Groupes de Chevalley et Classification des groupes simples finis

Antoine Commaret et Guillaume Rabineau
Sous la direction de Cyril Demarche

Résumé

Si la théorie des algèbres de Lie apparaît de manière naturelle en géométrie différentielle en considérant l'espace tangent d'un groupe de Lie en l'identité, elle fournit toutefois en elle-même un objet d'étude pertinent pour l'étude des groupes finis simples. Les algèbres de Lie disposent en effet d'une classification exhaustive, de laquelle peut être dérivée, en considérant leur groupe d'automorphismes ou groupe de Chevalley, un grand nombre de groupes simples "classiques" de matrices (groupe unitaire, groupe spécial projectif, groupe spécial linéaire, certains groupes orthogonaux). Pour progresser vers cette typologie exhaustive, on s'attachera à étudier les sytèmes de racines d'un espace euclidien et leur groupe de Weyl associées, que l'on combinera à des résultats de réduction sur les $\mathbb{C}$-algèbres de dimension finie dûs à Elie Cartan.

L'approche adoptée tout du long pour comprendre les groupes de Chevalley sera celle développée par Tits des groupes avec une paire (B, N), qui vérifient d'importantes propriétés de structure. Cette vision nous permettra aussi d'établir en définitive la simplicité des groupes de Chevalley.

Une dernière partie sera consacrée à une extension des groupes de Chevalley via leurs homologues tordus, ce afin de retrouver certains groupes simples classiques manquants - tels que les groupes orthogonaux.

Table des matières

I Algèbres de Lie

I.1 Préliminaires

Définition I.1.1 : Une *algèbre de Lie* $\mathfrak{L}$ sur un corps $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel muni d'une loi de composition interne [.] telle que :
(i) [.] est bilinéaire.
(ii) $\forall x \in \mathfrak{L}, [xx] = 0$
(iii) $\forall x, y, z \in \mathfrak{L}^3, [[xy]z] + [[yz]x] + [[zx]y] = 0$
Il suit de la définition que [.] est antisymétrique. Dans le présent mémoire, on ne s'intéressera qu'aux algèbres de Lie de dimension finie. Dans toute la suite, en l'absence de déclaration, $\mathfrak{L}$ est une algèbre de Lie complexe de dimension finie.

Exemple I.1.2 : Si $n \in \mathbb{N}^*$ et V est un $\mathbb{C}$-espace vectoriel de dimension n, $\mathcal{L}(V)$ muni du produit $[u, v] = u \circ v - v \circ u$ est une algèbre de Lie. On peut en vériter montrer que toute algèbre de Lie de dimension finie sur un corps $\mathbb{K}$ se comprend comme un sous-espace de $\mathcal{L}(V)$ où V $\mathbb{K}$-espace vectoriel d'une certaine dimension m : c'est le *théorème d'Ado*.
Dans la suite, nous ne considérerons que ce genre d'algèbres de Lie.

Définition I.1.3 : Soit $\mathfrak{L}$ une $\mathbb{K}$ algèbre de Lie. Une *sous-algèbre* de $\mathfrak{L}$ est un sous-espace vectoriel $\mathfrak{M}$ tel que $[\mathfrak{M}\mathfrak{M}] \subseteq \mathfrak{M}$. Un *idéal* de $\mathfrak{L}$ est un sous-espace vectoriel $\mathfrak{H}$ vérifiant $[\mathfrak{H}\mathfrak{L}] \subseteq \mathfrak{H}$

Définition I.1.4 : Soit $x \in \mathfrak{L}$. On définit *l'adjoint* de x [noté $ad\ x$] comme l'endomorphisme vérifiant :

$$\forall y \in \mathfrak{L},\ ad\ x.y = [xy]$$

Proposition I.1.5 : $x \mapsto ad\ x$ est un morphisme d'algèbres de Lie de $\mathfrak{L}$ dans l'algèbre de Lie associative des endomorphismes de $\mathfrak{L}$, muni du produit canonique $[uv] = u \circ v - v \circ u$

Définition I.1.6 : La *forme de Killing* est l'application (.) de $\mathfrak{L}^2$ dans $\mathbb{K}$ définie par :

$$\forall x, y \in \mathfrak{L},\ (x, y) = \mathrm{tr}(ad\ x \circ ad\ y)$$

On vérifie qu'elle définit une application bilinéaire et symétrique.

Définition I.1.7 : Une algèbre de Lie est dite *simple* si elle est sans idéaux triviaux.

