \simeq W_i\}$. En effet, si on note $U_i = \sum \{xW_1, x \in G \text{ et } xW_1 \simeq W_i\}$, on a $U_i \subset V_i$ par définition, mais comme $V = U_1 + \cdots + U_m$ par (i), $U_i = V_i$.

– Si U et U' sont deux $k[N]$-sous-modules de V, et $U \simeq U'$, alors $gU \simeq gU'$ pour tout $g \in G$. En effet, soit $\varphi : U \to U'$ un isomorphisme, $\varphi^g : gU \to gU'$ est une bijection linéaire, il reste à vérifier qu'il commute avec l'action de N. Mais si $x \in U$: $(g\varphi g^{-1})(n.gx) = g\varphi((g^{-1}ng).x) = g(g^{-1}ng)\varphi(x) = n.(g\varphi g^{-1})(gx)$.

On en déduit que $gV_i \subset V_j$ si $gW_i \simeq W_j$. Si l'inclusion est stricte, $V_i \subsetneq g^{-1}V_j$ mais comme $g^{-1}W_j \simeq W_i$, $g^{-1}V_j \subset V_i$ et l'on obtient une contradiction. G agit bien sur $\{V_1, \ldots, V_m\}$, et l'action est transitive car V est irréductible en tant que $k[G]$-module.

(iv) (On note que (iii) montre que $H_1 = g \in G, gW_1 \simeq W_1$). Soit $x_j \in G$ tel que $x_jV_1 = V_j$, de tels x_j existent par (iii). On vérifie immédiatement que les classes à gauche de H_1 dans G sont $x_1H_1, \ldots, x_mH_1$, en particulier $m = [G : H_1]$.

Ainsi, $k[G] \otimes_{k[H_1]} V_1 = (x_1 \otimes V_1) \oplus \cdots \oplus (x_m \otimes V_1)$. Si $v = x_i \otimes v_1 \in k[G] \otimes_{k[H_1]} V_1$ est un tenseur pur, et $g \in G$, on rappelle que l'action de g sur v est définie comme suit :

$$g.x_i \otimes v_1 = x_j \otimes hv_1 \quad \text{si } gx_i = x_jh$$

On définit $\varphi : x_1.V_1 \oplus \cdots \oplus x_m.V_1 \to x_1 \otimes V_1 \oplus \cdots \oplus x_mV_m$ par

$$\varphi : \sum x_i.u_i \mapsto \sum x_i \otimes u_i$$

si $g \in G$ est tel que $gx_i = x_jh$, alors $g(x_i.u_i) = x_j.hu_i$ et $g(x_i \otimes u_i) = x_j \otimes hu_i$, donc φ est bien un isomorphisme. Ceci montre que V_1 est irréductible comme $k[H_1]$-module, car s'il avait un sous-module non trivial V_1', $\mathrm{Ind}_{H_1}^G V_1'$ serait un $k[G]$-sous-module non-trivial de V.

[1]On rappelle que si W est un sous-module irréductible et U un sous-module de V, alors si $W \bigcap U \neq 0$, $W \subset U$ (considérer le sous-module engendré par un élément de $W \bigcap U$), donc en procédant par induction on peut bien obtenir une somme directe, non canonique, de modules irréductibles

(v) $W_i = x_i W_1$ et $V_i = x_i V_1$, donc $\dim W_i = \dim W_1$, $\dim V_i = \dim V_1$ pour tout i. Il suffit alors de poser $e = \dim V_1 / \dim W_1$.

(vi) Immédiat par (v). ■

Remarque A.2: Le Théorème A.1(iii) montre que V est imprimitif si $V_1 \neq V$. De plus $N \subset \{g \in G, gV_i = V_i \quad (\forall 1 \leqslant i \leqslant m)\}$.

Réciproquement, si V est un $k[G]$-module irréductible tel que V admet un système d'imprimitivité $\{V_1, \ldots, V_m\}$, posons $H = \{g \in G, gV_1 = V_1\}$ et $N = \{g \in G, gV_i = V_i \quad (\forall 1 \leqslant i \leqslant m)\}$. Alors $N = \bigcap_{g \in G} H^g$ est distingué dans H et dans G. De plus la même preuve que celle du Théorème A.1(iii) montre que $V \simeq \mathrm{Ind}_H^G V_1$ et que V_1 est un $k[H]$-module irréductible.

A.2 Les groupes linéaires primitifs finis

Soit V un $\mathbf{C}$-ev de dimension n et $G \subset \mathrm{GL}(V)$ un groupe linéaire primitif fini. On suppose que l'on a choisi une forme hermitienne définie positive telle que $G \subset \mathrm{U}(V)$.

Définition A.3 (phases d'une matrice unitaire): Si S est une matrice unitaire de $\mathrm{M}_n(\mathbf{C})$, et que les valeurs propres distinctes de S sont $\left\{e^{i\theta_1}, \ldots, e^{i\theta_m}\right\}$, alors les angles $\theta_1, \ldots, \theta_m$ sont appelés les phases de S.

Lemme A.4: *Soit $S, T \in \mathrm{U}_n(\mathbf{C})$ des matrices unitaires. On suppose de plus que S est diagonale, et que les phases de S sont sur un arc de cercle du cercle unité de longueur $< \pi$. Soit $U = T^{-1}ST$, et notons $S = (\alpha_i \delta_i^j), T = (a_{ij})$ et $U = (b_{ij})$. Alors*

(i) $b_{ii} \neq 0$ (pour tout $1 \leqslant i \leqslant n$)

(ii) Si b_{jj} est une racine de l'unité, et que i, l sont tels que $a_{ij} \neq 0, a_{lj} \neq 0$, alors $\alpha_i = \alpha_l$.

Démonstration:

(i) $T^{-1} = (\overline{a_{ji}})$, d'où

$$b_{ij} = \sum_{k,l} \overline{a_{ki}} \alpha_k \delta_k^l a_{lj} = \sum_k \overline{a_{ki}} a_{kj} \alpha_k$$

En particulier

$$b_{ii} = \sum_k |a_{ki}|^2 \alpha_k$$

Or comme T est unitaire, $\sum_k |a_{ki}|^2 = 1$. Comme les α_k sont du même côté du cercle unité, on a bien $b_{ii} \neq 0$.

(ii) Les deux équations

$$b_{jj} = \sum_k |a_{kj}|^2 \alpha_k, \quad 1 = \sum_k |a_{kj}|^2$$

et le cas d'égalité dans Cauchy-Schwartz montrent que $|b_{jj}| = 1$ si et seulement si les α_k sont égaux pour tout k tel que $a_{kj} \neq 0$. ■

Théorème A.5 (Blichfeldt): *On choisit une base de V, ce qui permet identifier G à un sous groupe de $\mathrm{U}_n(\mathbf{C})$. Soit $s \in G$ une matrice diagonale de phases $\theta_1, \dots, \theta_m$ telles que $|\theta_i - \theta_1| \leqslant \pi/3$ $(\forall 1 \leqslant i \leqslant m)$. Alors $s \in \mathcal{Z}(G)$.*

Démonstration: On note $\alpha_j = e^{i\theta_j}$. Quitte à conjuguer G par une matrice de permutation, on peut supposer que $s = \mathrm{diag}(\alpha_1, \dots, \alpha_1, \alpha_2, \dots, \alpha_m, \dots, \alpha_m)$, et on note k la multiplicité de la valeur propre α_1 dans s.

On dit qu'une matrice $n \times n$ est k-réduite si elle est de la forme :

$$\begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix}$$

où C est une matrice $k \times k$ et D une matrice $(n-k) \times (n-k)$. Si (a_{ij}) est une matrice unitaire, on définit $f((a_{ij})) := |a_{11} + \cdots + a_{kk}|$. Soit

$$S = \left\{ g^{-1}sg, g \in G \text{ et } g^{-1}sg \text{ n'est pas } k\text{-réduite} \right\}$$

Si $S \neq \varnothing$, prenons $t_0 \in S$ tel que $f(t_0)$ soit maximal. Alors

$$t_0^{-1} s t_0 \notin S \tag{A.1}$$

En effet, si on pose $s = (\gamma_i \delta_i^j)$ (ainsi $\gamma_1 = \cdots = \gamma_k = \alpha_1, \gamma_{k+1} = \alpha_2, \dots$), $t_0 = (a_{ij}$ et $t_0^{-1} s t_0 = (b_{ij})$ on a

$$b_{jj} = \sum_l |a_{lj}|^2 \gamma_l$$

De plus $1 = \sum_l |a_{lj}|^2 = \sum_l |a_{jl}|^2$ car t_0 est unitaire. En particulier, si $|a_{kk}| = 1$, les (a_{kl}) et les (a_{lk}) sont nuls pour tout $1 \leqslant k \leqslant n$. Comme t_0 n'est pas k-réduite, il existe $r_0 \in \{1, \dots, k\}$ tel que $|a_{r_0 r_0}| < 1$. De plus si on pose $\beta_l = e^{-i\theta_1}\gamma_l$ et que $\beta_l = \cos\varphi_l + i \sim \varphi_l$, par hypothèse $\varphi_l \leqslant \pi/3$ d'où $\cos\varphi_l \geqslant 1/2$ (et $\cos\varphi_l = 1$ si $1 \leqslant l \leqslant k$). On a :

$$\begin{aligned}
f(t_0^{-1}st_0) = |b_{11} + \cdots + b_{kk}| &= \left| \sum_{r=1}^{k} \sum_{j=1}^{n} |a_{jr}|^2 \gamma_j \right| = \left| \sum_{r=1}^{k} \sum_{j=1}^{n} |a_{jr}|^2 \beta_j \right| \\
&\geqslant \sum_{r=1}^{k} \sum_{j=1}^{n} |a_{jr}|^2 \cos\varphi_j \geqslant \sum_{r=1}^{k} \left(\sum_{j=1}^{k} |a_{jr}|^2 + \frac{1}{2} \sum_{j=k}^{n} |a_{jr}|^2 \right) \\
&= \sum_{r=1}^{k} \left(\sum_{j=1}^{k} |a_{jr}|^2 + \frac{1}{2} \left(1 - \sum_{j=1}^{k} |a_{jr}|^2 \right) \right) = \sum_{r=1}^{k} \left(\frac{1}{2} \left(1 + \sum_{j=1}^{k} |a_{jr}|^2 \right) \right) \\
&\geqslant \sum_{r=1}^{k} \frac{1}{2} \left(1 + |a_{rr}|^2 \right) > \sum_{r=1}^{k} |a_{rr}| \geqslant |a_{11} + \cdots + a_{kk}| = f(t_0)
\end{aligned}$$

où l'inégalité stricte vient du fait que $\frac{1}{2}(1 + x^2) \geqslant x$ pour tout $x \in \mathbf{R}$, avec égalité si et seulement si $x = 1$. Ce qui prouve bien (A.1).

$$S = \varnothing, \text{ autrement dit tous les conjugués de } s \text{ dans } G \text{ sont } k\text{-réduits} \tag{A.2}$$

Sinon, on prend t_0 comme dans (A.1), on sait alors que $t_0^{-1}st_0$ est k-réduite. Il existe une matrice $k \times k$ unitaire U telle que

$$\begin{pmatrix} U & 0 \\ 0 & \mathrm{Id} \end{pmatrix}^{-1} t_0^{-1}st_0 \begin{pmatrix} U & 0 \\ 0 & \mathrm{Id} \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & E \end{pmatrix}$$

où D est une matrice $k \times k$ diagonale. On remarque que conjuguer G par $\begin{pmatrix} U & 0 \\ 0 & \mathrm{Id} \end{pmatrix}$ ne change pas s (puisque s agit comme un scalaire sur les k premiers éléments de la base), de plus pour tout $g \in G$, si la décomposition en blocs de g est $g = \begin{pmatrix} A & B \\ C & F \end{pmatrix}$ avec A une matrice $k \times k$, alors

$$\begin{pmatrix} U & 0 \\ 0 & \mathrm{Id} \end{pmatrix}^{-1} \begin{pmatrix} A & B \\ C & F \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & \mathrm{Id} \end{pmatrix} = \begin{pmatrix} U^{-1}AU & U^{-1}B \\ CU & F \end{pmatrix}$$

et cette dernière matrice est k-réduite si et seulement si g l'est. Donc on peut conjuguer G par $\begin{pmatrix} U & 0 \\ 0 & \mathrm{Id} \end{pmatrix}$, puisque cela ne change pas S.

Ainsi on s'est ramené au cas $t_0^{-1}st_0 = \begin{pmatrix} D & 0 \\ 0 & E \end{pmatrix}$, où $D = (\tau_i\delta_i^j)_{1 \leqslant i,j \leqslant k}$ et les τ_i sont des racines de l'unité puisque $t_0^{-1}st_0$ est unitaire. De plus t_0 étant un conjugué de s, le Lemme A.4(i) montre que $a_{ii} \neq 0$. Soit $i \leqslant k$ et $l > k$, alors $\gamma_i \neq \gamma_j$ et le Lemme A.4(ii) (avec $j = i$) montre que $a_{li} = 0$. Ainsi t_0 est de la forme $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ où 0 est une matrice $(n-k) \times k$. Mais t_0 étant unitaire, on a :

$$\mathrm{Id} = \begin{pmatrix} t_{\overline{A}} & 0 \\ t_{\overline{B}} & t_{\overline{D}} \end{pmatrix} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} t_{\overline{A}}A & t_{\overline{A}}B \\ t_{\overline{B}}A & t_{\overline{B}}B + t_{\overline{D}}D \end{pmatrix}$$

ce qui force $B = 0$. Ainsi t_0 est k-réduit, ce qui contredit le choix de t_0 et montre (A.2).

Si l'on note G_0 le sous-groupe normal de G engendré par les conjugués de s, (A.2) montre que G_0 est réductible, et même complètement réductible par le Théorème A.1(i). De plus G étant primitif, le Théorème A.1(iii) montre que V n'a qu'une composante isotypique. Mais on a construit un $\mathbf{C}[G_0]$-module de dimension k sur lequel s agit comme un scalaire. Il existe donc un sous-module irréductible W sur lequel s agit comme un scalaire, par ce qui précède $V \simeq W \oplus \cdots \oplus W$ donc s agit comme un scalaire sur tout V. On a bien $s \in \mathcal{Z}(G)$. ■

Remarque A.6: Soit k un corps algébriquement clos, V un k-ev de dimension n et $G \subset \mathrm{GL}(V)$ un groupe linéaire primitif fini. La même méthode qu'à la fin de la preuve du Théorème A.5 montre plus généralement que si A un sous-groupe abélien et normal de G, alors A est cyclique et $A \subset \mathcal{Z}(G)$.

En effet, par le Théorème A.1, et comme G est primitif, $V = V_1$ (avec les notations du théorème). Ainsi $V \simeq W_1 \oplus \cdots \oplus W_1$ où W_1 est un $k[A]$-module irréductible. Comme l'action de A dans V est fidèle, c'est également le cas pour son action sur W_1. Comme W_1 est irréductible, et que k est algébriquement clos, $\mathrm{End}_{k[A]}(W_1) = k\,\mathrm{Id}_{W_1}$.

Comme A est abélien, $A \subset End_{k[A]}(W_1)$, donc A agit par des matrices scalaires sur W_1, d'où $\dim W_1 = 1$ vu que W_1 est irréductible. A agit aussi par matrices scalaires sur V, donc $A \subset \mathcal{Z}(G)$ et est cyclique car $\mathcal{Z}(G)$ l'est (on rappelle que si $G \subset \mathrm{GL}(V)$ est irréductible, $\mathcal{Z}(G) = k\,\mathrm{Id} \bigcap G$ est un sous-groupe de k, donc cyclique si G est fini).

Bibliographie

[Bec06] V. Beck. *TD du cours de Master 2 : Autour des groupes de réflexions.*, 2006. (`http://www.math.jussieu.fr/~beck/`).

[BMR98] M. Broué, G. Malle, and R. Rouquier. Complex reflection groups. *J. reine angew. Math*, 500 :127–190, 1998.

[Bou68] N. Bourbaki. *Groupes et algèbres de Lie, Chapitres 4-5-6*. Hermann, 1968.

[Bro00] M. Broué. Reflection groups, braid groups, hecke algebra, finite reductive groups. *Current Developments in Mathematics*, Current Developments in Mathematics :1–107, 2000.

[Coh76] A. M. Cohen. Finite complex reflection groups. *Annales scientifiques de l'École Normale Supérieure*, 9 :379–436, 1976.

[GAP06] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2006. (`http://www.gap-system.org`).

[Mic04] J. Michel. *Groupes finis de réflexion, cours de troisième cycle*, 2004. (`http://www.math.jussieu.fr/~jmichel/cours2004.pdf`).

[Spr74] T. A. Springer. Regular elements of finite reflection groups. *Canadian Journal of Mathematics*, 25 :159–198, 1974.

[ST54] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canadian Journal of Mathematics*, 6 :274–304, 1954.

[Ste74] R. Steinberg. Regular elements of finite reflection groups. *Invent. Math.*, 112 :392–400, 1974.

Modules de Clifford et K-théorie

Damien Robert et Mehdi Tibouchi
sujet proposé par François Pierrot

1er juillet 2004

Résumé

La multiplication de Clifford sur l'algèbre extérieure associée à un fibré vectoriel euclidien est un outil fécond pour l'étude, par exemple, des champs de vecteurs. On présente ici l'application que Atiyah, Bott et Shapiro [MA64] en ont donné en K-théorie, en construisant un isomorphisme de Thom pour une certaine classe de fibrés vectoriels. Les méthodes employées préfigurent une partie de celles qui interviendront plus tard dans la théorie de l'indice d'Atiyah-Singer.

Table des matières

1 Notions préliminaires : groupe de Grothendieck, modules, fibrés vectoriels

La notion de groupe de Grothendieck intervient à plusieurs niveaux dans les constructions qui nous intéressent ici. Il est sans doute intéressant de donner quelques définitions générales. On s'inspire largement des chapitres 1 et 2 de [Wei97] et [Hat03].

1.1 Groupe de Grothendieck d'une catégorie additive

Définition 1 Une catégorie $\mathcal{C}$, supposée petite,[1] est dite *additive* lorsque les deux axiomes suivants sont vérifiés :

- les ensembles de morphismes $\mathrm{Hom}_{\mathcal{C}}(A, B)$ sont munis d'une structure de groupe abélien, et cette la loi de groupe est distributive sur la composition des morphismes.
- $\mathcal{C}$ possède un objet nul (à la fois initial et final) et admet des produits finis.

Ces axiomes assurent l'existence de coproduits finis qui coïncident avec les produits (la flèche $A \to A \times B$ est obtenue, comme pour les groupes abéliens, en composant par l'isomorphisme évident $A \xrightarrow{\sim} A \times 0$). L'opération correspondante sur les objets est appelée *somme directe* et notée $\oplus$. Elle fait de l'ensemble des objets un monoïde commutatif.