I.2 Décomposition de Cartan

On démontre ici un résultat fort utile pour décomposer les algèbres de Lie en sommes directes d'espaces réguliers :

Théorème I.2.1 : ***(Engel)*** Soit $\mathfrak{g} \subset \mathcal{L}(V)$ une algèbre de Lie telle que tout élément de $\mathfrak{g}$ est nilpotent comme endomorphisme de V . Supposons que V est non trivial. Alors :
(i)$\exists v \in V \mid \forall g \in \mathfrak{g}, g(v) = 0$.

(ii) Il existe une base de V pour laquelle tout élément de $\mathfrak{g}$ est triangulaire strictement supérieur. En particulier, $\mathfrak{g}$ est nilpotent.

Preuve : : (i) Raisonnons par récurrence forte sur la dimension n de $\mathfrak{g}$. Les cas $n = 0$ et $n = 1$ étant triviaux, supposons $dim\mathfrak{g} > 1$.
Soit $\mathfrak{h}$ une sous-algèbre propre de $\mathfrak{g}$ de dimension maximale. Pour tout $x \in \mathfrak{h}$, $ad\ x$ agit sur $\mathfrak{h}$ et $\mathfrak{g}$, donc aussi sur $\mathfrak{g}/\mathfrak{h}$. $ad\ x$ étant nilpotent, toutes ces actions le sont aussi. Par hypothèse de récurrence, on dispose de $v \in \mathfrak{g}/\mathfrak{h}$ annulé par $ad\ x$ pour tout $x \in \mathfrak{h}$. Soit w un représentant de v dans $\mathfrak{g}$. Par maximalité, la sous-algèbre engendrée par $\mathfrak{h}$ et w est $\mathfrak{g}$. Toujours par hypothèse de récurrence, l'espace $W \subset V$ des vecteurs annulés par $\mathfrak{h}$ est non nul. Vu que $[w, \mathfrak{h}] \subset \mathfrak{h}$, il est stable par w. w étant nilpotent, on dispose donc de $v' \in V$ non nul annulé par tout élément de $\mathfrak{g}$.
(ii) Raisonnons par récurrence sur dimV . Par (i), on dispose de $v \in V$ annulé par $\mathfrak{h}$. On projette $\mathfrak{h}$ sur $\mathcal{L}(V/\langle v\rangle)$. Par hypothèse de récurrence, on dispose d'une base de $V/\langle v\rangle$ trigonalisant strictement $\mathfrak{h}$. En considérant des représentants de cette base dans V et en lui adjoignant v, le résultat suit. $\square$

Définition I.2.2 : Une sous-algèbre $\mathfrak{H}$ de $\mathfrak{L}$ est appelée *sous-algèbre de Cartan* si :
(i) $\exists r \in \mathbb{N}^*,\ [\mathfrak{H}]^{(r)} = 0$
(ii) $(\forall h \in \mathfrak{H},\ [xh] \in \mathfrak{H}) \Longrightarrow x \in \mathfrak{H}$
Les algèbres satisfaisant (i) sont dites *nilpotentes*. La propriété (ii) implique que $\mathfrak{H}$ n'est contenue comme idéal dans aucune autre sous-algèbre de $\mathfrak{L}$

On montrera plus tard que toute algèbre de Lie admet des sous-algèbres de Cartan

Notation I.2.3 : Soit $\mathfrak{g}$ une algèbre de Lie. Pour $x \in \mathfrak{g}$, on note :

$$\mathfrak{g}_x^\lambda = \{y \in \mathfrak{g} \mid (ad\ x).y = \lambda y\}$$

le sous-espace caractéristique associé à λ. Notons P_x le polynôme caractéristique de $ad\ x$. On a, si $n = dim\ \mathfrak{g}$:

$$P_x(T) = \sum_{i=0}^{n} a_i(x) T^i$$

où $a_i(x)$ est un polynôme homogène de degré $n - i$ en les éléments d'une base $x_1, ..., x_n$ de $\mathfrak{g}$.

Définition I.2.4 : On appelle *rang de* $\mathfrak{g}$ le plus petit entier l tel que la fonction a_l définie ci-dessus ne soit pas identiquement nulle. Un élément $x \in \mathfrak{g}$ tel que $a_l(x) \neq 0$ sera dit *régulier*.

Remarque I.2.5 : Vu que $a_n = 1$, nous avons $l \leq n$ avec égalité si et seulement si $\mathfrak{g}$ est nilpotente. De plus, étant donné que $(ad\ x).x = [xx] = 0$ pour tout $x \in \mathfrak{g}$, O est valeur propre de tout endomorphisme du type $ad\ x$. Il suit que $a_0 = 0$, donc $l \geq 1$.