Définition 2 Soit M un monoïde commutatif. On appelle *symétrisé* de M un groupe abélien $S(M)$ muni d'un morphisme de monoïdes $f : M \to S(M)$, et universel au sens où tout morphisme de monoïdes de M vers un groupe abélien se factorise de manière unique par f.

Il est clair que s'il existe, le symétrisé est unique à isomorphisme près. De plus, tout monoïde M admet bien un symétrisé, qu'on peut voir comme le groupe abélien engendré par les $[m]$, $m \in M$, soumis aux relations $[m + n] = [m] + [n]$. Cette construction possède en outre des propriétés évidentes de fonctorialité : S n'est autre, par parenthèse, que l'adjoint à gauche du foncteur d'oubli des groupes abéliens dans les monoïdes commutatifs.

Définition 3 Pour toute catégorie additive $\mathcal{C}$, on appelle groupe de Grothendieck de $\mathcal{C}$, et l'on note $K_0(\mathcal{C})$, le symétrisé du monoïde des objets de $\mathcal{C}$.

Les deux exemples cruciaux de cette construction qu'on va utiliser dans la suite sont celui de certaines catégories de modules sur un anneau, et celui des fibrés vectoriels sur un espace topologique. Dans ces deux cas (et pour une base commutative, dans le cas des anneaux), notons que l'on dispose en plus d'une structure multiplicative donnée par le produit tensoriel. Comme il est distributif sur la somme directe, il fournit une structure d'anneau commutatif sur le groupe de Grothendieck.

[1] On passera sous silence les détails de théorie des ensembles. Au besoin, on travaillera dans un univers fixé dans lequel on prendra tous les objets et morphismes, et toutes les catégories seront donc petites.

1.2 Modules sur un anneau et K_0 algébrique

Soit R un anneau non nécessairement commutatif. Le groupe de Grothendieck de la catégorie additive des R-modules à gauche quelconques n'est pas très intéressant, puisque pour tout module M, on peut écrire $M \oplus M^\infty = M^\infty$, et donc $[M] = 0$ dans le groupe de Grothendieck.

On obtient un objet beaucoup plus intéressant si l'on se restreint à la catégorie $\mathbf{Mod}(R)$ des R-modules à gauche de type fini, mais il a tendance, cette fois, à être trop gros (le théorème de structure des groupes abéliens de type fini dit par exemple que $K_0\,\mathbf{Mod}(\mathbf{Z})$ est le groupe abélien libre engendré par $[\mathbf{Z}]$ et les $[\mathbf{Z}/p^k\mathbf{Z}]$ pour tout nombre premier p et tout $k \geqslant 1$). La catégorie que l'on préfère considérer, et qui fournit une construction plus maniable, est celle des modules *projectifs* de type fini, c'est-à-dire des modules qui sont facteurs directs de R-modules libres de type fini.

Définition 4 On note $\mathbf{Pr}(R)$ la catégorie additive des R-modules à gauche projectifs de type fini. Son groupe de Grothendieck est appelé groupe de Grothendieck de R, et noté $K_0(R)$.

Par exemple, si tout R-module projectif de type fini est libre, $K_0(R)$ est le groupe monogène engendré par $[R]$. C'est par exemple le cas quand R est un corps ou un anneau principal (et alors $K_0(R)$ est même $\mathbf{Z}$ en tant qu'anneau).

Remarque Deux modules projectifs M et N définissent la même classe dans $K_0(R)$ si et seulement s'ils sont *stablement équivalents*, c'est-à-dire qu'il existe n tel que $M \oplus R^n$ est isomorphe à $N \oplus R^n$. En effet, $K_0(R)$ est obtenu à partir du monoïde des classes d'isomorphisme de $\mathbf{Pr}(R)$ en adjoignant formellement un inverse à $[R]$, puisque alors tout module projectif a un inverse : si $M \oplus M' = R^k$, on a : $-[M] = [M'] - k[R]$. C'est sous cette forme, comme théorie de l'équivalence stable, qu'apparaît classiquement la K-théorie.

Remarque Une autre remarque importante est que le K_0 algébrique est fonctoriel au sens suivant. Si $f : R \to S$ est un morphisme d'anneaux, on a un foncteur naturel $f_* : \mathbf{Pr}(R) \to \mathbf{Pr}(S)$ donné par l'extension des scalaires $(- \otimes_R S)$, qui commute aux sommes directes (et au produit tensoriel dans le cas commutatif), d'où un morphisme de groupes (et le cas échéant d'anneaux) $f_* : K_0(R) \to K_0(S)$. De plus, si S est un R-module projectif de type fini, la restriction des scalaires fournit dans l'autre sens un morphisme de groupes abéliens $f^* : K_0(S) \to K_0(R)$.

Exemple 1 Les anneaux dont on aura besoin du K_0 dans la suite sont des algèbres semi-simples finies sur des corps. Or il est facile de calculer le groupe de Grothendieck dans ce cas particulier. En effet, une telle algèbre A est produit d'un certain nombre n d'algèbres de matrices sur des corps gauches, a alors exactement n modules simples $V_1, \ldots, V_n$ à isomorphisme près (les «vecteurs colonnes» de ces algèbres de matrices), et tout module de type fini s'écrit comme somme de puissances des V_i (en particulier, tout module est projectif). Il en résulte que $K_0(A)$ est le groupe abélien libre engendré par les V_i.

1.3 Fibrés vectoriels et K_0 topologique

Soit X un espace topologique connexe. On a une théorie analogue à la précédente pour les fibrés vectoriels de base X.

1.3.1 Définition et constructions de base

Définition 5 Soit F un espace topologique non vide, et G un groupe d'homéomorphismes de F. On appelle *espace fibré sur* X de fibre F la donnée d'un espace topologique au-dessus de X, $\pi : E \to X$ dont les fibres sont homéomorphes à F, et tel que tout point x de X a un voisinage U au-dessus duquel il existe un homéomorphisme $\pi^{-1}(U) \to U \times F$ (où $U \times F$ est vu comme espace sur U par la première projection).

Un *fibré de groupe structural* G, ou G*-fibré*, sur X est un fibré E muni d'une action continue de G préservant les fibres, et telle que les trivialisations locales $\pi^{-1}(U) \to U \times F$ soient des G-morphismes pour l'action naturelle de G sur $U \times F$. Un G-fibré est dit *principal* si l'action sur chaque fibre est de plus simplement transitive.

Les morphismes de fibrés et de G-fibrés se définissent de la façon évidente.

Dans ce langage, un *fibré vectoriel* réel (resp. complexe) de rang n sur X est un fibré de fibre $\mathbf{R}^n$ (resp. $\mathbf{C}^n$) et de groupe structural $\mathrm{GL}_n(\mathbf{R})$ (resp. $\mathrm{GL}_n(\mathbf{C})$).

On note $\mathbf{VB_R}(X)$ et $\mathbf{VB_C}(X)$ les catégories des fibrés vectoriels réels et complexes sur X, et $\mathbf{VB}(X)$ si l'on ne veut pas préciser le corps de base. Ce sont des catégories additives : l'objet nul est $X \times 0$, la somme de morphismes de fibrés $E \to F$ se calcule fibre à fibre, et la somme directe $E \oplus F$ n'est autre que le produit fibré. Si l'on note $\pi : E \to X$ et $\pi' : F \to X$ les morphismes structuraux, on a :

$$E \oplus F = E \times_X F = \{(y, y') \in E \times F \ / \ \pi(y) = \pi'(y')\}$$

qui est naturellement un espace au-dessus de X, clairement localement trivial, et de fibre $(E \oplus F)_x = E_x \oplus F_x$.

Définition 6 On note $KO(X)$ et $K(X)$ les groupes de Grothendieck des catégories $\mathbf{VB_R}(X)$ et $\mathbf{VB_C}(X)$ respectivement. Ce sont les groupes de K-théorie réelle et complexe de l'espace X.

Exemple 2 L'exemple trivial, mais néanmoins essentiel, de cette construction, est celui où $X = *$ est réduit à un point. Alors un fibré vectoriel est juste la donnée d'un espace vectoriel, et l'on a donc $K(*) = KO(*) = \mathbf{Z}$. De façon moins triviale, la théorie qu'on va développer plus loin donnera une approche de la K-théorie des sphères. Il est en tout cas facile de voir que S^1 possède un fibré en droites réel non trivial, qui est le fibré de Möbius M. Il n'est pas très difficile de voir que $M \oplus M$ est trivial, et en fait $KO(S^1) = \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ est engendré par $[M]$ et le fibré trivial de rang 1.

Comme on l'a signalé, on dispose sur $\mathbf{VB}(X)$, et donc sur la K-théorie, d'une structure multiplicative donnée par le produit tensoriel. La façon la plus naturelle de le construire est sans doute par recollement.

De manière générale, pour un G-fibré $\pi : E \to X$ de fibre F, il existe un recouvrement ouvert (U_i) de X qui le trivialise. Notons $\eta_i : \pi^{-1}(U_i) \to U_i \times F$ les trivialisations locales. Alors les $\eta_j \circ \eta_i^{-1}$, avec l'abus de notation habituel, déterminent des G-automorphismes de $(U_i \cap U_j) \times F$, c'est-à-dire des applications $g_{ij} : U_i \cap U_j \to G$. E peut alors se voir comme quotient de la réunion disjointe des $U_i \times F$ par l'identification de $(x, v) \in U_i \times F$ avec $(x, g_{ij}(x)(v)) \in U_j \times F$ quand $x \in U_i \cap U_j$. Réciproquement, on vérifie immédiatement que la donnée, pour un recouvrement (U_i) de X, d'applications de recollement g_{ij} vérifiant la condition de compatibilité $g_{jk}g_{ij} = g_{ik}$ sur $U_i \cap U_j \cap U_k$ détermine un G-fibré sur X de fibre F.

On dispose alors d'une construction naturelle du produit tensoriel de deux fibrés E_1 et E_2 sur X, de rangs n_1 et n_2. On se donne pour cela un recouvrement (U_i) qui trivialise E_1 et E_2, et les applications de recollement correspondantes $g_{ij}^{(k)} : U_i \cap U_j \to \mathrm{GL}(E_k)$, $k = 1, 2$. Alors $E_1 \otimes E_2$ est le fibré vectoriel de rang $n_1 n_2$ déterminé par les applications de recollement :

$$g_{ij}^{(1)} \otimes g_{ij}^{(2)} : U_i \cap U_j \to \mathrm{GL}(E_1 \otimes E_2)$$

Il résulte des propriétés du produit tensoriel d'espaces vectoriels que l'opération $\otimes$ ainsi définie sur $\mathbf{VB}(X)$ est commutative, associative, distributive sur la somme directe, et a pour élément neutre le fibré trivial de rang 1. Elle fait donc de $K(X)$ et $KO(X)$ des anneaux commutatifs unitaires.

D'autres fibrés peuvent être déduits d'un fibré E de rang n par le même type de construction. Il s'agit des constructions habituelles de l'algèbre multilinéaire, comme les puissances symétriques et extérieures $\mathrm{Sym}^q(E)$, $\Lambda^q(E)$ et les algèbres graduées correspondantes, le fibré dual $\check{E} = \Lambda^{n-1}(E)$, les exponentielles internes, etc., mais aussi par exemple du fibré projectif $\mathbf{P}(E)$ de groupe structural PGL_n, et dont les fibres sont les $\mathbf{P}(E_x)$.

On sera amené à considérer plus particulièrement le cas où les fibres de E sont des espaces euclidiens ou hermitiens. Notons que quand la base X est paracompacte, tout fibré vectoriel a au moins une structure euclidienne ou hermitienne. En effet, par exemple dans le cas réel, soit (U_i) est un recouvrement de X trivialisant localement fini, (ϕ_i) une partition de l'unité subordonnée, et $\eta_i : \pi^{-1}(U_i) \to U_i \times \mathbf{R}^n$ les trivialisations locales. On obtient pour chaque i un produit scalaire $\langle \cdot, \cdot \rangle_i$ sur $\pi^{-1}(U_i)$ à partir de celui de $\mathbf{R}^n$, et il suffit de poser en chaque point $x \in X$:

$$\langle u, v \rangle_x = \sum_i \phi_i(x) \langle u, v \rangle_i$$

Cette structure euclidienne sur les fibres permet d'associer encore de nouveaux fibrés à E, notamment le fibré des sphères unité $\mathbf{S}(E)$, celui des boules unité $\mathbf{B}(E)$, ou encore le fibré principal de groupe $O(n)$ des bases orthonormées de E.

1.3.2 Fonctorialité et K-théorie relative

Tout ce qui suit s'applique à la K-théorie réelle comme à la K-théorie complexe. On notera $K(X)$ le groupe de K-théorie sans plus de précision.

Soit $f : Y \to X$ une application continue. On peut tirer en arrière par f les fibrés vectoriels de base X de la façon suivante. Si $\pi : E \to X$ est un tel fibré, de rang n, on considère :

$$f^*E = Y \times_X E = \{(y, v) \in Y \times E \ / \ f(y) = \pi(v)\}$$

muni de $f^*\pi : f^*E \to Y$ la première projection. Alors pour tout $y \in Y$, on a l'identification naturelle :

$$(f^*E)_y = (f^*\pi)^{-1}(y) = \{(y, v) \ / \ v \in E_{f(y)}\} \cong E_{f(y)}$$

qui fournit une action de GL_n sur f^*E préservant les fibres. De plus, $f^*\pi$ est bien localement trivial. En effet, pour $y \in Y$, on considère U un voisinage trivialisant de $f(y)$ dans X, et une trivialisation linéaire $\phi : \pi^{-1}(U) \to U \times F$. Alors on obtient encore une trivialisation linéaire en tirant en arrière par f :

$$\begin{array}{rcl} f^*\phi : (f^*\pi)^{-1}(f^{-1}(U)) & \to & f^{-1}(U) \times F \\ (y, v) & \mapsto & \big(y, \mathrm{pr}_2 \circ \phi(v)\big) \end{array}$$

Donc $f^*\pi$ est bien un fibré vectoriel sur Y, et on peut tirer en arrière de manière générale les morphismes de fibrés vectoriels, d'où un foncteur :

$$f^* : \mathbf{VB}(X) \to \mathbf{VB}(Y)$$

qui commute de plus aux sommes directes et aux produits tensoriels. On en déduit donc un morphisme d'anneaux $K(X) \to K(Y)$ encore noté f^*. En particulier, K est un foncteur contravariant des espaces topologiques dans les anneaux commutatifs.

Définition 7 Soit X un espace muni d'un point de base $*$, et $\iota : * \to X$ l'inclusion. On appelle K-théorie réduite de X l'idéal $\widetilde{K}(X)$ de $K(X)$ qui est le noyau de ι^*. Si Y est un sous-espace fermé de X, on note en particulier $K(X, Y) = \widetilde{K}(X/Y)$, où X/Y est l'espace obtenu en contractant Y en un point (et muni de la topologie quotient).

On a alors la suite exacte de $K(X)$-modules :

$$0 \to \widetilde{K}(X) \to K(X) \to K(*) \to 0$$

(la surjectivité résultant de l'existence des fibrés triviaux). En particulier, comme $K(*) = \mathbf{Z}$, la structure de $\widetilde{K}(X)$ ne dépend pas du point de base choisi. De plus, en tant que suite exacte de groupes abéliens, la suite est scindée, puisque le morphisme $K(X) \to K(*)$ a pour section le morphisme $K(*) \to K(X)$ induit par l'application constante $X \to *$. Ainsi, comme groupe abélien, on a :

$$K(X) = K(*) \oplus \widetilde{K}(X) = \mathbf{Z} \oplus \widetilde{K}(X)$$

Pour finir, il nous faut mentionner la propriété essentielle qui fait de la K-théorie une construction intéressante du point de vue topologique.

Théorème 1 *Soit $\pi : E \to X$ un fibré vectoriel, et $f_0, f_1 : Y \to X$ des applications homotopes. Alors si Y est paracompact, les fibrés vectoriels f_0^*E et f_1^*E sont isomorphes.*

Si l'on note $F : Y \times I \to X$ une homotopie de f_0 à f_1, f_0^*E et f_1^*E sont les restrictions à $Y \times \{0\}$ et $Y \times \{1\}$ de F^*E. Le théorème découle donc de la proposition suivante.

Proposition 2 *Soit X un espace paracompact, et E un fibré vectoriel sur $X \times I$. Alors les restrictions de E à $X \times \{0\}$ et $X \times \{1\}$ sont isomorphes.*

Démonstration. On commence par les deux observations suivantes.

1. Si les restrictions E_1 et E_2 d'un fibré $E \to X \times [a, b]$ à $X \times [a, c]$ et $X \times [c, b]$ sont triviales pour un certain $c \in [a, b]$, alors E est trivial. En effet, soit $h_1 : E_1 \to X \times [a, c] \times \mathbf{R}^n$ et $h_2 : E_2 \to X \times [c, b] \times \mathbf{R}^n$ des trivialisations. Quitte à composer h_2 par l'isomorphisme $X \times [c, b] \times \mathbf{R}^n \to X \times [c, b] \times \mathbf{R}^n$ donné sur chaque «tranche» $X \times \{x\} \times \mathbf{R}^n$ par la fonction que donne $h_1 h_2^{-1}$ sur $X \times \{c\} \times \mathbf{R}^n$, on peut supposer que h_1 et h_2 coïncide sur $X \times \{c\} \times \mathbf{R}^n$, et donc se recollent pour fournir une trivialisation $h : E \to X \times [a, b] \times \mathbf{R}^n$.
2. On peut en déduire que pour tout fibré E sur $X \times I$, il existe un recouvrement ouvert (U_i) de X tel que E soit trivial sur chaque $U_i \times I$. En effet, pour chaque point $x \in X$, la trivialité locale fournit des voisinages $U_{x,1}, \ldots, U_{x_k}$ de x et une subdivision $0 = t_0 < \cdots < t_k = 1$ de I telle que E soit trivial sur $U_{x,j} \times [t_{j-1}, t_j]$. La remarque précédente permet d'en déduire que E est trivial sur $U_x \times I$, avec U_x l'intersection des $U_{x,j}$.

À partir de là, raisonnons d'abord sur une base X compacte. On dispose alors d'un recouvrement ouvert fini $(U_1, \ldots, U_m)$ de X telle que E soit trivial au dessus de $U_i \times I$, et il existe une partition de l'unité $(\phi_1, \ldots, \phi_m)$ subordonnée au recouvrement. On note alors $\psi_i = \phi_1 + \cdots + \phi_i$, $0 \leqslant i \leqslant m$. En particulier, $\psi_0 = 0$ et $\psi_1 = 1$. Soit de plus $X_i = \{(x, y) \in X \times I \ / \ y = \psi_i(x)\}$ le graphe de ψ_i, et E_i la restriction de E à X_i.

L'homéomorphisme naturel $X_i \to X_{i-1}$ donné par $(x, \phi_i(x)) \mapsto (x, \phi_{i-1}(x))$ est l'identité en dehors de U_i. Comme E est trivial sur $U_i \times I$, il se prolonge en un isomorphisme de fibrés $h_i : E_i \to E_{i-1}$ qui est l'identité en dehors de $\pi^{-1}(U_i)$. Le composé $h_1 \circ \cdots \circ h_m : E_m \to E_0$ fournit alors bien un isomorphisme entre la restriction de E à $X_m = X \times \{1\}$ et sa restriction à $X_0 = X \times \{0\}$.

Dans le cas d'une base paracompacte quelconque, on peut procéder de même avec un recouvrement (U_i) qui est cette fois dénombrable et localement fini. Il suffit de voir que la «composée infinie» $h_1 \circ h_2 \circ \cdots$ a bien un sens, ce qui est le cas puisqu'au voisinage de tout point $x \in X$, toutes les fonctions h_i sauf un nombre fini sont l'identité. □

On peut noter que le résultat reste valable, avec la même preuve, pour des espaces fibrés qui ne sont pas nécessairement des fibrés vectoriels. Par ailleurs, on en déduit immédiatement l'invariance par homotopie de la K-théorie :

Corollaire 3 *Si $f : Y \to X$ est une équivalence d'homotopie entre espaces paracompacts, le foncteur $f^* : \mathbf{VB}(X) \to \mathbf{VB}(Y)$ est une équivalence de catégories, qui*

induit donc un isomorphisme $f^* : K(X) \to K(Y)$ en K-théorie. En particulier, tout fibré vectoriel sur un espace paracompact contractile est trivial.

1.3.3 Fibré supplémentaire et théorème de Swan

Même si ça ne sera pas directement utile, il est difficile de parler de K-théorie algébrique et de K-théorie topologique sans mentionner les liens profonds qui existent entre les deux. Remarquons tout d'abord que dans le cas d'une base compacte, la K-théorie comme nous l'avons définie est aussi, comme dans le cas les anneaux, l'ensemble des classes d'équivalence stable de fibrés vectoriels, d'après le théorème suivant.

Théorème 4 *Soit X un espace compact, et $\pi : E \to X$ un fibré vectoriel. Il existe un fibré $E^\perp$ tel que $E \oplus E^\perp$ soit trivial.*

Démonstration. Notons qu'il suffit de construire une application $E \to \mathbf{R}^N$ (ou $E \to \mathbf{C}^N$) pour un certain N qui soit linéaire injective sur les fibres. En effet, une telle application fournit un plongement f de E dans le fibré trivial $X \times \mathbf{R}^N$, et en utilisant le produit scalaire sur $\mathbf{R}^N$, on peut construire l'espace :

$$E^\perp = \{(x, v) \in X \times \mathbf{R}^N \ / \ v \in f(E_x)^\perp \subset \mathbf{R}^N\}$$

dont on voit facilement que c'est un sous-fibré vectoriel de $X \times \mathbf{R}^N$. Il est alors évident que $E \oplus E^\perp \cong X \times \mathbf{R}^N$.

L'application $u : E \to \mathbf{R}^N$ recherchée peut s'obtenir par une construction analogue à celle du plongement de Whitney pour une variété compacte. On commence par prendre un recouvrement fini (U_i) de X par m ouverts trivialisants, et une partition de l'unité (ϕ_i) subordonnée. Soit de plus $h_i : \pi^{-1}(U_i) \to U_i \times \mathbf{R}^n$ une trivialisation linéaire au-dessus de U_i. On pose alors, avec l'abus de notation évident :

$$\begin{array}{rcl} u : E & \to & (\mathbf{R}^n)^m \\ x & \mapsto & \big(\phi_i(\pi(x))\,\mathrm{pr}_2(h_i(x))\big)_{1 \leqslant i \leqslant m} \end{array}$$

C'est une application continue, linéaire sur les fibres, et la i-ème composante est un isomorphisme sur les fibres au-dessus de U_i, donc elle vérifie bien les conditions voulues. □

Considérons alors la correspondance qui à un fibré vectoriel $\pi : E \to X$ associe l'espace vectoriel $\Gamma(X, E)$ de ses sections globales continues :

$$\Gamma(X, E) = \{s : X \to E \ / \ \forall x,\ \pi(s(x)) = x\}$$

Si l'on note $C(X)$ l'anneau des fonctions continues sur X (à valeurs dans $\mathbf{R}$ ou $\mathbf{C}$ selon le cas), alors $\Gamma(X, E)$ est de façon évidente un $C(X)$-module. De plus, si l'on choisit $E^\perp$ tel que $E \oplus E^\perp$ soit un fibré trivial de rang N, il vient :

$$\Gamma(X, E) \oplus \Gamma(X, E^\perp) = \Gamma(X, E \oplus E^\perp) = C(X)^N$$

donc quand X est compact, $\Gamma(X,E)$ est un $C(X)$-module projectif de type fini. Bien sûr, si $f : E \to F$ est un morphisme de fibrés, il induit un morphisme de $C(X)$-modules $u_f : \Gamma(X,E) \to \Gamma(X,F)$, $u_f(s) = f \circ s$, et donc $\Gamma(X,-)$ est un foncteur $\mathbf{VB}(X) \to \mathbf{Pr}(C(X))$.

Il est pleinement fidèle. En effet, soit u un morphisme de $C(X)$-modules $\Gamma(X,E) \to \Gamma(X,F)$, et x un point de X. On considère un voisinage trivialisant U de x, et $\phi : X \to [0,1]$ une fonction continue valant 1 en x et nulle hors de U. Alors l'extension par multiplication par ϕ fournit un morphisme de $C(X)$-modules :

$$u_x : C(U) \otimes_{\mathbf{R}} E_x = \Gamma(U, E|_U) \to \Gamma(X,E) \to \Gamma(X,F)$$

et on a alors une application $f : E \to F$ définie par :

$$f(v) = u_x(1 \otimes v)(x) \quad \text{avec } x = \pi(v)$$

La $C(X)$-linéarité de u assure alors que $f(v)$ ne dépend que de v et pas du choix de l'application ϕ. De plus, f est linéaire sur les fibres, donc c'est un morphisme de fibrés vectoriels, et il vérifie en outre $u_f = u$, ce qui démontre bien la pleine fidélité :

$$\mathrm{Hom}_{\mathbf{VB}(X)}(E,F) = \mathrm{Hom}_{C(X)}(\Gamma(X,E), \Gamma(X,F))$$

On peut voir enfin que le foncteur est essentiellement surjectif. En effet, soit $M \in \mathbf{Pr}C(X)$, facteur direct d'un module libre de rang N : $M \oplus M' = C(X)^N = \Gamma(X, X \times \mathbf{R}^N)$. On introduit naturellement l'espace :

$$E = \{(x,v) \in X \times \mathbf{R}^N \ / \ \exists s \in M,\ v = s(x)\}$$

qui est un espace au-dessus de X dont les fibres sont des sous-espaces vectoriels de $\mathbf{R}^N$. De plus, si l'on note E' l'espace correspondant de la même manière à M', on a en tout point $x \in X$, $E_x \oplus E'_x = \mathbf{R}^N$. En particulier, si l'on fixe un point x, il existe des éléments $s_1, \ldots, s_r$ dans M et $s_{r+1}, \ldots, s_N$ dans M' tels que $(s_1(x), \ldots, s_N(x))$ forme une base de $\mathbf{R}^N$. Mais par continuité de $y \mapsto \det(s_1(y), \ldots, s_N(y))$, cela reste vrai au voisinage de x. Il en résulte que E est bien un sous-fibré vectoriel de $X \times \mathbf{R}^N$. Enfin, une section globale de E est en particulier une section globale de $X \times \mathbf{R}^N$, donc s'écrit $s + s'$ avec $s \in M$ et $s' \in M'$. Mais l'on a nécessairement $s'(x) = 0$ pour tout x, et donc $\Gamma(X,E) = M$, ce qui est la surjectivité recherchée.

Finalement, on a obtenu le théorème de Swan :

Théorème 5 *Soit X un espace compact. Le foncteur $\Gamma(X,-)$ est une équivalence de catégories entre les fibrés vectoriels sur X et les modules projectifs de type fini sur $C(X)$. En particulier, $K(X) = K_0C(X)$.*

2 Algèbres et modules de Clifford

2.1 Rappels d'algèbres tensorielles

Nous supposons déjà connue la notion de produit tensoriel. Nous rappelons juste les points principaux, afin de motiver l'introduction des algèbres de Clifford. Soit

donc E un module sur k de dimension n. [2] Nous notons son algèbre tensorielle $T(E) = \sum_{k=0}^{\infty} T^k E = k \oplus E \oplus E \otimes E \oplus \ldots$. C'est une algèbre graduée. Elle est munie de la propriété universelle suivante :

Propriété universelle 1 *Soit f un morphisme de modules de E vers une algèbre F. Alors f s'étend d'une unique manière en un morphisme d'algèbres de $T(E)$ sur F.*

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow & \nearrow & \\ T(E) & & \end{array}$$

En particulier, en prenant $f = Id$, on voit que toute algèbre sur E est un quotient de l'algèbre tensorielle $T(E)$, qui est par là «l'algèbre universelle sur E».

Le problème de cette algèbre est qu'elle est trop «grosse». En particulier, elle n'est pas de dimension finie. On va donc prendre des restrictions de cette algèbre (ou plus exactement des quotients), en essayant de trouver des algèbres qui soient à la fois assez «générales» (c'est à dire qui aient de bonnes propriétés universelles) et si possible de dimensions finies. Une première idée est de considérer l'idéal I engendré par les éléments $x \otimes x$ dans $T(E)$ et d'introduire l'algèbre extérieure $\Lambda(E) = T(E)/I$. Comme I est engendré par des éléments d'ordres 2, I est un idéal gradué : $I = \oplus I_k$ avec $I_k = I \bigcap T^k(E)$. Ainsi, la structure d'algèbre graduée de $T(E)$ induit une structure d'algèbre graduée sur $\Lambda(E) = \sum_{k=0}^{n} \Lambda^k E$, avec $\Lambda^k E = T^k E / I_k$. Il est facile de vérifier que Λ^k est de dimension C_n^k, donc que $\Lambda(E)$ est de dimension 2^n. [3] On a la propriété universelle suivante :

Propriété universelle 2 *Soit f un morphisme de modules de E vers une algèbre F tel que pour tout $x \in E$, $f(x)^2 = 0$. Alors f s'étend d'une unique manière en un morphisme d'algèbres de $\Lambda(E)$ sur F.*

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow & \nearrow & \\ \Lambda(E) & & \end{array}$$

En effet, f s'étend en un morphisme de $T(E)$ sur f, et les propriétés de f montrent que l'on peut passer au quotient par I.

On peut également remarquer qu'on a un isomorphisme entre applications k-alternées de E vers F et les applications linéaires de $\Lambda^k E$ vers F, cela se déduit de l'isomorphisme entre les applications k-linéaires de E vers F et les applications linéaires de $T^k E$ vers F.[4]

[2] Nous supposons pour simplifier que la caractéristique de k est différente du 2. De toute façon dans la suite de ce mémoire, on s'intéresse à des espaces vectoriels sur $\mathbf{R}$ ou $\mathbf{C}$.

[3] En effet, $\Lambda^k E = \underbrace{E \hat{\otimes} E \cdots \hat{\otimes} E}_{k fois}$, l'algèbre extérieure est ainsi l'algèbre universelle gauche sur E.

[4] Ce qui prouve au passage la note 3...

$\Lambda^k E$ est l'ensemble des combinaisons linéaires de k-vecteurs, c'est à dire d'éléments de la forme $x_1 \wedge x_2 \wedge \cdots \wedge x_k$, $x_i \in E$. On peut donner une vision géométrique simple des k-vecteurs. Si on suppose que E est un espace euclidien (ou plus généralement que E est muni d'une forme quadratique), alors on peut étendre le produit scalaire à $\Lambda^k E$ par

$$< x_1 \wedge \cdots \wedge x_k, y_1 \wedge \cdots \wedge y_k >= \begin{vmatrix} x_1 \cdot y_1 & \dots & x_1 \cdot y_k \\ \vdots & & \vdots \\ x_k \cdot y_1 & \dots & x_k \cdot y_k \end{vmatrix}$$

En effet,

$$(y_1, \dots, y_k) \mapsto \begin{vmatrix} x_1 \cdot y_1 & \cdots & x_1 \cdot y_k \\ \vdots & & \vdots \\ x_k \cdot y_1 & \dots & x_k \cdot y_k \end{vmatrix}$$

est une application anti-symétrique.

Ainsi, $< x_1 \wedge \cdots \wedge x_k, x_1 \wedge \cdots \wedge x_k >$ est le volume du parallélépipède de base $(x_1, \dots, x_k)$. Comme $x_1 \wedge \cdots \wedge x_k$ est orienté, on peut ainsi visualiser ce k-vecteur comme un volume orienté.

y

x

FIG. 1 – Le bivecteur $x \wedge y$

Citons pour conclure ces quelques rappels un lemme algébrique caractérisant les k-vecteurs.

Lemme 6 *Condition de décomposabilité*
Soit $z \in \Lambda^k E$. Soit V_z le sous-module de E formé par les $x \in E$ tels que $z \wedge x = 0$. Alors z est un k-vecteur si et seulement si $\dim V_z = k$.

Démonstration. Soit $q = \dim V_z$ et (x_i) une base de V_z. Montrons qu'il existe $v \in \Lambda^{k-q} E$ tel que $z = v \wedge x_1 \wedge \cdots \wedge x_q$.

En effet, complétons (x_i) en une base de E. Comme $z \in \Lambda^k E$, $z = \sum \alpha_{i_1,\dots,i_q} x_{i_1} \wedge \cdots \wedge x_{i_k}$. Par définition, $z \wedge x_i = 0$ pour $1 \leqslant i \leqslant q$. Donc les α_I ne contenant pas l'indice i, $1 \leqslant i \leqslant q$ sont nuls (car quand on multiplie par x_i il ne reste plus que les termes ne contenant originellement pas x_i et ils restent libres). Tous les termes contiennent donc au moins $x_1 \wedge \cdots \wedge x_q$ et $z = v \wedge x_1 \wedge \cdots \wedge x_q$.

Or si $q = p$, alors forcément $v \in k$ et z est bien un k-vecteur. Réciproquement, si $z = x_1 \wedge \cdots \wedge x_k \neq 0$, les (x_i) forment un système libre de V_z, donc $\dim V_z = p$ car on vient de voir que $\dim V_z \leqslant p$ dans tous les cas. □

2.2 Construction de l'algèbre de Clifford

Nous prenons toujours E un k-ev et nous le munissons d'une forme quadratique Q. Un des problèmes majeurs concernant l'algèbre extérieure, c'est que $\|a \wedge b \leqslant |a||b|$ mais il n'y a pas égalité en général (car $x \wedge x = 0$!). Or on aimerait bien une algèbre ayant cette propriété, car la multiplication par un vecteur engendrerait une rotation. On va donc chercher une algèbre $C(E)$ telle que[5]

- $x^2 = Q(x)$ pour tout $x \in E$ (on aura alors trivialement : $2b(x, y) = xy + yx$ si b est la forme bilinéaire associée à Q).
- E engendre $C(E)$

On remarque que ΛE vérifie ces propriétés pour $Q = 0$. Ce qui motive la construction suivante :

Définition 8 Soit $I(Q)$ l'idéal bilatère engendré par les éléments $x \otimes x - Q(x).1$ dans $T(E)$. Alors on définit l'algèbre de Clifford comme étant le quotien de $T(E)$ par $I(Q)$, c'est-à-dire : $C(Q) = T(E)/I(Q)$. [6]

Remarque
- Soit $i_Q : E \to C(Q)$ la composée canonique de $E \to T(E) \to C(Q)$. On voit facilement que i_Q est une injection (car les éléments annulés par le passage au quotient sont de degré au moins deux), ce qui nous permet d'identifier E à $i_Q(E) \subset C(Q)$.
- Par construction même, on a $x \cdot x = Q(x) \cdot 1$, donc $C(E)$ répond bien à la motivation initiale.

Les propriétés de l'algèbre extérieure que nous avons vu en rappel se généralisent trivialement aux algèbres de Clifford. Elles vérifient la propriété universelle suivante :

Propriété universelle 3 *Soit $\Phi : E \to A$ une application linéaire de E dans une algèbre unifère A, qui vérifie $\Phi(x)^2 = Q(x) \cdot 1$ pour tout $x \in E$. Alors il existe un unique morphisme $\tilde{\Phi} : C(Q) \to A$ qui prolonge ϕ.*

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & A \\ \downarrow & \nearrow & \\ C(E) & & \end{array}$$

Démonstration. On procède comme dans les rappels, on étend Φ à $T(E)$ puis on passe au quotient. □

2.3 Premières propriétés, structure élémentaire.

2.3.1 Quelques morphismes

L'idéal $T(E)$ définissant l'algèbre de Clifford n'est pas un idéal gradué pour la $\mathbf{Z}$-graduation usuelle de l'algèbre tensorielle. En revanche, comme $T(E)$ est engendré par

[5] En fait ces propriétés caractérisent l'algèbre de Clifford si on suppose de plus que C(E) n'est pas engendrée par un sous-espace strict de E.

[6] Nous noterons de temps en temps par abus de notation l'algèbre de Clifford $C(E)$ si l'on sous-entend la forme quadratique définie sur E.

une somme d'éléments de degré pair, on peut munir $C(E)$ d'une $\mathbf{Z}/2$-graduation : la graduation induite par $T(E) = T^+E \oplus T^-E$ où $T^+E = \oplus T^{2i}E$ et $T^-E = \oplus T^{2i+1}E$. Ainsi $C(E) = C^+E \oplus C^-E$ où C^+E est l'ensemble des éléments «pairs» de $C(E)$ et C^-E des éléments «impairs». On vérifie sans problème que

$$C^+C^+ \subset C^+$$
$$C^-C^- \subset C^-$$
$$C^+C^- \subset C^-$$
$$C^-C^+ \subset C^-$$

donc on a bien une $\mathbf{Z}_2$-graduation.

Nous allons maintenant nous servir de la propriété universelle 3 pour construire quelques morphismes.

Proposition 7 *On a un foncteur pleinement fidèle de* $\mathbf{Mod}_Q \to \mathbf{Alg}$ *de la catégorie des modules munis d'une forme quadratique dans la catégorie des algèbres par*

- $E \to C(E)$
- $f : (E, Q) \to (F, Q')$ *(où pour tout* $x \in E$, $Q'(f(x)) = Q(x)$*)* $\mapsto \tilde{f} : C(E) \to C(F)$

Démonstration. Il suffit de vérifier que l'on peut bien étendre f. Or f est à valeur dans F, donc dans l'algèbre $C(F)$ via l'injection canonique de F dans $C(F)$, et pour tout $x \in E$, $f(x)^2 = Q'(f(x)) = Q(f(x))$, donc on peut bien étendre f à $C(E)$. □

Définition 9

- En prenant le cas $E = F$ et $f = -Id$ on obtient un automorphisme $\alpha : E \to C(Q)$ tel que $\alpha(x) = -x$. α est appelé l'automorphisme canonique de $C(Q)$.
- Si on considère $C(E)^{\mathbf{opp}}$ l'algèbre opposée de $C(E)$ et f l'identité de E dans $C(E)^{\mathbf{opp}}$, toujours par la propriété universelle on obtient un anti-automorphisme β de $C(Q)$ qui est l'identité sur E. C'est la transposée : $\beta(x_1 \cdot x_2 \cdots x_n) = x_n \cdots x_2 \cdot x_1$ On note $x^t = \beta(x)$
- Ainsi, $x \mapsto \bar{x}$ défini par $x \mapsto \alpha(x^t) = \alpha(x)^t$ est un anti-automorphisme.