Nous aurons par la suite besoin du lemme topologique suivant :

Lemme I.2.6 : Soit $\mathfrak{g}$ une algèbre de Lie. L'ensemble $\mathfrak{g}_r$ des éléments réguliers de $\mathfrak{g}$ est ouvert,

dense et connexe dans $\mathfrak{g}$.
Preuve : On a $\mathfrak{g}_r = \mathfrak{g} \setminus V$ où V est l'espace d'annulation de a_l. $\mathfrak{g}_r$ est donc clairement ouvert. Si l'intérieur de V était non nul, a_l étant polynômiale en plusieurs variables complexes, elle serait identiquement nulle, ce qui contredirait la définition du rang. Enfin, si $x, y \in \mathfrak{g}_r$, la droite complexe D joignant x et y rencontre V en un nombre fini de points. Le plan privé d'un nombre fini de points étant connexe, on en déduit que $D \cap \mathfrak{g}_r$ est connexe, donc x et y sont dans la même composante connexe de $\mathfrak{g}_r$. Il suit que $\mathfrak{g}_r$ est connexe. □

Proposition I.2.7 : Soit $x \in \mathfrak{g}$; Alors :
(a) $\mathfrak{g}$ est la somme directe des espaces $\mathfrak{g}_x^\lambda$.
(b) $\forall \lambda, \mu \in \mathbb{C},\ [\mathfrak{g}_x^\lambda, \mathfrak{g}_x^\mu] \subset \mathfrak{g}_x^{\lambda+\mu}$
(c)g_x^0 est une sous-algèbre de $\mathfrak{g}$.
Preuve : (a) C'est un résultat classique de réduction des endomorphismes.
(b) Soit $y \in g_x^\lambda$, $z \in g_x^\mu$; on montre par récurrence :

$$(ad\ x - \lambda - \mu)^n[yz] = \sum_{p=0}^{n} \binom{n}{p} [(ad\ x - \lambda)^p.y, (ad\ x - \mu)^{n-p}.z]$$

Prenons n suffisamment grand de sorte que tous les termes de droite s'annulent ; on a donc prouvé $[yz] \in \mathfrak{g}_x^{\lambda+\mu}$
(c) Il suffit d'appliquer (b) avec $\lambda = \mu = 0$ □

Théorème I.2.8 : Si x est régulier, g_x^0 est une sous-algèbre de Cartan de $\mathfrak{g}$. Sa dimension est égale au rang l de $\mathfrak{g}$.

Preuve : Montrons tout d'abord que g_x^0 est nilpotente. Par le théorème d'Engel, il suffit de montrer que pour tout $y \in g_x^0$, la restriction de $ad\ y$ à g_x^0 est nilpotente. Notons $ad^1\ y$ cette restriction et $ad^2\ y$ l'endomorphisme induit sur $\mathfrak{g}/\mathfrak{g}_x^0$. On note :

$$U = \left\{ y \in \mathfrak{g}_x^0 \mid ad^1\ y \text{ n'est pas nilpotent} \right\}$$

$$V = \left\{ y \in \mathfrak{g}_x^0 \mid ad^2\ y \text{ inversible} \right\}$$

Les ensembles U et V sont ouverts dans g_x^0. V est non vide, car il contient x. V étant le complémentaire d'une sous-variété algébrique de $\mathfrak{g}_x^0$, il est dense dans $\mathfrak{g}_x^0$.
Supposons donc que U est non vide. Alors U rencontre V, soit donc $y \in U \cap V$. Comme $y \in U$, 0 est valeur propre de $ad^1\ y$ de multiplicité au plus $dim\ \mathfrak{g}_x^0 - 1$. Au passage, on a clairement $l = dim\ \mathfrak{g}$. D'autre part, comme $v \in V$, 0 n'est pas valeur propre de $ad^2\ y$. Par conséquent la multiplicité de 0 comme valeur propre de $ad\ y$ est strictement inférieure à l, ce qui contredit la définition du rang. Donc U est vide et $\mathfrak{g}$ est une algèbre nilpotente.
Montrons désormais que $\mathfrak{g}_x^0$ est égal à son normalisateur $\mathfrak{n}(\mathfrak{g}_x^0)$. On a $ad.z(\mathfrak{g}_x^0) \subset \mathfrak{g}_x^0$ donc en particulier $[zx] \in \mathfrak{g}_x^0$. Par définition de $\mathfrak{g}_x^0$, on dispose de p tel que $(ad\ x)^p[zx] = 0$, ce qui donne $(ad\ x)^{p+1}.z = 0$, soit $z \in \mathfrak{g}_x^0$, d'où le résultat. □