2.3.2 Structure élémentaire

Nous allons maintenant étudier la structure de l'algèbre de Clifford. Nous utiliserons le :

Lemme 8 *Soit* $E = E_1 \oplus E_2$ *une décomposition orthogonale de* E *par rapport à* Q. *Alors* $C(Q) \cong C(Q_1)\hat{\otimes}C(Q_2)$.

Remarque Ici $C(Q_1)\hat{\otimes}C(Q_2)$ dénote le produit tensoriel gauche de $C(Q_1)$ et $C(Q_2)$, où si $A = \sum A^\alpha$ et $B = \sum B^\beta$, sont deux algèbres $\mathbf{Z}/2\mathbf{Z}$-graduées, on définit $A\hat{\otimes}B$ comme étant l'espace vectoriel $\sum_{\alpha,\beta} A^\alpha \otimes B^\beta$ muni de la multiplication : $(u \otimes x_i) \cdot (y_j \otimes v) = (-1)^{ij} u y_j \otimes x_i v$ On remarque que $A\hat{\otimes}B$ est aussi graduée par $\sum A^i \otimes B^j (i+j \equiv k \pmod 2)$

Démonstration. On définit $\Psi : E \to C(Q_1)\hat{\otimes}C(Q_2)$ par $\Psi(x) = x_1 \otimes 1 + 1 \otimes x_2$ si $x = x_1 + x_2$ dans $E_1 \oplus E_2$. Alors

$$\begin{aligned}\Psi(x)^2 &= (x_1 \otimes 1 + 1 \otimes x_2)^2 \\ &= (x_1^2 \otimes 1 + 1 \otimes x_2^2) \text{ car l'algèbre est gauche} \\ &= (Q_1(x_1) + Q_2(x_2)) \cdot (1 \otimes 1) \\ &= Q(x) \cdot (1 \otimes 1)\end{aligned}$$

Donc Ψ s'étend en $\tilde{\Psi} : C(Q) \to C(Q_1)\hat{\otimes}C(Q_2)$. Or $C(Q_1)\hat{\otimes}C(Q2)$ est engendrée en tant qu'algèbre par les $x_1 \otimes 1$ et les $1 \otimes x_2$ donc $\tilde{\Psi}$ est surjective. L'injectivité viendra de l'égalité des dimensions, que nous étudions maintenant. □

Théorème 9 *$C(Q)$ est de dimension 2^n, et une base est donnée par $(e_{i_1} \cdots e_{i_p})$ avec $1 \leqslant i_1 < i_2 \ldots < i_m \leqslant n$ et (e_i) une base de E*

Démonstration. Nous procédons par récurrence sur la dimension.

Si $\dim E = 1$, $T(E)$ s'identifie à l'algèbre des polynômes $k[X]$ et $I(Q)$ est l'idéal engendré par $X^2 - a$. Donc $C(Q)$ est de dimension 2.

Si $\dim E > 1$, on écrit $E = E' \oplus E_1$, la somme étant orthogonale et $\dim E_1 = 1$.

Le lemme nous donne une surjection de $C(E)$ sur $C(E')\hat{\otimes}C(E_1)$. Or par hypothèse de récurrence, $C(E')$ est de dimension 2^{n-1} donc $C(E)$ est au moins de dimension 2^n.

Mais il est facile de voir que les $(e_{i_1} \cdots e_{i_p})$ où $1 \leqslant i_1 < i_2 \ldots < i_m \leqslant n$ sont générateurs (car $e_i^2 \in k$), donc $C(E)$ est de dimension 2^n ce qui conclut la récurrence. (ce qui montre au passage que les $(e_{i_1} \cdots e_{i_p})$ forment bien une base.) □

En particulier, on a ainsi (par exemple en prenant une base orthogonale $(e_1, \ldots, e_n)$ de E) :

$$C(Q) = k[t_1]\hat{\otimes}k[t_2]\hat{\otimes}\ldots\hat{\otimes}k[t_n] \tag{1}$$

où les t_i sont des éléments de degré deux sur k : $t_i^2 = Q(e_i)$.

Nous voyons par là l'importance de la structure graduée de $C(Q)$. $C^i(Q) = \{x \in C(Q) \mid \alpha(x) = (-1)^i x\}$. Cette structure graduée est donc fonctionnelle.

Nous concluons cette section par quelques exemples dans le cas où $k = \mathbf{R}$, qui montrent la généralité des algèbres de Clifford.

Exemple 3

- Si E est de dimension 1. $C(E)$ a pour base $(1, u)$ avec $u^2 = Q(e)$.
  - Si $Q(e) = -1$, on retrouve l'ensemble $\mathbf{C}$.
  - Si $Q(e) = 1$ on trouve l'ensemble des nombres complexes hyperboliques.
  - Si $Q(e) = 0$, on trouve l'ensemble des nombres duaux.
- Si $\dim E = 2$ et $Q(x) = -x_1^2 - x_2^2$, $C(Q)$ est engendré par $1, e_1, e_2, e_1e_2$. On a :

$$\begin{gathered}e_1^2 = -1 \\ e_2^2 = -1 \\ (e_1e_2)^2 = -(-1)^2 = -1 \\ e_2 \cdot (e_1e_2) = -e_1e_2^2 = e_1 \\ (e_1e_2) \cdot e_1 = e_2\end{gathered}$$

On obtient l'algèbre des quaternions.

2.4 Cas des algèbres de Clifford réelles

2.4.1 L'algèbre C_k

Nous allons spécialiser ce qui précède au cas des espaces réels de dimension finie. Soit donc $\mathbf{R}^k$ l'espace réel de dimension k et $Q_k(x_1,\ldots,x_k) = -\sum x_i^2$ la forme quadratique négative canonique. Alors on définit l'algèbre C_k comme l'algèbre $C(Q_k)$ et bien sûr on identifie $\mathbf{R}^k$ et son injection dans C_k, ainsi que $\mathbf{R}$ avec $\mathbf{R}\cdot 1 \subset C_k$

Si on note $(e_1,\ldots,e_k)$ la base canonique de R^k, on voit que C_k est engendrée (en tant qu'algèbre) par $(e_1,\ldots,e_k)$ Ainsi, pour $k=0, C_k = \mathbf{R}$

Nous allons maintenant déterminer la structure de C_k.

Proposition 10 *L'algèbre C_k est isomorphe (en tant que $\mathbf{R}$-algèbre) à des produits tensoriels gauches de $\mathbf{C}$:*

$$C_k \cong \mathbf{C}\hat{\otimes}\mathbf{C}\hat{\otimes}\ldots\hat{\otimes}\mathbf{C} \text{ } k \text{ termes} \tag{2}$$

Démonstration. Grâce au lemme 8, il suffit de montrer que C_k est isomorphe à $\mathbf{C}$. Or C_1 est engendré par 1 et e_1. Or par définition, $e_1 \otimes e_1 = -1$. D'où $C_1 \cong \mathbf{R}[X]/(X^2-1) \cong \mathbf{C}$. □

Corollaire 11 *C_k est l'algèbre universelle unifère engendrée sur $\mathbf{R}$ par k symboles $e_1,\ldots,e_k$ vérifiant les relations :*

$$e_j^2 = -1, \qquad e_ie_j + e_je_i = 0 \tag{3}$$

Démonstration. $e_ie_j + e_je_i = 0$ vient de ce que les e_i sont dans $C^1(Q_k)$ et que l'algèbre est gauche. Quand à $e_j^2 = -1$ cela vient immédiatement de la structure de C_1 et de la proposition 10. □

2.4.2 Détermination des algèbres C_k

Le problème, pour déterminer les C_k, c'est que ce sont des produits tensoriels gauches de C. Nous allons nous ramener au calcul de vrais produits tensoriels en introduisant C'_k, l'algèbre de Clifford sur $\mathbf{R}^k$ de $Q_k(x_1,\ldots,x_k) = \sum x_i^2$. C'est l'algèbre universelle unifère engendrée sur $\mathbf{R}$par les k symboles $e'_1,\ldots,e'_k$ vérifiant les relations :

$$e_j'^2 = -1, \qquad e'_ie'_j + e'_je'_i = 0 \tag{4}$$

(Il suffit d'adapter le corollaire 11).

Pour cela, on utilisera la

Proposition 12

$$C_k \otimes_{\mathbf{R}} C'_2 \cong C'_{k+2}$$
$$C'_k \otimes_{\mathbf{R}} C_2 \cong C_{k+2}$$

Rappel Il peut être utile de rappeler que si A et B sont deux algèbres, alors $A \otimes B$ peut être munie d'une structure d'algèbre par $a_1 \otimes b_1 \cdot a_2 \otimes b_2 = (a_1 \cdot a_2) \otimes (b_1 \cdot b_2)$

Dans le cas d'algèbres de dimensions finies, $C = A \otimes B$ est caractérisée par les propriétés suivantes[7]

- $ab = ba$ pour tout $a \in A$ et $b \in B$
- C est engendrée par A et B
- $\dim C = (\dim A)(\dim B)$

Démonstration. Pour distinguer $\mathbf{R}^k \subset C'_k$ de $\mathbf{R}^k \subset C_k$, on note le premier $\mathbf{R}'$.

Soit $\Psi : \mathbf{R}'^{k+2} \to C_k \otimes C'_2$ défini par

$$\Psi(e'_i) = \begin{cases} e_{i-2} \otimes e'_1 e'_2 & 2 < i \leqslant k \\ 1 \otimes e'_i & 1 \leqslant i \leqslant 2 \end{cases}$$

Un calcul facile montre que Ψ satisfait la propriété universelle des algèbres de Clifford et s'étend donc en un morphisme de $C'_{k+2} \to C_k \otimes C'_2$ Or Ψ est clairement surjective (l'image de la base contient des générateurs de $C_k \otimes C'_2$, donc c'est un automorphisme, par égalité des dimensions). La première assertion se démontrer de même, en considérant :

$$\Psi'(e_i) = \begin{cases} e'_{i-2} \otimes e_1 e_2 & 2 < i \leqslant k \\ 1 \otimes e_i & 1 \leqslant i \leqslant 2 \end{cases}$$

□

Nous avons maintenant tous les outils qu'il faut, en utilisant les isomorphismes élémentaires suivants :

$$\begin{cases} \mathbf{F}(n) & \cong & \mathbf{R}(n) \otimes_{\mathbf{R}} \mathbf{F} \\ \mathbf{R}(n) \otimes_{\mathbf{R}} \mathbf{R}(m) & \cong & \mathbf{R}(nm) \\ \mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} & \cong & \mathbf{C} \oplus \mathbf{C} \\ \mathbf{H} \otimes_{\mathbf{R}} \mathbf{C} & \cong & \mathbf{C}(2) \\ \mathbf{H} \otimes_{\mathbf{R}} \mathbf{H} & \cong & \mathbf{R}(4) \end{cases} \tag{5}$$

où $\mathbf{F}$désigne un des trois corps $\mathbf{R}$, $\mathbf{C}$ou $\mathbf{H}$et $\mathbf{F}(n)$ représente l'anneau des matrices $n \times n$ sur $\mathbf{F}$.

Enfin, les relations entre les e_i et les e'_i nous donnent :

$$\begin{array}{ll} C_1 \cong \mathbf{C} & C'_1 \cong \mathbf{R} \oplus \mathbf{R} \\ C_2 \cong \mathbf{H} & C'_2 \cong \mathbf{R}(2) \end{array}$$

Démonstration. On a déjà vu dans l'exemple 3 que $C_1 \cong \mathbf{C}$, que $C'_1 \cong \mathbf{R} \oplus \mathbf{R}$ et $C_2 \cong \mathbf{H}$ (en effet, $\mathbf{R} \oplus \mathbf{R}$, qui est vue comme algèbre par multiplication composante par composante, peut-être vue comme l'ensemble des éléments de la forme : $a + jb$, avec $j^2 = 1, j \neq 1$, en prenant par exemple $1 = (1, 1)$ et $j = (1, -1)$. C'est donc bien l'algèbre des nombres complexes hyperboliques).

Pour C'_2, on considère le morphisme :

$$e_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

k	C_k	C'_k	$C_k \otimes_{\mathbf{R}} \mathbf{C} = C'_k \otimes_{\mathbf{R}} \mathbf{C}$
1	$\mathbf{C}$	$\mathbf{R} \oplus \mathbf{R}$	$\mathbf{C} \oplus \mathbf{C}$
2	$\mathbf{H}$	$\mathbf{R}(2)$	$\mathbf{C}(2)$
3	$\mathbf{H} \oplus \mathbf{H}$	$\mathbf{C}(2)$	$\mathbf{C}(2) \oplus \mathbf{C}(2)$
4	$\mathbf{H}(2)$	$\mathbf{H}(2)$	$\mathbf{C}(4)$
5	$\mathbf{C}(4)$	$\mathbf{H}(2) \oplus \mathbf{H}(2)$	$\mathbf{C}(4) \oplus \mathbf{C}(4)$
6	$\mathbf{R}(8)$	$\mathbf{H}(4)$	$\mathbf{C}(8)$
7	$\mathbf{R}(8) \oplus \mathbf{R}(8)$	$\mathbf{C}(8)$	$\mathbf{C}(8) \oplus \mathbf{C}(8)$
8	$\mathbf{R}(16)$	$\mathbf{R}(16)$	$\mathbf{C}(16)$

TAB. 1 – Représentation des algèbres de Clifford euclidiennes et anti-euclidiennes.

On vérifie sans difficulté que c'est un isomorphisme. □

En appliquant 12 et 5 on obtient ainsi la table 2.4.2.

Et on a fini. En effet, la proposition 12, on a $C_4 \cong C'_4$, $C_{k+4} \cong C_k \otimes C_4$, $C_{k+8} \cong C_4 \otimes C_8$. Or $C_8 = C'_8 = \mathbf{R}(16)$ Ainsi, on a en utilisant $\mathbf{R}(n) \otimes_{\mathbf{R}} \mathbf{R}(m) \cong \mathbf{R}(nm)$, on a $C_{8k} \cong \mathbf{R}(16^k)$. Plus généralement, si on augmente la dimension de 8, la structure n'est pas changée, mais les dimensions sont multipliées par 16. (car $\mathbf{F}(n) \cong R(n) \otimes_{\mathbf{R}} F$). On remarque que l'évolution du complexifié de C_k, qui n'est autre que l'algèbre de Clifford de Q_k sur $\mathbf{C}$, est bien plus simple : sa période est d'ordre 2.

2.4.3 Cas général

Encore une fois, seuls les résultats concernant la détermination de l'algèbre C_k nous seront utile pour la suite de ce mémoire. Toutefois, par souci de complétude, nous donnons ici des descriptions pour toute algèbre de Clifford associée à un espace vectoriel réel. Comme les formes quadratiques réelles sont déterminées par leur indice de Sylvester (p, q), nous allons étudier la structure des algèbres de Clifford associées $C_{p,q}$ (en terme d'algèbres de Matrices). Nous avons déjà étudié dans la section précédente le cas des formes définies positives et définies négatives.

Il faut cependant remarquer que nous perdons des informations en représentant. En effet, dans les algèbres de Clifford, il y a un sous-espace caractéristique, à savoir E. Dans les représentations que nous avons déjà vue, il n'y a pas de telles caractérisations «immédiates» de E.

Commençons par remarquer que l'on a aussi déjà trouvé la structure des formes quadratiques complexes. Cela vient du lemme suivant :

Lemme 13 *Soit K' un sur-corps commutatif du corps K. Soit Q une forme quadratique sur E, un K-espace vectoriel. Soit Q' le forme quadratique étendue à l'amplifié de E par K' : $E' = E \otimes K'$. Alors $C'(E) = C(E) \otimes K' \cong C(E')$.*
(«L'algèbre de Clifford de l'amplifié est l'amplifié de l'algèbre de Clifford.»)

[7] En effet, la propriété1 donne un morphisme Ψ de $A \otimes B$ dans C, qui est surjectif par 1 et injectif par 1.

Démonstration. Soit u l'application K'-linéaire qui envoie $e_i \otimes 1 \in E' \mapsto e_i \otimes 1 \in C'(E)$. (Si l'on note i l'injection canonique de $E \to C(E)$, u n'est autre que $i \otimes 1$).

On calcule

$$(u(x \otimes a))^2 = (x \otimes a)^2 = (x \cdot x) \otimes a^2 = a^2 Q(x) = Q'(x \otimes a)$$

or comme les éléments de E' s'écrivent comme sommes finies d'éléments de cette forme, on a donc : $\forall z \in E', u(z)^2 = Q'(z)$.

D'où par propriété universelle des algèbres de Clifford on obtient un morphisme de $C(E')$ dans $C'(E)$. C'est un isomorphisme car les bases s'appliquent l'une sur l'autre. □

Soit donc Q_1 une forme quadratique sur $\mathbf{C}^n$. Soit Q_2 la forme quadratique définie négative canonique sur $\mathbf{R}^n$, et Q_2' son extension au complexifié $R^n \otimes_{\mathbf{R}} \mathbf{C} \cong \mathbf{C}^n$. Par le lemme 13, on sait que $C(Q_2') \cong C(Q_2) \otimes_{\mathbf{R}} \mathbf{C}$. Or comme $\mathbf{C}$ est algébriquement clos, toutes les formes quadratiques sont équivalentes, et par fonctorialité (proposition 7), $C(Q_2') \cong C(Q_1)$.

D'où

$$C(Q_1) \cong C(Q_2) \otimes_{\mathbf{R}} \mathbf{C} = \begin{cases} \mathbf{C}(n) & \text{si } n \text{ est pair} \\ \mathbf{C}(n-1) \oplus \mathbf{C}(n-1) & \text{sinon} \end{cases}$$

Passons maintenant à la structure des $C_{p,q}$. Nous nous servirons de celles que nous connaissons déjà grâce aux isomorphismes suivants :

Proposition 14

1. $Cl_{p+1,q+1} \cong \mathrm{Mat}(2, C_{p,q})$
2. $Cl_{p,q} \cong C_{q+1,p-1}$ *(symétrie)*

Démonstration. Commençons par l'isomorphisme 1. Soit $e_1, \ldots, e_n$ une base orthogonale de $\mathbf{R}^{p+q}$. Alors les matrices

$$\begin{pmatrix} e_i & 0 \\ 0 & -e_i \end{pmatrix} \quad \text{pour } i = 1, \ldots, n, \quad e_+ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad e_- = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

anticommutent donc génèrent l'algèbre de Clifford $C_{p+1,q+1}$ (car de plus $e_+^2 = 1$ et $e_-^2 = -1$). $C_{p+1,q+1}$ est ainsi isomorphe à l'algèbre de matrices 2×2 à éléments dans $C_{p,q}$ donc à $\mathrm{Mat}(2, C_{p,q})$.