On vient donc de prouver que toute algèbre de Lie $\mathfrak{L}$ admet une sous-algèbre de Cartan $\mathfrak{h}$ et une décomposition du type $\mathfrak{L} = \mathfrak{h} \oplus \sum_\lambda \mathfrak{g}_x^\lambda$ pour un $x \in \mathfrak{L}$ régulier, et que $\mathfrak{h}$ laisse les $\mathfrak{g}_x^\lambda$ invariants. Si $\mathfrak{L}$ est simple, on peut affiner via le théorème suivant :

Théorème I.2.9 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple. Alors il existe $k \in \mathbb{N}^*$, $\mathfrak{H} \subset \mathfrak{L}$ une sous-algèbre de Cartan et $\mathfrak{L}_{r_1}, ..., \mathfrak{L}_{r_k}$ des sous-espaces vectoriels de dimension 1 telles que :
- $\mathfrak{L} = \mathfrak{H} \oplus \mathfrak{L}_{r_1} \oplus \mathfrak{L}_{r_2} \oplus ... \oplus \mathfrak{L}_{r_k}$
- $\forall i \in [\![1, k]\!]\,,\ [\mathfrak{H}\mathfrak{L}_{r_i}] = L_{r_i}$ Une telle décomposition est dite *décomposition de Cartan*

Le théorème I.2.8 nous a permis de construire une sous-algèbre de Cartan. En vérité il nous permet de les obtenir tous :

Définition I.2.10 : Un *automorphisme* de $\mathfrak{g}$ est une application $\theta \in \mathcal{L}(\mathfrak{g})$ telle que :

$$\forall x, y \in \mathfrak{g},\ [\theta(x), \theta(y)] = [x, y]$$

Théorème I.2.11 : Soit $\mathfrak{g}$ une algèbre de Lie. Notons G le *groupe des automorphismes intérieurs* de $\mathfrak{g}$, i.e le sous-groupe de $Aut(\mathfrak{g})$ engendré par les $e^{ad\,y}$, $y \in \mathfrak{g}$. Alors G agit transitivement sur l'ensemble des sous-algèbres de Cartan de $\mathfrak{g}$.

En combinant ceci avec le théorème I.2.9, on a :

Corollaire I.2.12 : La dimension d'une sous-algèbre de cartan de $\mathfrak{g}$ est égale au rang de $\mathfrak{g}$.

Corollaire I.2.13 : Toute sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$ s'écrit sous la forme $\mathfrak{h} = \mathfrak{g}_x^0$ pour un certain $x \in \mathfrak{g}$.

Exemple I.2.14 : Soit $n \in \mathbb{N}^*, \mathfrak{L} = \{M \in \mathcal{M}_n(\mathbb{C}) \mid tr(M) = 0\}$ muni du produit de Lie canonique. On prouve aisément que l'ensemble des matrices diagonales de trace nulle forme une sous-algèbre de Cartan $\mathfrak{H}$. Il vient :

$$\mathfrak{L} = \mathfrak{H} \oplus \sum_{i \neq j} \mathbb{C}E_{ij}$$

Cette décomposition est une décomposition de Cartan.
Preuve : Soit $H \in \mathfrak{H}$. On dispose de $(\lambda_1, ..., \lambda_n) \in \mathbb{C}^n$ tels que $H = diag(\lambda_1, ..., \lambda_n)$. Il vient : $\forall (i, j) \in [\![1, n]\!]\,, i \neq j,\ [HE_{ij}] = HE_{ij} - E_{ij}H = (\lambda_i - \lambda_j)E_{ij}$

I.3 Intermède : Groupes de Weyl

Notation I.3.1 : Dans tout ce qui suit, $\mathfrak{V}$ est un espace euclidien de dimension n. Pour chaque vecteur $r \in \mathfrak{V}$, on note w_r la réflexion par rapport à l'hyperplan orthogonal à r, laquelle s'écrit :

$$\forall x \in \mathfrak{V},\ w_r(x) = x - \frac{2(r, x)}{(r, r)} r$$

Définition I.3.2 : Un sous-ensemble $\Phi \in \mathfrak{V}$ est appelé un système de racines s'il vérifie :