Remarquons que $x \in C_{p,q}$ est envoyé sur

$$\begin{pmatrix} x & 0 \\ 0 & \alpha(x) \end{pmatrix}$$

On peut aussi représenter x par

$$x^+ + x^- \cdot e_+ e_- = \begin{pmatrix} x & 0 \\ 0 & \alpha(x) \end{pmatrix}$$

où $x = x^+ + x^-$ est la décomposition de x en éléments pairs et en éléments impairs. On vérifie que $e'_i = e_i e_+ e_-$ génèrent une copie de $Cl_{p,q}$, or ils commutent avec e_+ et e_- (qui engendrent $C_{1,1}$), et les e'_i, e_+ et e_- génèrent $C_{p+1,q+1}$. D'où

$$C_{p+1,q+1} \cong C_{p,q} \otimes C_{1,1} \cong C_{p,q} \otimes \mathrm{Mat}(2, \mathbf{R})$$

ce qui donne une autre preuve du résultat.

Pour le second isomorphisme, soit toujours $e_1, \ldots, e_n$ une base orthogonale de $\mathbf{R}^{p+q}$. Soit $e'_1 = e_1$ et $e'_i = e_i e_1$ si $i > 1$. Les e'_i anticommutent et $e'^2_1 = e^2_1$, $e'^2_i = -e^2_i$ donc ils génèrent $C_{q+1,p-1}$. Comme ils ont même dimension, on conclut que

$$C_{p,q} \cong C_{q+1,p-1}$$

□

Cela nous permet grâce au tableau 2.4.2 de caractériser tous les $C_{p,q}$, $p + q \leqslant 7$. (cf tableau 2, où on a noté pour simplifier ${}^2\mathbf{F} = \mathbf{F} \oplus \mathbf{F}$). Nous retrouvons la périodicité de 8, en fait on a même une double périodicité : sur les diagonales, et sur les horizontales. Nous retrouverons cette périodicité lors de l'étude du K_0 de certains fibrés vectoriels. Ces périodicités découlent du

Théorème 15
- $C_{p,q} \cong C_{p-4,q+4}$ *pour* $p \geqslant 4$ *(Cartan, 1908)*
- $C_{p+8,q} \cong C_{p,q+8} \cong \mathrm{Mat}(16 C_{p,q})$

Démonstration. Soit $e_1, \ldots, e_n$ une base orthogonale de R^{p+q}. Formons

$$e'_i = e_i e_1 e_2 e_3 e_4 \qquad \text{pour } i = 1, 2, 3, 4$$
$$e'_i = e_i \qquad \text{pour } i > 4$$

alors les e'_i génèrent $C_{p-4,q+4}$ ce qui montre que $C_{p,q} \cong C_{p-4,q+4}$.

Pour la deuxième assertion, soit $e_1, \ldots, e_{n+8}$ une base orthogonale de $C_{p,q+8}$. Posons

$$e'_i = e_i e_{n+1} \cdots e_{n+9} \quad \text{pour } 1 \leqslant i \leqslant n$$

Alors les e'_i génèrent une sous-algèbre isomorphe à $C_{p,q}$ tandis que $e_{n+1}, \ldots, e_{n+8}$ engendrent $C_{0,8} \cong \mathrm{Mat}(16, \mathbf{R})$ (cf le tableau 2.4.2). Or ces deux algèbres commutent et engendrent $C_{p,q+8}$, d'où

$$C_{p,q+8} \cong C_{p,q} \otimes \mathrm{Mat}(16, \mathbf{R}) \cong \mathrm{Mat}(16, C_{p,q})$$

L'autre assertion se démontre de même, par symétrie. □

2.5 Algèbres de Clifford sur un corps quelconque.

Pour le lecteur intéressé, nous citons ici quelques résultats concernant les algèbres de Clifford sur un corps quelconque (en particulier sur des corps algébriquement clos). Comme cette section a juste un intérêt culturel, nous ne prouverons généralement pas les résultats obtenus. Elles peuvent se trouver dans [Cru74] par exemple.

$p+q$ \ $p-q$	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
0								$\mathbf{R}$							
1							$\mathbf{C}$		$^2\mathbf{R}$						
2						$\mathbf{H}$		$\mathbf{R}(2)$		$\mathbf{R}(2)$					
3					$^2\mathbf{H}$		$\mathbf{C}(2)$		$^2\mathbf{R}(2)$		$\mathbf{C}(2)$				
4				$\mathbf{H}(2)$		$\mathbf{H}(2)$		$\mathbf{R}(4)$		$\mathbf{R}(4)$		$\mathbf{H}(2)$			
5			$\mathbf{C}(4)$		$^2\mathbf{H}(2)$		$\mathbf{C}(4)$		$^2\mathbf{R}(4)$		$\mathbf{C}(4)$		$^2\mathbf{H}(2)$		
6		$\mathbf{R}(8)$		$\mathbf{H}(4)$		$\mathbf{H}(4)$		$\mathbf{R}(8)$		$\mathbf{R}(8)$		$\mathbf{H}(4)$		$\mathbf{H}(4)$	
7	$^2\mathbf{R}(8)$		$\mathbf{C}(8)$		$^2\mathbf{H}(4)$		$\mathbf{C}(8)$		$^2\mathbf{R}(8)$		$\mathbf{C}(8)$		$^2\mathbf{H}(4)$		$\mathbf{C}(8)$

TAB. 2 – Représentation des algèbres de Clifford réelles.

Soit donc E un k-ev de dimension n, Q une forme quadratique sur E. Comme cela peut se remarquer lorsqu'on étudie les algèbres de Clifford réelles ou complexes, on obtient des résultats très différents selon que n est pair ou non.

En fait, on a le résultat suivant, qui montre qu'il suffit d'étudier l'un de ces cas :

Proposition 16 *Si $n = 2r+1$, Q forme quadratique sur E non dégénérée, alors*
- *$C^+(Q) \cong C(Q_1)$, Q_1 étant une forme quadratique sur un espace de dimension $2r$.*
- *$C(Q) \cong C^+(Q_2)$, Q_2 étant une forme quadratique sur un espace de dimension $2r+2$.*

et Q_1, Q_2 sont non dégénérées.

Démonstration. Soit $x_0 \in E$ non isotrope et $F = (x_0)^\perp$. Sur F, nous considérons la forme quadratique Q_1 :

$$Q_1(y) = -Q(x_0)Q(y), y \in F$$

Q_1 est non dégénérée, en effet, si $u = x + y \in E$, avec $x \in kx_0$, $y \in F$:

$$\begin{aligned} Q(u) &= Q(x+y) \\ &= Q(x) + Q(y) \\ &= (a_0)^2 Q(x_0) + Q(y) \end{aligned}$$

Donc si Q_1 était dégénérée, on aurait une décomposition de Q en moins de n carrés. C'est impossible.

Enfin, si $y \in F$,

$$(x_0 y)^2 = -y^2 x_0^2 = -Q(x_0)Q(y) = Q_1(y)$$

. Donc $y \mapsto x_0 y$ se prolonge en un morphisme de $C(Q_1)$ dans $C^+(Q)$. Par égalité des dimensions, c'est un isomorphisme (l'injectivité vient de ce que si $y \in \Lambda(F) \neq 0$, $x_0 y \neq 0$ car $x_0 \notin F$. Comme x_0 est non isotrope, $x_0 y \neq 0$ dans $C(E)$ non plus).

Pour construire Q_2, il suffit de considérer $F = E \oplus x_0 k$, et on définit Q_2 par $Q_2(x_0) = \alpha \neq 0$, $-\alpha Q_2(y) = Q(y)$ pour $y \in E$, et en prenant $x_0 \perp E$. La même démonstration que précédemment appliquée à $C(Q_2)$ montre que $C^+(Q_2) \cong C(Q)$. □

Théorème 17 *Si $n = 2r$ est pair, Q non dégénérée, alors $C(Q)$ est une algèbre centrale simple ($Z = k \cdot 1$).*

Si de plus Q est neutre, alors $C(Q)$ est isomorphe à l'algèbre des endomorphismes d'un espace vectoriel S de dimension 2^r sur k : $C(Q) \cong \operatorname{End} S$.

Dans ce cas, et si $r > 0$, $C^+(Q)$ est composée directe de deux idéaux isomorphes à l'algèbre des endomorphismes d'un espace vectoriel de dimension 2^{r-1} sur k.

Si $n = 2r+1$ est impair, Q non dégénérée, alors $C(Q)$ a pour centre une extension quadratique de k ($Z = k.1 + k \cdot e_1 \cdots e_n$). Soit D le discriminant de Q. Alors

- *Si $(-1)^{\frac{n(n-1)}{2}} D$ n'est pas un carré, le centre est un corps et $C(Q)$ est simple.*
- *Si $(-1)^{\frac{n(n-1)}{2}} D$ est pas un carré, le centre s'écrit $Z = ku \oplus kv$, avec $uv = 0$, $u^2 = u$, $v^2 = v$. De plus, $C(Q) = C(Q)u \oplus C(Q)v$, et $C(Q)u$, $C(Q)v$ sont les seuls idéaux non triviaux de $C(Q)$.*

Enfin, si Q est d'indice maximum, alors $C(Q)$ est composée directe de deux idéaux isomorphes à l'algèbre des endomorphismes d'un espace vectoriel de dimension 2^r sur k, $C^+(Q)$ est isomorphe à l'algèbre des endomorphismes d'un espace vectoriel de dimension 2^r sur k

Rappel L'indice d'une forme quadratique est la dimension d'un sous-espace vectoriel complètement isotrope maximal (La théorème de Witt montre que l'indice ne dépend pas du sous-espace isotrope maximal choisi). Q est neutre si elle est non dégénérée et d'indice maximum (dans ce cas, si n est pair, E est hyperbolique). C'est toujours le cas si Q est non dégénérée et que k est algébriquement clos.

Ainsi, le théorème précédent montre que les représentations pour les algèbres de Clifford sur des corps algébriquement clos sont les mêmes que les représentations d'algèbres de Clifford complexes.

2.6 Spineurs

2.6.1 Motivations

On sait que le groupe spécial orthogonal $\mathrm{SO}(2, \mathbf{R})$ est l'ensemble des matrices de la forme

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad a^2 + b^2 = 1$$

Il est donc isomorphe au groupe unité $\mathbf{U}$ de $\mathbf{C}$ (on le voit en prenant par exemple la représentation classique de $\mathbf{C}$ dans $\mathbf{R}^2$, ou encore en faisant agir $\mathbf{U}$ sur $\mathbf{C} \cong \mathbf{R}^2$ par $u \cdot x \mapsto ux$).

Ceci nous donne une paramétrisation de $\mathrm{SO}(2, \mathbf{R})$. Il est classique que l'on peut également paramétrer $\mathrm{SO}(3, R)$ et $\mathrm{SO}(4, \mathbf{R})$ grâce aux quaternions.

Plus précisément si on note G le groupe unité de $\mathbf{H}$ (c'est à dire l'ensemble des $\{x \in \mathbf{H} \mid N(x) = x\bar{x} = 1\}$, alors l'action par conjugaison de G sur les quaternions purs $\mathrm{Im}(\mathbf{H}) \cong \mathbf{R}^3$ induit une suite exacte

$$1 \to \{1, -1\} \to G \overset{u \cdot x = uxu^{-1}}{\to} \mathrm{SO}(3, \mathbf{R})$$

(on vérifie que cette suite est non scindée, donc on ne peut pas paramétrer fidèlement $\mathrm{SO}(3,\mathbf{R})$ à l'aide d'un sous-groupe de G).

On peut également paramétrer $\mathrm{SO}(4,\mathbf{R})$ par $(u_1,u_2)\cdot x \mapsto u_1 x u_2^{-1}$. Cela induit également une suite exacte

$$1 \to \{(1,1),(-1,-1)\} \to G\times G \to \mathrm{SO}(4,\mathbf{R})$$

Enfin, on peut noter que G permet de paramétrer fidèlement $\mathrm{SU}(2,\mathbf{C})$ via $u\cdot x \mapsto ux$. (on peut trouver ces résultats dans [Lou97]).

On cherche à étendre ceci à des espaces de dimensions supérieures (et également à d'autres formes quadratiques que la forme euclidienne canonique).

Une des idées qui vient, est de multiplier par des k-vecteurs. Mais on a déjà vu que ça ne marchait pas, car l'algèbre extérieure ne conserve pas la norme. Par contre, si on considère $x = x_1\cdots x_k$ un «k-vecteur» de $C(Q)$, on peut définir sa norme par : $N(x) = Q(x_1)\cdots Q(x_k) = xx^t$. Si $N(x)=1$, et $y\in E$, alors $N(xy)=N(y)$. Cependant, xy n'a aucune raison d'être dans E. Par contre ce sera le cas pour xyx^{-1}. Pour pouvoir paramétrer tout le groupe orthogonal, il nous faudra étendre ceci à d'autres éléments de $C(Q)$ et utiliser une norme «tordue».

2.6.2 Les groupes $\mathrm{Pin}\,Q$ et $\mathrm{Spin}\,Q$

Précisons donc les idées de la partie précédente. Soit $\mathbf{K}=\mathbf{R}$ ou $\mathbf{C}$ (en fait, on peut étendre ce qui va suivre à tout corps commutatif de caractéristique 0, modulo les résultats admis dans la section précédente). Q une forme quadratique non dégénérée sur E, un $\mathbf{K}$-ev de dimension n.

On note $C^*(Q)$ le groupe des éléments inversibles de $C(Q)$.

Définition 10 Le groupe de Clifford (tordu) $\mathbf{\Gamma}$ est le sous-groupe des éléments $x\in C^*(Q)$ qui vérifient pour tout $y\in E$: $\alpha(x)yx^{-1}\in E$.

Enfin, on pose $\mathbf{\Gamma}^+ = \mathbf{\Gamma}\bigcap C^+(Q)$

Comme α est un automorphisme, $\mathbf{\Gamma}$ est clairement un sous-groupe. De plus, comme α et la transposition β laissent E stable, α et β induisent un automorphisme et un anti-automorphisme sur $\mathbf{\Gamma}$ (et donc la conjugaison, $x\to\bar{x}$ induit également un anti-automorphisme).

La définition de $\mathbf{\Gamma}$ nous donne immédiatement une représentation $\rho:\mathbf{\Gamma}\to\mathrm{Aut}(E)$ par $\rho(x)\cdot y = \alpha(x)yx^{-1}$. Cette représentation est presque fidèle.

Proposition 18 *Le noyau de ρ est $\mathbf{K}^*$.*

Démonstration. Si $x\in\mathrm{Ker}\,\rho$, on a donc

$$\alpha(x)y = yx \quad \text{pour tout } y\in E \tag{6}$$

Décomposons x en $x=x^+ + x^-$. Alors (6) devient

$$x^+y = yx^+ \tag{7}$$
$$x^-y = yx^- \tag{8}$$

Soit $(e_1, \ldots, e_n)$ une base orthonormale de E et $\alpha_k = Q(e_k)$. Écrivons $x^+ = a + e_1 b$, où e_1 n'apparaît ni dans a, ni dans b. Donc $a \in C^+(Q)$ et $b \in C^-(Q)$. En spécifiant $y = e_1$ dans (7), on obtient :

$$ae_1 - \alpha_1 b = ae_1 + \alpha_1 b$$

Comme Q est non dégénérée, $\alpha_1 \neq 0$ donc $b = 0$. Ce qui montre que e_1 n'apparaît pas dans l'écriture de x^+. En appliquant ceci aux autres éléments de la base, on trouve que $x^+ \in \mathbf{K}$.

On procède de même pour x^-, si $x^- = a + e_1 b$, alors (8) appliqué à $y = e_1$ nous donne

$$ae_1 + e_1 b e_1 = -(e_1 a + e_1^2 b)$$
$$ae_1 + \alpha_1 b = ae_1 - \alpha_1 b$$

D'où comme précédemment, $x^- \in \mathbf{K}$, ce qui n'est possible que si $x^- = 0$ car $x^- \in C^-(Q)$. □

Ceci va nous permettre de définir une norme sur le groupe de Clifford.

Définition 11 Nous définissons $N : C(Q) \to C(Q)$ par [8]

$$N(x) = x\bar{x}$$

Si $x \in E$, $N(x) = -Q(x) = -\|x\|^2$.

Proposition 19 *N est un morphisme de $\mathbf{\Gamma}$ dans $\mathbf{K}^*$, stable par α.*

Démonstration. Soit $x \in \mathbf{\Gamma}$. Pour montrer que $N(x) \in \mathbf{K}^*$, il suffit de montrer que $N(x) \in \operatorname{Ker}\rho$. Or

$$\alpha(x) y x^{-1} = y', \quad y' = \rho(x) y \in E$$

D'où, puisque $y^t = y$,

$$(x^t)^{-1} y \alpha(x)^t = \alpha(x) y x^{-1}$$
$$y\alpha(x^t) x = x^t \alpha(x) y$$

Donc $\alpha(x^t)x \in \operatorname{Ker}\rho \subset \mathbf{K}^*$, ce qui amène (en transposant) $N(x^t) = x^t\alpha(x) \in \mathbf{K}^*$. Comme β est un anti-automorphisme de $\mathbf{\Gamma}$, on a bien $N(\mathbf{\Gamma}) \subset \mathbf{K}^*$.

$N(xy) = xy\bar{y}\bar{x} = xN(y)\bar{x} = N(x)N(y)$, donc c'est bien un morphisme.

Enfin, $N(\alpha(x)) = \alpha(x)x^t = \alpha(N(x)) = N(x)$. □

Proposition 20 *$\rho(\mathbf{\Gamma})$ est contenu dans le groupe des isométries de (E, Q).*

Démonstration. En utilisant la proposition 19 et le fait que $E\backslash\{0\} \subset \mathbf{\Gamma}$, on obtient :

$$N(p(x) \cdot y) = N(\alpha(x) y x^{-1}) = N(\alpha(x))N(y)N(x^{-1}) = N(y)$$

□

[8] On remarque que pour $C_1 = \mathbf{C}$ et $C_2 = \mathbf{H}$, on retrouve la norme habituelle.

En fait, ρ est une surjection de $\mathbf{\Gamma}$ sur $\mathrm{O}(Q)$ (cf le théorème suivant). Cependant, ce groupe est trop gros, (en particulier, il n'est pas simplement connexe, on a donc aucune chance de trouver le revêtement universel de $\mathrm{O}(Q)$ de cette manière).

On va essayer de restreindre l'espace de départ. On a déjà vu que $\rho(x) = \rho(y) \Leftrightarrow x \in Ky$. On va donc essayer de se restreindre aux éléments de norme 1. Cependant, si $\mathbf{K} = \mathbf{R}$, si $N(x) < 0$, on ne peut pas trouver de tel élément dans $\mathbf{K}x$. Ceci nous conduit en fait à restreindre ρ aux éléments de norme ± 1 (plus généralement, pour un corps $\mathbf{K}$ quelconque, si on note A un système de représentant de $\mathbf{K}/\mathbf{K}^2$, on se restreindra aux éléments de normes dans A.)

Nous supposons dans la suite que $\mathbf{K} = \mathbf{R}$. Nous traiterons ensuite le cas $\mathbf{K} = \mathbf{C}$.

Théorème 21 *Soit* $\mathrm{Pin}\, Q = N^{-1}(\pm 1)$. *On a une suite exacte*

$$1 \to \mathbf{Z}_2 \to \mathrm{Pin}\, Q \xrightarrow{\rho} \mathrm{O}(q) \to 1$$

(on note $\mathbf{Z}_2$ le groupe $\mathbf{Z}/2\mathbf{Z}$)

Démonstration. Montrons d'abord que ρ est surjective. Soit $a \in E \bigcap C^*(Q)$ ($E \bigcap C^*(Q)$ est l'ensemble des vecteurs non isotropes de E). On calcule

$$\rho(a) \cdot x = -axa^{-1} = \frac{axa}{Q(a)} = \frac{a}{Q(a)}(2B(x,a) - ax) \tag{9}$$

$$= -x + \frac{2B(x,a)}{Q(a)} \tag{10}$$

ce qui prouve que $a \in \mathbf{\Gamma}$, et de plus que la symétrie par rapport à l'hyperplan $a^\perp \in \rho(\mathbf{\Gamma})$. Appliquant ceci à $\frac{a}{\sqrt{\pm N(a)}}$ (suivant que $N(a) > 0$ ou non), on trouve que les réflexions orthogonales sont dans $\rho(\mathrm{Pin}\, Q)$. Comme ces réflexions engendrent $\mathrm{O}(q)$ (théorème de Cartan-Dieudonné), on a donc $\rho(\mathrm{Pin}\, Q) = \mathrm{O}(q)$.

Enfin, $\mathrm{Ker}\, \rho \bigcap \mathrm{Pin}\, Q = \{\lambda \in \mathbf{K}^* \mid N(\lambda) = \pm 1\} = \left\{\lambda \in \mathbf{R}^* \mid \lambda^2 = \pm 1\right\} = \pm 1$.

D'où le résultat. □

Corollaire 22 $\mathbf{\Gamma} = \{\lambda x_1 \cdots x_k\}$, *avec* $\lambda \in \mathbf{R}^*$ *et les* x_i *des vecteurs isotropes de* E. *(et* $\mathbf{\Gamma}^+$ *est obtenu en prenant* k *pair).*

Ainsi dans C_n, on peut définir $\mathrm{Pin}\, Q$ comme étant le noyau de $N : \mathbf{\Gamma} \to \mathbf{R}^*$.

Démonstration. Soit $x \in \mathbf{\Gamma}$. Écrivons $p(x) = u_1 \cdots u_k$, où les u_i sont des réflexions orthogonales par rapport à $x_i^\perp$. Alors $p(x) = p(x_1 \cdots x_k)$, d'où $x_1 \cdots x_k x^{-1} \in \mathrm{Ker}\, p = \mathbf{R}^*$. Ce qui prouve l'assertion. □

On a aussi un revêtement de $\mathrm{SO}(q)$, il est donné par le groupe des spineurs.

Définition 12 On pose $\mathrm{Spin}(Q) = \mathrm{Pin}^+(Q) = \mathrm{Pin}(Q) \bigcap \mathbf{C}^+(Q)$. C'est le groupe des spineurs de Q.[9]

Proposition 23

[9] On a aussi une autre notion, qui est celle de représentation spinorielle. Il s'agit d'une représentation irréductible de $C(Q)$ dans un espace S. S est alors appelé espace des spineurs, et par abus les représentations induites sur $\mathrm{Pin}\, Q$ et $\mathrm{Spin}\, Q$ sont également qualifiées de représentations spinorielles.

– $\operatorname{Pin} Q = \operatorname{Pin}^+ Q \bigcup \operatorname{Pin}^- Q$
– *On a la suite exacte :*

$$1 \to \mathbf{Z}_2 \to \operatorname{Spin} Q \xrightarrow{\rho} \mathrm{SO}(q) \to 1$$

Démonstration. La première assertion vient de ce que $\operatorname{Pin} Q = \{\pm x_1 \cdots x_k\}$, or $x_1 \cdots x_k \in C^{\pm}(Q)$ selon que k est pair ou impair.

Ainsi, un élément de $\operatorname{Spin} Q$ s'envoie sur un produit pair de réflexions orthogonales, donc est dans $\mathrm{SO}(Q)$ (et il s'agit bien d'une surjection car $\operatorname{Pin}^- Q \bigcap \mathrm{SO}(Q) = \emptyset$). □

Passons maintenant au cas complexe. Tout ce qui s'étend se transpose immédiatement au cas complexe, si l'on définit $\operatorname{Pin} Q$ comme le noyau de la norme. Cependant ceci nous donne une paramétrisation de $\mathrm{O}(Q)$, c'est à dire d'une forme hyperbolique (car $\mathbf{C}$ est complexe).

Cependant, nous préférons nous intéresser aux liens entre $\mathrm{U}(Q)$, $\operatorname{Pin} Q$ et $\mathrm{O}(Q)$, pour Q la forme euclidienne (resp hermitienne) canonique. On constate facilement que Q ou $-Q$ conduisent au mêmes groupes, on va alors en fait plutôt étudier $C_k = C(-Q)$ car alors $\operatorname{Pin}_k = \operatorname{Ker} N$.

On prolonge α et β sur le complexifié $C_k \otimes_{\mathbf{R}} \mathbf{C}$ par

$$\alpha(x \otimes z) = \alpha(x) \otimes z \tag{11}$$
$$(x \otimes z)^t = x^t \otimes \bar{z} \tag{12}$$

Ce qui suit découle mécaniquement du cas réel.

Définition 13
– $\mathbf{\Gamma}_k^c$ est le sous-groupe des éléments inversibles $x \in C_k \otimes_{\mathbf{R}} \mathbf{C}$ pour lesquels $y \in \mathbf{R}^k$ implique $\alpha(x) y x^{-1} \in \mathbf{R}^k$.
– On munit $C_k \otimes_{\mathbf{R}} \mathbf{C}$ de $N(x) = x\bar{x}$
– On a un morphisme

$$\begin{aligned} \mathbf{\Gamma}_k^c &\to \operatorname{Aut}(\mathbf{R}^k) \\ \rho(x) \cdot y &\mapsto \alpha(x) y x^{-1} \end{aligned}$$

Et on a en reprenant les démonstrations

Proposition 24
– $\operatorname{Ker} \rho = \mathbf{C}^*$
– *N est un morphisme de $\mathbf{\Gamma}_k^c \to \mathbf{C}^*$*
– $\rho(\mathbf{\Gamma}_k^c) = \mathrm{O}(k)$

ce qui fait que si on définit Pin_k^c comme étant le noyau de N sur $\mathbf{\Gamma}^c(k)$, on obtient le

Théorème 25 *On a une suite exacte*

$$1 \to \mathbf{U} \to \operatorname{Pin}^c(k) Q \xrightarrow{\rho} \mathrm{O}(k) \to 1$$

où l'on identifie $\mathbf{U}$ *et* $1 \otimes \mathbf{U} \subset \mathbf{C}_k \otimes_{\mathbf{R}} \mathbf{C}$

Démonstration. En effet cette fois, le noyau est composé des $1 \otimes z$ tels que $z\bar{z} = 1$, c'est bien **U** □

Corollaire 26 *On a un isomorphisme naturel*

$$\mathrm{Pin}(k) \times_{Z_2} \mathrm{U}(1) \to \mathrm{Pin}^c(k)$$

Démonstration.

Les inclusions $\mathrm{Pin}(k) \subset C_k$ et $U(1) \subset \mathbf{C}$ induisent une inclusion du produit fibré $\mathrm{Pin}(k) \times_{Z_2} \mathrm{U}(1)$ dans $C_k \otimes_{\mathbf{R}} \mathbf{C}$. Par définition de $\mathrm{Pin}^c(k)$, l'inclusion se factorise en un morphisme

$$\Psi : \mathrm{Pin}(k) \times_{Z_2} \mathrm{U}(1) \to \mathrm{Pin}^c(k)$$

On a le diagramme commutatif suivant :

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{U}(1) & \to & \mathrm{Pin}(k) \times_{Z_2} \mathrm{U}(1) & \to & \mathrm{Pin}(k)/\mathbf{Z}_2 & \to & 1 \\ \downarrow & & \downarrow & & \downarrow \Psi & & \downarrow & & \downarrow \\ 0 & \to & \mathbf{U} & \to & \mathrm{Pin}^c(k) & \to & \mathrm{O}(k) & \to & 1 \end{array}$$

Comme toutes les flèches (sauf Ψ) entre les deux suites exactes sont des isomorphismes, le «lemme des cinq» (ou lemme du serpent) montre que Ψ est en fait un isomorphisme.

□

On définit ensuite $\mathrm{Spin}^c(k)$ comme l'image réciproque de $\mathrm{SO}(k)$. Alors le corollaire 26 nous donne

$$\mathrm{Spin}^c(k) \cong \mathrm{Spin}(k) \times_{Z_2} \mathrm{U}(1)$$

(il suffit de prendre l'intersection avec les éléments de $C^+(k)$).

L'intérêt des spineurs complexes est le suivant : alors que le morphisme naturel

$$j : \mathrm{U}(k) \to \mathrm{SO}(2k)$$

ne s'étend à $\mathrm{Spin}(2k)$, en revanche le morphisme

$$l : \mathrm{U}(k) \to \mathrm{SO}(2k) \times \mathrm{U}(1) \tag{13}$$

$$T \mapsto j(T) \times \det T \tag{14}$$

s'étend à $\mathrm{Spin}^c(2k)$.

En effet, soit $T \in \mathrm{U}(k)$, qui s'écrit dans une base orthogonale $(f_1, \ldots, f_k)$

$$\begin{pmatrix} \exp it_1 & & & \\ & \exp it_2 & & \\ & & \ddots & \\ & & & \exp it_k \end{pmatrix}$$

et soit $(e_1, \ldots, e_{2k})$ la base correspondante de f dans $\mathbf{R}^{2k}$:

$$e_{2j-1} = f_j \qquad e_{2j} = if_j$$

Alors l'extension $\tilde{l}$ s'obtient par :

$$\tilde{l}(T) = \prod_{j=1}^{k} (\cos t_j/2 + \sin t_j/2 \cdot e_{2j-1}e_{2j}) \times \exp\left(\frac{i\sum t_j}{2}\right)$$

2.6.3 Digression : représentation tordue contre représentation naturelle

On peut se demander pourquoi on n'a pas introduit comme on l'avait fait dans les remarques préliminaires le groupe de Clifford comme étant

$$G = \{x \in C^*(q) \mid \forall y \in E, xyx^{-1} \in E\}$$

On aurait ensuite pu définir $\phi(x) \cdot y = xyx^{-1}$ et $N(x) = xx^t$. On aurait eu bien eu cette fois, si $x \in E$, $N(x) = Q(x)$.

Cependant, il y a plusieurs inconvénients à cette méthode. Tout d'abord, si $x \in E$, $\phi(x)$ est l'opposé de la réflexion orthogonale par rapport à $x^\perp$. Ce qui fait qu'on ne peut obtenir toutes les isométries que dans le cas n pair.

Ensuite, $N(x) \in \mathbf{K}^*$ que si $x \in G$ et n pair ou $x \in G^+$ (en effet, si n est impair, le centre de $C(Q)$ n'est pas forcément $\mathbf{K}$).

C'est ce qui explique qu'on ait introduit une représentation «tordue» ρ à la place. Toutefois on peut définir le groupe des Spineurs sur G^+ ou sur $\mathbf{\Gamma}^+$, on vérifie facilement qu'on obtient le même groupe. On peut également définir le groupe $\operatorname{Pin} Q$ sur G si n est pair.

2.6.4 Algèbre de Lie de $\operatorname{Spin} Q$

Nous allons identifier l'algèbre de Lie de $\operatorname{Spin} Q$ et montrer (si Q est définie, et $n \geqslant 3$) que $\operatorname{Spin} Q$ est le revêtement universel de $\mathrm{SO}(Q)$.

Commençons par déterminer la structure d'algèbre de Lie de $C^*(Q)$. [10]

Posons $\theta_X : Y \in C(Q) \mapsto XY \in C(Q)$.

Lemme 27 *$\theta : X \mapsto \theta_X$ est un homéomorphisme analytique de $C(Q)$ sur un sous-espace de* $\operatorname{End} C(Q)$.

Démonstration. Si θ_{X_n} admet une limite, alors $X_n = \theta_{X_n}$ également. Donc θ est bien un homéomorphisme. Le reste est évident. □

Définition 14 On pose

$$\exp X = \theta^{-1} \exp \theta_X = \sum_0^\infty \frac{X^k}{k!}$$

$X \mapsto \exp X$ vérifie toutes les propriétés habituelles de l'exponentielle (continuité, si $XY = YX$, $\exp(X+Y) = \exp X \exp Y$). C'est en fait l'exponentielle de l'algèbre de Lie $\mathfrak{l}(C^*(Q))$ de $C^*(Q)$ dans $C^*(Q)$ soit encore que $\mathfrak{l}(C^*(Q)) = C(Q)$.

En effet, $t \in \mathbf{R} \mapsto \exp tX$ est un morphisme de groupe de Lie, donc X, sa dérivée en 0 appartient à $\mathfrak{l}(C^*(Q))$. Ce qui nous donne une inclusion, et pour des raisons de dimensions on a forcément égalité. D'où au passage $\dim C^*(Q) = 2^n$.

[10] C^*Q est clairement un groupe de Lie, calculer X^{-1} revient à résoudre un système de Cramer, donc il s'agit d'une application analytique.

Enfin, $\theta(C(Q))$ est une sous-algèbre de Lie de $\operatorname{End} C(Q)$, avec le crochet habituel :

$$\begin{aligned}[\theta_X, \theta_Y] &= \theta_X\theta_Y - \theta_Y\theta_X = \theta(XY - YX) \\ &= [\mathrm{d}\,\theta(X), \mathrm{d}\,\theta(Y)] = \mathrm{d}\,\theta[X,Y] = \theta[X,Y] \quad \text{par linéarité de } \theta\end{aligned}$$

d'où le crochet de Lie est $[X,Y] = XY - YX$.

Maintenant, $\operatorname{Spin} Q$ est un sous-groupe fermé de $C^*(Q)*$, donc c'est un sous-groupe de Lie. Son algèbre de Lie est l'ensemble des éléments $X \in C(Q)$ tels que $\exp tX \in \operatorname{Spin} Q$.

En particulier, elle est incluse dans les X tels que

$$\exp tX\beta(\exp tX) = \pm 1$$

en dérivant en $t = 0$, on obtient $\beta(X) + X = 0$ (car β commute avec exp).

Or l'espace de ces tels X est de dimension $n(n-1)/2$. Comme $\operatorname{Spin} Q$ est un revêtement de $\mathrm{SO}(Q)$ (Z_2 est un sous-groupe distingué discret de $\operatorname{Spin} Q$, le passage au quotient induit un revêtement). Donc l'algèbre de Lie de $\mathrm{SO}(Q)$ est isomorphe à celle de $\operatorname{Spin} Q$, en particulier elle est de dimension $n(n-1)/2$.

On a donc

$$\mathfrak{L}(\operatorname{Spin} Q) = \{X \mid X + X^t = 0\}$$

on vérifie facilement (par dimension) qu'elle est engendrée par les e_ie_j, $i < j$ (les e_i formant une base orthogonale de E)

Proposition 28 *Si Q est une forme quadratique définie positive (ou négative),* $\operatorname{Spin}\mathbf{Q}$ *est connexe ($n \geq 2$).*

Démonstration. Comme $\operatorname{Spin} Q$ est un revêtement de $\mathrm{SO}(Q)$, qui est connexe lorsque Q est défini, il suffit de montrer que $+1$ et -1, le noyau du revêtement peuvent être connectés.

Or dans les deux cas, $(e_1e_2)^2 = -1$ d'où en développant en série,

$$\exp(te_1e_2) = \cos t + \sin t(e_1e_2) \tag{15}$$

$$\exp(\pi xy) = -1 \tag{16}$$

donc $t \mapsto \exp(te_1e_2)$ est bien un chemin reliant 1 et -1. □

Enfin, si $n \geq 3$, $\pi_1 \mathrm{SO}(n) = \mathbf{Z}_2$, donc $\mathrm{Spin}(n)$ est simplement connexe. C'est le revêtement universel de $\mathrm{SO}(n)$.

2.7 Modules sur les algèbres de Clifford standard

Comme on l'a vu, les algèbres de Clifford C_k et $C_k \otimes_{\mathbf{R}} \mathbf{C}$ présentent une certaine périodicité. Cette périodicité se traduit encore plus nettement sur les groupes de Grothendieck des catégories de modules (grâce à l'équivalence de Morita), et il apparaît naturellement dans ces constructions des groupes très similaires aux groupes de K-théorie des sphères, et dont la périodicité correspond au théorème de Bott.

Ces similitudes sont le point de départ de l'intervention des modules de Clifford en K-théorie, qu'élucide l'article d'Atiyah, Bott et Shapiro.

2.7.1 Classification

Commençons par classifier les modules gradués sur les algèbres de Clifford C_k. Comme, encore une fois, la graduation risquerait d'être problématique, on peut se ramener à des modules non gradués grâce à la proposition suivante :

Proposition 29 *Le foncteur de la catégorie* $\mathbf{Mod}_{gr}(C_k)$ *des modules gradués de type fini sur* C_k *dans* $\mathbf{Mod}(C_k^0)$ *qui à* $M = M^0 \oplus M^1$ *associe* M^0 *est une équivalence de catégorie.*

Démonstration. Il suffit de vérifier que le foncteur d'extension des scalaires, qui à M^0 associe $C_k \otimes_{C_k^0} M^0$ muni de la graduation évidente, est bien un quasi-inverse. Mais c'est clair : d'une part, on a les isomorphismes naturels

$$C_k \otimes_{C_k^0} M^0 = (C_k^0 \oplus C_k^1) \otimes_{C_k^0} M^0 = M^0 \oplus (C_k^1 \otimes_{C_k^0} M^0)$$

et donc $(C_k \otimes_{C_k^0} M^0)^0 = M^0$. D'autre part, le morphisme naturel de « multiplication externe » $C_k \otimes_{C_k^0} M^0 \to M$ est surjectif, et injectif sur $1 \otimes M^0$ et $e \otimes M^0$ (pour e un élément quelconque de C_k^1), donc c'est un isomorphisme. □

En particulier, comme les algèbres C_k^0 sont semi-simples, $\mathbf{Mod}_{gr}(C_k)$ est une catégorie semi-simple, et son groupe de Grothendieck $K_{gr}(C_k)$ est le groupe abélien libre engendré par les modules gradués simples de type fini. Il est isomorphe au groupe abélien libre $K_0(C_k^0)$ engendré par les C_k^0-modules simples de type fini. On aura donc une assez bonne description de $\mathbf{Mod}_{gr}(C_k)$ si l'on arrive à décrire le groupe $K_0(C_k^0)$.