(i) Φ est un ensemble fini de vecteurs non nuls.
(ii) Φ engendre $\mathfrak{V}$
(iii) $\forall r, s \in \Phi, w_r(s) \in \Phi$
(iv) $\forall r, s \in \Phi, \frac{2(r,s)}{(r,r)} \in \mathbb{Z}$
(v) $\forall r \in \phi, \lambda \in \mathbb{R},\ \lambda r \in \phi \Longrightarrow \lambda \pm 1$

Pour Φ un système de racines, on note $W(\phi)$ (ou simplement W) le groupe généré par les réflexions W_r pour $r \in \Phi$. On l'appelle *groupe de Weyl* de Φ. On vérifie aisément que c'est un sous-groupe de $\mathcal{O}_n(\mathbb{R})$, qu'il agit fidèlement sur Φ. Φ étant fini, $W(\Phi)$ l'est donc aussi.

Proposition I.3.3 : Soit Φ un système de racines de $\mathfrak{V}$. Il existe un unique $\Pi \subset \phi$ satisfaisant les propriétés suivantes :
- Π est une famille libre de vecteurs
- Tout élément de Φ est une combinaison linéaire de vecteurs de Π à coefficients tous positifs ou tous négatifs.

Un tel sous-ensemble sera appelé *système fondamental de racines*

Preuve : Munissons $\mathfrak{V}$ d'un ordre total compatible avec l'addition et la multiplication par un scalaire positif. Pour cela, choisissons un sous-ensemble $\mathfrak{V}^+$ de $\mathfrak{V}$ étant stable par les opérations précédentes et vérifiant de plus :

$$\forall v \in \mathfrak{V},\ v \in \mathfrak{V}^+ \text{ ou } -v \in \mathfrak{V}^+ \text{ ou } v = 0$$

Par exemple, choisissons une base $v_1, ..., v_l$ de $\mathfrak{V}$ et prenons pour $\mathfrak{V}^*$ l'ensemble des vecteurs du type $\sum_{i=1}^{l} \lambda_i v_i$ où le premier coefficient non nul est positif. On peut alors munir $\mathfrak{V}$ de l'ordre total $>$ définit par :

$$v1 > v2 \Longleftrightarrow v1 - v_2 \in \mathfrak{V}^+$$

Appelons système positif de racines un sous-ensemble Φ^+ de Φ de la forme $\Phi \cap \mathfrak{V}^+$ pour un ordre total sur $\mathfrak{V}$. Soit donc Φ^+ un tel sous-ensemble de Φ. Alors on dispose [1] de $\Pi \subset \Phi^+$ tel que :
(i) Toute racine de Φ^+ est combinaison linéaire d'élements de Π avec des coefficients positifs.
(ii) Aucun sous-ensemble de Π ne satisfait (i)
Montrons que Π est une famille libre de vecteurs. Pour cela on prouve le lemme suivant :

$$\forall r, s \in \Pi, (r, s) \leq 0$$

Supposons par l'absurde qu'on dispose de $(r, s) \in \Pi$ avec $(r, s) > 0$. Alors $w_r(s) = s - \lambda r$ où $\lambda > 0$.
- Si $w_r(s) \in \Phi^+$, $w_r(s) = \sum_{r_i \in \Pi} \alpha_i r_i$ avec les α_i positifs. D'où $s = \lambda r + \sum_{r_i \in \Pi} \alpha_i r_i$. Le coefficient pour s du terme de droite doit être ≤ 1 sinon $\lambda r + \sum_{r_i \in \Pi} \alpha_i r_i - s \in \mathfrak{V}^+$, d'où s est une combinaison linéaire à coefficients positifs des racines restantes de Π, ce qui contredit la minimalité.

1. Un tel ensembke existe : Φ^+ satisfait ces critères, et il suffit par la suite de raisonner par minimalité

- On procède de même si $-w_r(s) \in \Phi^+$. Le lemme est démontré.

Soit donc $v \in \mathfrak{V}$ s'écrivant $v = \sum \alpha_i r_i = \sum \beta_i s_i$ avec les α_i, β_i positifs, $r_i, s_i \in \Pi$. Alors :

$$(v, v) = \sum_{i,j} \alpha_i \beta_j (r_i, s_j) \leq 0$$

D'où $v = 0$. Donc Π est libre. Il suit que Π est un système fondamental de racines. □

On peut en réalité établir une correspondance exacte entre systèmes de racines et système fondamentaux associés :

Proposition I.3.4 : Tout système positif de racines Φ^+ admet exactement un système fondamental.