Tous les résultats précédents ont bien sûr leur analogue évident sur le algèbres complexes $C_k \otimes_{\mathbf{R}} \mathbf{C}$. On note $K_{gr}^c(C_k)$ et $K_0^c(C_k^0)$ les groupes de Grothendieck correspondants.

Remarquons par ailleurs que l'on connaît déjà les algèbres C_k^0. En effet :

Proposition 30 *On a pour tout* k, $C_k \cong C_{k+1}^0$.

Démonstration. En effet, considérons l'application linéaire $\phi : \mathbf{R}^k \to C_{k+1}^0$ définie par $\phi(e_i) = e_i e_{k+1}$. On a, pour tout i, $\phi(e_i)^2 = e_i e_{k+1} e_i e_{k+1} = -e_i^2 e_{k+1}^2 = -1$, donc ϕ se prolonge en un morphisme d'algèbres $C_k \to C_{k+1}^0$, qui est injectif car il envoie la base canonique de C_k sur une famille libre de C_{k+1}. C'est donc un isomorphisme par égalité des dimensions. □

On a en particulier :

$$K_{gr}(C_k) = K_0(C_k^0) = K_0(C_{k-1})$$

Soit $i : C_k \to C_{k+1}$ le morphisme qui prolonge l'inclusion $\mathbf{R}^k \to \mathbf{R}^{k+1}$. Il induit par restriction des scalaires un morphisme de groupes $i^* : K_{gr}(C_{k+1}) \to K_{gr}(C_k)$. Son conoyau A_k, et l'analogue complexe A_k^c, vont jouer un rôle crucial dans toute la théorie développée par la suite. On note enfin a_k la dimension réelle de M^0, pour M un C_k-module gradué simple (ils ont clairement tous même dimension, vu la structure des algèbres C_k), et a_k^c l'analogue complexe. L'entier a_k a une très belle interprétation géométrique en termes de champs de vecteurs sur les sphères — on en dira quelques mots plus loin. On est en mesure de calculer l'ensemble des objets que l'on a définis ici.

k	C_k	$K_{gr}(C_k)$	A_k	a_k	$K^c_{gr}(C_k)$	A^c_k	a^c_k
1	$\mathbf{C}(1)$	$\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$	1	$\mathbf{Z}$	0	1
2	$\mathbf{H}(1)$	$\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$	2	$\mathbf{Z}\oplus\mathbf{Z}$	$\mathbf{Z}$	1
3	$\mathbf{H}(1)\oplus\mathbf{H}(1)$	$\mathbf{Z}$	0	4	$\mathbf{Z}$	0	2
4	$\mathbf{H}(2)$	$\mathbf{Z}\oplus\mathbf{Z}$	$\mathbf{Z}$	4	$\mathbf{Z}\oplus\mathbf{Z}$	$\mathbf{Z}$	2
5	$\mathbf{C}(4)$	$\mathbf{Z}$	0	8	$\mathbf{Z}$	0	4
6	$\mathbf{R}(8)$	$\mathbf{Z}$	0	8	$\mathbf{Z}\oplus\mathbf{Z}$	$\mathbf{Z}$	4
7	$\mathbf{R}(8)\oplus\mathbf{R}(8)$	$\mathbf{Z}$	0	8	$\mathbf{Z}$	0	8
8	$\mathbf{R}(16)$	$\mathbf{Z}\oplus\mathbf{Z}$	$\mathbf{Z}$	8	$\mathbf{Z}\oplus\mathbf{Z}$	$\mathbf{Z}$	8

$$K_{gr}(C_{k+8}) = K_{gr}(C_k) \qquad A_{k+8} = A_k \qquad a_{k+8} = 16a_k$$
$$K^c_{gr}(C_{k+2}) = K^c_{gr}(C_k) \qquad A^c_{k+2} = A^c_k \qquad a^c_{k+2} = 2a^c_k$$

TAB. 3 – Groupes de Grothendieck des catégories $\mathbf{Mod}_{gr}(C_k)$.

La majeure partie de ce tableau découle immédiatement du tableau précédent et des résultats connus sur les modules sur les algèbres de matrices. Les seuls résultats non évidents sont la détermination de A_{4n} et A^c_{2n}.

Pour expliciter ce calcul, remarquons qu'à tout module gradué $M = M^0 \oplus M^1 \in \mathbf{Mod}_{gr}(C_k)$, on peut associer un autre module gradué $M^* = M^1 \oplus M^0$ en translatant la graduation. Cette opération, qui commute évidemment aux sommes directes, définit ainsi une involution, encore notée $*$, sur le groupe $K_{gr}(C_k)$, et de même sur $K^c_{gr}(C_k)$.

Le fait que $A_{4n} = \mathbf{Z}$ découle alors de la proposition suivante.

Proposition 31 *Soit x et y les deux classes de C_{4n}-modules gradués simples. On a $x^* = y$ et $y^* = x$.*

Cette proposition donne bien le résultat, puisque si z désigne le générateur de $K_{gr}(C_{4n+1})$, on a $z^* = z$, donc i^*z est également stable par $*$. Par raison de dimension, il en résulte nécessairement que $z = x + y$, ce qui conclut.

La proposition découle quant à elle du lemme suivant.

Lemme 32 *Soit $y \in \mathbf{R}^k \setminus \{0\}$, et A_y l'automorphisme intérieur de C_k défini par y : $A_y(w) = ywy^{-1}$. On a alors :*

- *Pour tout module $M \in \mathbf{Mod}_{gr}(C_k)$, le module A_yM, sur lequel C_k agit par $w \cdot m = A_y(w)m$, est isomorphe à M^*.*
- *Sous les mêmes hypothèses, si l'on note A^0_y la restriction de A_y à C^0_k, alors $A^0_yM^0 = M^1$.*
- *En notant ϕ l'isomorphisme $C_{k-1} \to C^0_k$ introduit à la proposition 30, on a :*

$$A^0_{e_k}(\phi(w)) = \phi(\alpha(w))$$

où α est l'automorphisme canonique de C_{k-1}.

Démonstration. Soit $M \in \mathbf{Mod}_{gr}(C_k)$. L'isomorphisme $\mathbf{R}$-linéaire $f : A_y M \to M^*$ donné par $f(m) = y^{-1}m$ vérifie, pour tout $w \in C_k$:

$$f(w \cdot m) = y^{-1}(w \cdot m) = y^{-1}ywy^{-1}m = wf(m)$$

donc f est C_k-linéaire. De plus, comme y^{-1} est un élément de degré 1 de C_k, f envoie $(A_y M)^0 = A_y^0 M^0$ sur $M^1 = (M^*)^0$, et de même pour la composante de degré 1, donc c'est un isomorphisme de C_k-modules gradués. L'isomorphisme $A_y^0 M^0 = M^1$ est alors clair.

Par ailleurs, la dernière partie de l'énoncé est le calcul élémentaire suivant :

$$A^0_{e_k}(\phi(w)) = e_k(we_k)e_k^{-1} = e_k w = \alpha(w)e_k = \phi(\alpha(w))$$

qui résulte de ce que $e_k e_i = \alpha(e_i)e_k$ pour $1 \leqslant i \leqslant k-1$. □

Démonstration (de la proposition). La morale lemme, en passant aux groupes de Grothendieck, c'est que sous l'isomorphisme groupes abéliens $K_{gr}(C_k) \cong K_0(C_{k-1})$, l'opération $*$ se traduit par α. Mais l'on sait décrire l'action de α sur les deux classes de C_{4n-1}-modules simples : il suffit pour cela de remarquer que le centre de C_{4n-1} est engendré par 1 et $w = e_1 e_2 \cdots e_{4n-1}$, qui vérifie $w^2 = 1$. Les idempotents centraux minimaux sont donc $(1+w)/2$ et $(1-w)/2$, et comme $\alpha(w) = -w$, l'automorphisme α les échange. Il échange donc les deux classes de C_{4n-1}-modules simples, et donc les deux classes de C_{4n}-modules gradués simples dans $K_{gr}(C_{4n})$. □

2.7.2 Structure de Clifford sur l'algèbre extérieure

Bien sûr, on montre *mutatis mutandis* que $A^c_{2n} = \mathbf{Z}$. Cependant, on peut donner une description un peu plus explicite dans ce cas-là. En effet, considérons l'algèbre extérieure $\Lambda^*(\mathbf{C}^k)$, muni du produit hermitien pour lequel les $e_{i_1} \wedge \cdot \wedge e_{i_p}$, $1 \leqslant i_1 < \cdot < i_p \leqslant k$, forment une base orthonormée. On note $d_v : w \mapsto v \wedge w$ la multiplication extérieure par v, et d_v^* son adjoint. Alors on a une application bilinéaire :

$$\begin{array}{rcl} \mathbf{C}^k \times \Lambda^*(\mathbf{C}^k) & \to & \mathbf{C} \\ (v, w) & \mapsto & L(v)w = (d_v - d_v^*)(w) \end{array}$$

avec, de plus, $L(v)^2 w = -\|v\| w$. En effet, on peut supposer, quitte à faire un changement de base orthogonal, que $v = \lambda e_1$. Alors on a :

$$d_v(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \begin{cases} \lambda e_1 \wedge e_{i_1} \wedge \cdots \wedge e_{i_p} & \text{si } i_1 \neq 1 \\ 0 & \text{sinon} \end{cases}$$

$$d_v^*(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \begin{cases} \lambda e_{i_2} \wedge \cdots \wedge e_{i_p} & \text{si } i_1 = 1 \\ 0 & \text{sinon} \end{cases}$$

donc :

$$L(v)(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \begin{cases} \lambda e_1 \wedge e_{i_1} \wedge \cdots \wedge e_{i_p} & \text{si } i_1 \neq 1 \\ -\lambda e_{i_2} \wedge \cdots \wedge e_{i_p} & \text{sinon} \end{cases}$$

ce qui donne bien $L(v)^2 = -\lambda^2 \,\mathrm{id} = \|v\|^2 \,\mathrm{id}$. Par conséquent, L s'étend en une action *complexe* de l'algèbre de Clifford $C_{2k} = C(\mathbf{R}^{2k})$ sur $\Lambda^*(\mathbf{C}^k)$, c'est-à-dire une structure

de $(C_{2k} \otimes_{\mathbf{R}} \mathbf{C})$-module, avec la $\mathbf{Z}/2$-graduation naturelle par la parité du degré. Comme $\Lambda^*(\mathbf{C}^k)$ est un $\mathbf{C}$-espace vectoriel de dimension $2^k = a^c_{2k}$, c'est l'un des deux modules gradués simples de $\mathbf{Mod}_{gr}(C_{2k} \otimes_{\mathbf{R}} \mathbf{C})$. En particulier, il fournit par passage au quotient un générateur de A^c_{2k} (qu'on pourra même identifier plus précisément comme $(-1)^k(\mu^c)^k$ avec les notations introduites plus loin).

2.7.3 Champs de vecteurs sur les sphères

On peut difficilement étudier les modules de Clifford réels et introduire les nombres de Radon-Hurwitz a_k sans évoquer leur lien important avec les champs de vecteurs sur les sphères, tel qu'il est décrit par exemple dans [MA64] **S**15b.

En effet, s'il existe une structure de C_k-module (non gradué) sur un $\mathbf{R}$-espace vectoriel M de dimension n, alors on peut munir M d'un produit scalaire $\langle \cdot, \cdot \rangle$ invariant par le groupe compact image de $\mathrm{Pin}(k)$ dans $\mathrm{End}(M)$. On regarde la sphère S^{n-1} comme la sphère unité pour ce produit scalaire. Alors, si l'on note $e_1, \ldots, e_k$ les générateurs usuels de C_k, on a pour tout $x, y \in M$, puisque les e_i sont dans $\mathrm{Pin}(k)$:

$$\langle e_i x, e_i y \rangle = \langle x, y \rangle \quad \text{et} \quad \langle e_i x, y \rangle = \langle e_i x, e_i(-e_i y) \rangle = -\langle x, e_i y \rangle$$

Autrement dit, les e_i sont des isométries antisymétriques. En particulier, on a pour tous $i \neq j$, on a $\langle e_i x, e_j x \rangle = \langle e_i^2 x, e_i e_j \rangle = -\langle x, e_i e_j x \rangle$, et comme cette expression est symétrique en i et j, et $e_i e_j = -e_j e_i$, il vient :

$$\langle e_i x, x \rangle = \langle e_i x, e_j x \rangle = 0$$

Il en résulte que les applications :

$$\begin{array}{rccc} X_i : S^{n-1} & \to & M \\ x & \mapsto & e_i x \end{array}$$

sont des champs de vecteurs unitaires tangents deux à deux orthogonaux sur S^{n-1}.

Or il existe une structure de C_k-module sur M si et seulement si la dimension commune a_k des C_k-modules simples (non gradués) divise n. On peut donc formuler l'énoncé suivant :

Théorème 33 *Soit r_n le plus grand entier k tel que a_k divise n. Alors il existe au moins r_n champs de vecteurs indépendants sur la sphère S^{n-1} (autrement dit, le fibré tangent à S^{n-1} possède un sous-fibré trivial de rang r_n).*

Comme on connaît déjà a_k, évaluer r_n est l'affaire d'un calcul facile. On trouve :

$$r_n = 2^c - 1 + 8d \quad \text{avec } n = 2^{c+4d}m,\ m \text{ impair et } 0 \leqslant c \leqslant 3$$

En particulier, $r_2 = 1$, $r_4 = 3$ et $r_8 = 7$. On retrouve ainsi le fait que S^1, S^3 et S^7 sont parallélisables.

D'après un résultat célèbre d'Adams [Ada62], le résultat ainsi obtenu est en fait optimal : r_n est exactement le nombre maximal de champs de vecteurs indépendants sur S^{n-1}.

On peut signaler en passant que le théorème d'Adams répond à la question, récemment survenue sur `forum` (`sciences.maths:9497` et suivants) de déterminer la dimension maximale possible d'un sous-espace vectoriel de $\mathbf{R}(n)$ qui ne contienne, outre 0, que des matrices inversibles : c'est exactement $r_n + 1$. En effet, si $\mathbf{R}^n$ est un C_k-module, les endomorphismes induits par $1, e_1, \cdots, e_k$ engendrent un espace vectoriel qui convient, car tout élément de cet espace s'écrit $u = \lambda \cdot 1 + x$, $x \in \mathbf{R}^k$, et alors :

$$N(u) = u\bar{u} = (\lambda + x)(\lambda - x) = \lambda^2 + \|x\|^2$$

Réciproquement, si V est un sous-espace de $\mathbf{R}(n)$ tel que toute matrice de $V \setminus \{0\}$ soit inversible, on peut supposer sans perte de généralité que V contient l'identité, et a donc une base de la forme $1, u_1, \ldots, u_k$. Mais alors en chaque point $x \in S^{n-1}$, $u_1(x), \ldots, u_k(x)$ se projettent sur $x^\perp$ en k vecteurs linéairement indépendants, ce qui détermine k champs de vecteurs indépendants sur S^n : d'où le résultat, qui est cependant un peu plus élémentaire que le théorème d'Adams, puisqu'il est seulement question de champs de vecteurs *linéaires* sur la sphère.

2.7.4 Propriétés multiplicatives : l'anneau gradué A_*

Soit M un C_k-module gradué et N un C_l-module gradué. Alors leur produit tensoriel gauche $M\hat{\otimes}N$ est naturellement un module gradué sur $C_k\hat{\otimes}C_l$, la graduation étant choisie de façon évidente :

$$(M\hat{\otimes}N)^0 = (M^0 \otimes N^0) \oplus (M^1 \otimes N^1) \quad \text{et} \quad (M\hat{\otimes}N)^1 = (M^0 \otimes N^1) \oplus (M^1 \otimes N^0)$$

et l'action de $C_k\hat{\otimes}C_l$ donnée par :

$$(x \otimes y) \cdot (m \times n) = (-1)^{qi}(xm) \cdot (yn) \quad \text{pour } y \in C_l^q \text{ et } m \in M^i$$

Or comme C_k est la puissance k-ième de C_1 au sens du produit tensoriel gauche, on a naturellement $C_k\hat{\otimes}C_l \cong C_{k+l}$. Le produit tensoriel gauche induit donc une application bilinéaire $\hat{\otimes} : K_{gr}(C_k) \times K_{gr}(C_l) \to K_{gr}(C_{k+l})$, Par conséquent, si l'on note $K_* = \bigoplus_{k=0}^{\infty} K_{gr}(C_k)$, K_* est une $\mathbf{Z}$-algèbre graduée pour $\hat{\otimes}$, dont on voit aisément qu'elle est associative. Donc on dispose d'un anneau gradué $(K_*, +, \cdot)$, muni de l'automorphisme $*$ introduit plus haut.

Il vérifie de plus $(u \cdot v)^* = u \cdot (v^*)$: c'est évident par définition de la graduation. Et si l'on note $i^* : K_{gr}(C_k) \to K_{gr}(C_{k-1})$ le morphisme de restriction des scalaires, on a $u \cdot (i^*v) = i^*(u \cdot v)$. Une propriété moins immédiate est que, pour $(u, v) \in K_{gr}(C_k) \times K_{gr}(C_l)$:

$$u \cdot v = \begin{cases} v \cdot u & \text{si } kl \text{ est pair} \\ (v \cdot u)^* & \text{sinon} \end{cases}$$

Elle résulte de ce que l'opération $M\hat{\otimes}N \mapsto N\hat{\otimes}M$ est l'automorphisme induit sur le groupe de Grothendieck par l'automorphisme d'algèbre $T : C_{k+l} \to C_{k+l}$ qui étend l'échange, dans $\mathbf{R}^{k+l}$, des k premières coordonnées et des l suivantes. T s'obtient donc, au signe près, comme composé de kl automorphismes intérieurs de C_{k+l} par des vecteurs e_i. Sur K_{gr}, l'action est donc celle de kl applications de l'opération $*$, ce qui donne bien l'expression annoncée.

Remarquons que l'on a :

Proposition 34 *Soit $\lambda \in K_{gr}(C_8)$ la classe d'un C_8-module gradué simple. Alors la multiplication par λ induit un isomorphisme $K_{gr}(C_k) \cong K_{gr}(C_{k+8})$.*

Démonstration. Le résultat est clair si $K_{gr}(C_k) = K_{gr}(C_{k+8}) = \mathbf{Z}$, c'est-à-dire quand k n'est pas multiple de 4. Si maintenant $k = 4n$, soit x et $y = x^*$ les deux classes de C_k-modules gradués simples. Par raison de dimension, $\lambda \cdot x \in K_{gr}(C_{k+8})$ est l'une des deux classes de modules simples. Mais alors :

$$\lambda \cdot y = \lambda \cdot x^* = (\lambda \cdot x)^*$$

ce qui est l'autre classe de modules simples. □

De plus, l'image de $i^* : K_* \to K_*$ est un idéal gradué, et donc le conoyau $A_* = \bigoplus_{k=0}^{\infty} A_k$ est muni d'une structure d'anneau gradué déduite de celle de K_*. La multiplication par λ induit encore un isomorphisme $A_k \cong A_{k+8}$, et le résultat de commutation sur K_* se traduit par la commutativité (ou, ce qui revient au même dans ce cas, l'anticommutativité) de A_*. On peut préciser complètement la structure de cet anneau.

Théorème 35 *A_* est l'anneau gradué anticommutatif engendré par $1 \in A_0$ et par des éléments $\xi \in A_1$, $\mu \in A_4$ et $\lambda \in A_8$ soumis aux relation $2\xi = \xi^3 = 0$ et $\mu^2 = 4\lambda$.*

Démonstration. En prenant pour ξ un générateur de A_1, on a clairement $2\xi = \xi^3 = 0$, puisque $A_1 = \mathbf{Z}/2$ et $A_3 = 0$. De plus, le générateur de A_2 est ξ^2 par raison de dimension. Reste alors le calcul de μ^2.

Pour pouvoir faire des choix de signe cohérents, on introduit la terminologie suivante. Notons que pout $k = 4n$, si l'on pose $\omega = e_1 \dots e_{4n}$, ω est dans le centre de C_k^0 et est de carré 1. Si $M \in \mathbf{Mod}_{gr}(C_k)$ est un module simple, ω agit donc sur M^0 par $\varepsilon = \pm 1$. De manière générale, on dit qu'un module gradué M est un ε-module si ω agit sur M^0 par multiplication scalaire par ε. Comme $e_i\omega = -\omega e_i$, on a clairement que si M est un ε-module, M^* est un $(-\varepsilon)$-module. De plus, si M et M' sont respectivement un ε-module et un ε'-module, alors $M \hat{\otimes} M'$ est un $\varepsilon\varepsilon'$-module.

Convenons alors de choisir pour λ la classe d'un $(+1)$-module simple W dans A_8. Si μ est la classe d'un ε-module simple M sur C_4, alors $M \hat{\otimes} M$ est un $(+1)$-module simple sur C_8, de dimension réelle $(2a_4)^2 = 4 \cdot (2a_8)$. On a donc nécessairement $M \hat{\otimes} M \cong 4W$, d'où en effet $\mu^2 = 4\lambda$. □

Le raisonnement se transporte *mutatis mutandis* au cas complexe, et fournit des anneaux gradués K_*^c et A_*^c, et la périodicité s'obtient par multiplication par une classe μ^c de $(C_2 \otimes_{\mathbf{R}} \mathbf{C})$-module gradué simple. En fait, le théorème devient :

Théorème 36 *L'anneau gradué A_*^c est isomorphe à l'anneau de polynômes $\mathbf{Z}[\mu^c]$.*

Les conventions de signes interviennent encore dans le cas complexe. Cette fois, pour $k = 2l$, on a $\omega^2 = (-1)^l$, donc ω agit sur un $(C_k^0 \otimes_{\mathbf{R}} \mathbf{C})$-module simple par $(\pm i)^l$. On convient de choisir pour μ^c la classe d'un $(+i)$-module gradué simple dans A_2^c. C'est avec cette convention qu'on obtient, dans A_k^c :

$$\Lambda(\mathbf{C}^k) = (-1)^k (\mu^c)^k$$

quand on muni l'algèbre extérieure de sa structure de Clifford complexe.

Par ailleurs, on peut alors exprimer le morphisme $A_* \to A_*^c$ induit par la complexification $M \mapsto M \otimes_{\mathbf{R}} \mathbf{C}$. En prenant pour $\mu \in A_2$ la classe d'un (-1)-module simple, la complexification envoie μ sur $2(\mu^c)^2$ et donc λ sur $(\mu^c)^4$.

3 Lien avec la K-théorie

On a introduit la plupart des outils techniques nécessaires pour présenter le morphisme construit dans [MA64] **S**11, qui suggère le lien profond existant entre modules de Clifford et K-théorie. Il reste cependant une construction topologique importante à intoduire, qui est l'objet du paragraphe suivant.

3.1 Le fibré différence

Soit X un espace, et Y un sous-espace fermé. On aura besoin d'associer à un morphisme $f : E_1 \to E_0$ de fibrés vectoriels sur X qui est un isomorphisme sur Y une élément $d(f)$ de $K(X,Y)$, de façon naturelle en le couple (X,Y) et invariante par addition d'un morphisme qui est un isomorphisme sur tout X. Pour $Y = \emptyset$, on peut prendre $d(f) = [E_0] - [E_1]$, mais si Y est plus grand, une construction plus élaborée est nécessaire.

On introduit à cette fin l'espace A, somme amalgamée de deux copies X_0, X_1 de X le long de Y. Il est muni de rétractions $\pi_i : A \to X_i$, obtenues en envoyant les points de X_0 et X_1 sur le point correspondant de X_i. Les π_i fournissent alors des suites exactes scindées :

$$0 \to K(A, X_i) \xrightarrow{\rho_i^*} K(A) \xrightarrow{j_i^*} K(X_i) \to 0$$

Par ailleurs on a un homéomorphisme naturel $\phi_i : X_i/Y \to A/X_{i+1}$ qui fournit un isomorphisme $\phi_i^* : K(A, X_{i+1}) \to K(X,Y)$.

Soit alors $f : E_1 \to E_0$ un morphisme comme indiqué plus haut. On construit un fibré F sur A valant E_i en restriction à X_i, en identifiant les deux fibrés par f le long de Y. Cette construction est bien fonctorielle en f. De plus, $F_i = \pi_i^*(E_i)$ vérifie $F|_{X_i} \cong E_i \cong F_i|_{X_i}$. Par conséquent, $F - F_i$ est dans le noyau du morphisme $j_i^* : K(A) \to K(X_i)$, ce qui permet, d'après la suite exacte précédente, de définir un élément $d(f)$ de $K(X,Y)$ par :

$$\rho_i^*[(\phi_i^*)^{-1} d(f)] = F - F_1$$

Alors d est clairement additif : $d(f \oplus g) = d(f) + d(g)$. De plus, si f est un isomorphisme sur X tout entier, on a $F \cong F_1$, donc $d(f) = 0$. Il en résulte en particulier que d est invariant par addition d'un isomorphisme.

Ainsi, si l'on note $L(X,Y)$ le monoïde des classes d'isomorphisme de morphismes f à addition près d'un isomorphisme, on a défini une flèche $d : L(X,Y) \to K(X,Y)$, qui est une transformation naturelle de foncteurs additifs sur la catégorie des couples espace, sous-espace fermé. Quand $Y = \emptyset$, A est la somme disjointe de X_0 et X_1, F est le fibré valant E_i sur X_i, et l'on retrouve donc $d(f) = [E_0] - [E_1]$.

On peut noter, même si l'on ne s'en servira pas, que ces propriétés formelles suffisent à assurer, sous réserve que le couple (X, Y) soit topologiquement «gentil» (typiquement une CW-paire), que d est en fait un isomorphisme naturel, ce qui permet de donner une définition alternative de la K-théorie comme monoïde d'isomorphisme de complexes de fibrés vectoriel, dans l'esprit de la définition des groupes G_0 de Grothendieck [MA64] **SS**7–8. De plus, la définition ainsi obtenue a de bonnes propriétés multiplicatives, ce qui est un aspect de la méthode d'Atiyah-Bott qui fait souvent défaut aux démarches ultérieures, notamment que Karoubi présente dans [Kar68].

3.2 Les fibrés de Clifford

On en arrive enfin à la façon dont on peut, étant donné une structure convenable sur un fibré vectoriel $V \to X$ de rang k, associer à tout module de Clifford sur C_k une classe dans la K-théorie réduite du compactifié d'Alexandrov de V. On obtient en particulier une description particulièrement agréable de la K-théorie des sphères.

3.2.1 Cas du point, K-théorie des sphères

Commençons par considérer le cas où l'espace de base X est réduit à un point. Alors on se donne un espace euclidien V de dimension k, et un module gradué M sur $C(V) = C_k$.

Pour tout $v \in V$, la multiplication par v fournit une application linéaire $M^0 \to M^1$ dont l'adjoint $M^1 \to M^0$, au sens d'un produit scalaire quelconque invarant par $\mathrm{Spin}(V)$, est la multiplication par $-v$. De plus, comme tout élément non nul de V est de norme non nulle dans $C(V)$, cette application est un isomorphisme dès que $v \neq 0$. Par conséquent, si l'on considère le morphisme suivant, entre fibrés vectoriels triviaux sur la boule unité $\mathbf{B}(V)$ de V :

$$\begin{array}{rcl} \sigma(M) : M^1 \times \mathbf{B}(V) & \to & M^0 \times \mathbf{B}(V) \\ (m, v) & \mapsto & (-vm, v) \end{array}$$

$\sigma(M)$ est un isomorphisme en restriction à la sphère unité $\mathbf{S}(V)$. La construction du fibré différence fournit donc une classe de K-théorie $\chi_V(M) = d(\sigma(M)) \in KO(\mathbf{B}(V), \mathbf{S}(V))$, qui ne dépend bien sûr que de la classe d'isomorphisme de M et est additive en M. Or $\mathbf{B}(V)/\mathbf{S}(V)$ n'est autre que le compactifié d'Alexandrov de V, à savoir S^k. D'où un morphisme de groupes $\chi_V : K_{gr}(C_k) \to \widetilde{KO}(S^k)$.

De plus, supposons que la structure de $C(V)$-module de M s'étende en une structure de module gradué sur $C(V \oplus 1) = C_{k+1}$. Alors la restriction de $\sigma(M)$ au-dessus de $\mathbf{S}(V)$ s'étend en un isomorphisme de fibrés sur $\mathbf{S}(V \oplus 1)$, et donc en particulier en un isomorphisme $\sigma^+(M)$ sur l'hémisphère supérieur $\mathbf{S}^+(V \oplus 1)$. Or on a bien sûr $(\mathbf{B}(V), \mathbf{S}(V)) \cong (\mathbf{S}^+(V \oplus 1), \mathbf{S}(V))$. Il en résulte, par naturalité de d, que $d(\sigma(M))$ est l'image par un endomorphisme de $KO(\mathbf{B}(V), \mathbf{S}(V))$ de $d(\sigma^+(M)) = 0$. D'où $d(\sigma(M)) = 0$. L'image de la restriction des scalaires $K_{gr}(C_{k+1}) \to K_{gr}(C_k)$ s'envoie donc sur 0 par χ_V, ce qui fournit par passage au quotient un morphisme de groupes :

$$\chi_V : A_k \to \widetilde{KO}(S^k)$$

Cela s'écrit encore, en introduisant la notation «cohomologique» $\widetilde{KO}^{-n}$ pour le groupe $\widetilde{KO}$ de la n-ième suspension et $\widetilde{KO}^{*}$ pour l'anneau gradué anticommutatif $\bigoplus_n \widetilde{KO}^{-n}$ (avec la multiplication donnée par le smash-produit), sous la forme d'un morphisme de groupes additifs :

$$\chi_V : A_* \to \widetilde{KO}^{*}(*)$$

qui est en fait un morphisme d'anneaux (cela se vérifie assez mécaniquement si l'on vérifie les propriétés multiplicatives de toutes les constructions qu'on a introduites [MA64] **S**11).

Il se trouve que l'on a :

Théorème 37 *Le morphisme d'anneaux χ_V ainsi défini est un* isomorphisme*, et l'on obtient de la même manière un isomorphisme $\chi_V^c : A_*^c \to \widetilde{K}^*(*)$.*

ce qui fournit une description complète de la K-théorie réelle et complexe des sphères entièrement en termes de modules de Clifford, et en particulier leur périodicité de 8 et 2 respectivement .

Malheureusement, la démonstration donnée dans l'article est, du goût même des auteurs, assez peu satisfaisante : elle se limite à rappeler que la structure de ces anneaux est déjà connue, et à constater que les morphismes envoient bien générateurs sur générateurs. C'est décevant, mais en un sens peu surprenant : du point de vue topologique, les constructions que l'on a développées ici sont assez tautologiques. Des méthodes plus élaborées ont été mises au point ensuite pour obtenir une démonstration vraiment satisfaisante. On peut citer en particulier l'approche très élégante, mais aussi très abstraite, de Karoubi [Kar68], qui *définit* la K-théorie à coefficients dans une «catégorie de Banach» quelconque en termes de modules de Clifford, ce qui lui permet de déduire la périodicité de Bott et l'isomorphisme de Thom (dont il sera question dans un instant) de manière presque immédiate. Le théorème difficile et central de l'article est alors une version (hautement) généralisée de celui que nous venons d'énoncer, qui exprime que cette définition alternative de la K-théorie coïncide avec la définition usuelle.

3.2.2 Cas général et isomorphisme de Thom

Pour finir, examinons de quelle façon la construction qui précède se généralise au cas «relatif», où X est un espace quelconque, et V un fibré vectoriel euclidien de rang k. On lui associe un fibré en algèbres graduées $C(V)$ sur X, dont la fibre au-dessus de x est $C(V_x)$ et les applications de transition sont déduites de celles de V.

On considère alors un $C(V)$-module gradué $M = M^0 \oplus M^1$, ce qui revient à donner des fibrés vectoriels M^0 et M^1 sur X, avec des morphismes $V \otimes_{\mathbf{R}} M^0 \to M^1$ et $V \otimes_{\mathbf{R}} M^1 \to M^0$, notés $v \otimes m \mapsto vm$, tels que $v(vm) = -\|v\|^2 m$. On munit alors M^0 d'un produit scalaire invariant par $\mathrm{Spin}(V)$, qui s'étend à M en un produit scalaire invariant par $\mathrm{Pin}(V)$. Alors en tout point x, l'adjoint de la multiplication par v sur M_x^0 est la multiplication par $-v$ sur M_x^1.

Si l'on note $\pi : \mathbf{B}(V) \to X$ le fibré en boules unité associé au fibré euclidien V, on obtient alors un morphisme de fibrés vectoriels :

$$\sigma(M) : \pi^* M^1 \to \pi^* M^0$$

qui, sur la fibre au-dessus de $v \in \mathbf{B}(V)$, est la multiplication par $-v$. En restriction au fibré en sphères $\mathbf{S}(V)$, ce morphisme devient un isomorphisme, et si la structure de $C(V)$-module s'étend en une structure de $C(V \oplus 1)$-module (où 1 est le fibré en droite euclidien trivial), cet isomorphisme se prolonge au fibré en hémisphères $\mathbf{S}(V \oplus 1)$. Il en résulte que si l'on note $K_{gr}(C(V))$ le groupe de Grothendieck des $C(V)$-modules gradués de rang fini, et $A(V)$ le conoyau de la restriction $K_{gr}(C(V \oplus 1)) \to K_{gr}(C(V))$, on a un morphisme de groupes :

$$\chi_V : A(V) \to KO(\mathbf{B}(V), \mathbf{S}(V)) = \widetilde{KO}(X^V)$$

où X^V est *l'espace de Thom* de V, c'est-à-dire son compactifié d'Alexandrov.

Supposons alors que V est un *fibré spinoriel*, c'est-à-dire le fibré vectoriel $P \times_{\mathrm{Spin}(k)} \mathbf{R}^k$ associé à un $\mathrm{Spin}(k)$-fibré principal P. Alors pour tout C_k-module gradué M, $P \times_{\mathrm{Spin}(k)} M$ est naturellement un $C(V)$-module, ce qui fournit un morphisme de groupes $\beta_P : A_k \to A(V)$. On en déduit un morphisme de groupes important :

$$\alpha_P = \chi_V \beta_P : A_k \to \widetilde{KO}(X^V)$$

L'importance de ce morphisme peut par exemple se voir en considérant, pour $k = 8n$, l'élément $\mu_V = \alpha_P(\lambda^n) \in \widetilde{KO}(X^V)$, où λ est le générateur usuel de A_8. On a en effet :

Théorème 38 (isomorphisme de Thom) *$\widetilde{KO}^*(X^V)$ est le $KO^*(X)$-module gradué libre de rang 1 engendré par μ_V.*

Ce théorème profond a en particulier pour conséquence la périodicité de Bott. En effet, si l'on choisit pour V le fibré trivial $X \times \mathbf{R}^k$, et si l'on note X_+ l'espace pointé obtenu en adjoignant un point à X, on trouve :[11]

$$X^V = \mathbf{B}(V)/\mathbf{S}(V) = (X \times B^k)/(X \times S^{k-1}) = X_+ \wedge (B^k/S^{k-1}) = X_+ \wedge S^k$$

Donc en prenant $k = 8$ et V le fibré spinoriel trivial de rang 8, il vient $\widetilde{KO}(X_+) = KO(X) \cong \widetilde{KO}(X^V) = \widetilde{KO}^{-8}(X_+)$, ce qui est précisément la périodicité de Bott !

Encore une fois, cependant, la démonstration de l'isomorphisme de Thom proposée dans l'article n'est pas complètement satisfaisante. Elle utilise en effet beaucoup de propriétés topologiques non triviales de la K-théorie, et en particulier la périodicité de Bott elle-même. L'article de Karoubi [Kar68] apporte là aussi une approche éclairante.

[11] Rappelons que si A et B sont deux espaces pointés, leur somme $A \vee B$ est la somme amalgamée sur les points-base, et leur smash-produit $A \wedge B$ est $A \times B / A \vee B$. Alors la suspension est le smash-produit par S^1, et par récurrence immédiate, la n-ième suspension est le smash-produit par S^n.

Références

[Ada62] J.F. Adams. Vector fields on spheres. *Ann. Math. (2)*, vol. 75 :603–632, 1962.

[Cru74] A. Crumeyrolle. *Algèbres de Clifford et spineurs*. Cours et séminaires du département de Mathématiques de l'université Paul Sabatier, 1974.

[Hat03] A. Hatcher. Vector bundles & K-theory. . `http://www.math.cornell.edu/~hatcher/VBKT/VBpage.html`, 2003.

[Hou73] C. Houzel. *K-Théorie (Cours de D.E.A)*. Insitut de Mathématiques et Sciences Physiques de Nice, 1972-1973.

[Kar68] M. Karoubi. K-théorie. *Ann. Sci. ÉNS (4)*, vol. 1 :161–270, 1968.

[Kar69] M. Karoubi. *K-Théorie*. Les presses de l'université de Montréal, 1969.

[Lou97] P. Lounesto. *Clifford Algebra and Spinors*. Cambridge university press, 1997.

[MA64] A. Shapiro M.F. Atiyah, R. Bott. Clifford modules. *Topology*, vol. 3 :3–38, 1964.

[Wei97] C. Weibel. An introduction to algebraic K-theory. . `http://www.math.rutgers.edu/~weibel/Kbook.html`, 1997.