Preuve : Soit $\{r_1, ..., r_l\}$ et $\{s_1, ..., s_l\}$ deux systèmes fondamentaux dans Φ^+. Alors :

$$r_i = \sum_{j=1}^{l} \alpha_{ij} s_j \ ; \ s_i = \sum_{j=1}^{l} \beta_{ij} r_j$$

avec $\forall i, j, \ \alpha_{ij} \geq 0, \ \beta_{ij} \geq 0$ et $(\alpha_{ij})_{i,j}, \ (\beta_{ij})_{i,j})$ matrices inversibles. Pour tout i, on dispose de j tel que $\alpha_{ij} \neq 0$. Puisque :

$$\sum_{m=1}^{l} \alpha_{im} \beta_{mk} = 0$$

pour tout $k \neq i$, on a $\beta_{jk} = 0$ (par positivité). Donc $\beta_{ij} \neq 0$. De même, $\alpha_{ik} = 0$ pour $k \neq j$. Quitte à renuméroter $s_1, ..., s_l$, $(\alpha_{ij})_{i,j}$ est diagonale, à coefficients strictement positifs. Par l'axiome I.3.2 (v), $\alpha_{ii} = 1$ pour tout i. Donc $s_i = r_i$. □

Proposition I.3.5 : Soit Φ un système de racines, Π son système fondamental. Alors toute racine de Φ est combinaison linéaire de racines de Π à *coefficients entiers*.

Preuve : Il suffit de le prouver pour $r \in \Phi^+$. Supposons $r \notin \Pi$. Alors $r = \sum_{r_i \in \Pi} \lambda_i r_i$ où au moins deux λ_i sont > 0. On dispose de $r_i \in \Pi$ tel que $(r_i, r) > 0$. Alors :

$$w_{r_i}(r) = r - 2\frac{(r_i, r)}{(r_i, r_i)} r_i$$

$w_{r_i}(r)$ diffère de r de seulement un coefficient lorsqu'il est exprimé dans la base Π. Ainsi au moins un coefficent de $w_{r_i}(r)$ est strictement positif, et donc $w_{r_i}(r) \in \Phi^+$.

Définissons $h(r) = \sum \lambda_i$ (*fonction de hauteur*). Alors $h(w_{r_i})(r) < h(r)$. Ainsi pour chaque racine positive non fondamentale il en existe une autre de hauteur inférieure. Donc les racine positives minimisant h sont les racines fondamentales, sur lesquelles $h = 1$.

Prouvons désormais le résultat souhaité par récurrence sur $h(r)$. Le résultat est vrai pour les racines de taille 1. Si $r \in \Phi^+$ avec $r \notin \Pi$, choisissons r_i comme ci-dessus. Alors, par hypothèse de récurrence, $w_{r_i}(r)$ est une combinaison à coefficients rationnels d'éléments de Π. Donc r aussi, puisque $r = w_{r_i}(r) + \frac{2(r_i,r)}{(r_i,r_i)}$, et que d'autre part $2\frac{(r_i,r)}{r_i,r_i)} \in \mathbb{Z}$ par l'axiome (iv).

Proposition I.3.6 : Soit Φ un système de racines, Π son système fondamental.
(i) Tout élément de Φ est l'image d'un élément de Π par l'action d'un élément de W.
(ii) W est engendré par les réflexions w_r pour $r \in \Pi$

Preuve : (i) Soit W_0 le sous-groupe de W engendré par les réflexions $w_r, r \in \Pi$. Montrons que toute racine $r \in \Phi$ est de la forme $w(s)$ pour un $w \in W_0, s \in \Pi$. Faisons-le par récurrence sur $h(r)$. Si $h(r) > 1$, on dispose de $r_i \in \Pi$ telle que $(r_i, r) > 0$. Ainsi, $w_{r_i}(r) \in \Phi^+$ et $h(w_{r_i}(r)) < h(r)$. Par hypothèse de récurrence, $w_{r_i}(r) = w'(s)$ pour un $w' \in W_0,\ s \in \Pi$.
Donc $r = w_{r_i} w'(s)$ et $w_{r_i} w' \in W_0$. On vérifie que les racines négatives peuvent aussi s'exprimer de même. (ii) Montrons que $W_0 = W$. W étant engendré par les réflexions w_r pour $r \in \Phi$, il suffit de montrer $w_r \in W_0$. Or $r = w(s)$ pour un $s \in \Pi$ et $w \in W_0$. Donc $w_r = w w_s w^{-1}$. En effet :

$$w w_s w^{-1}(x) = w\left(w^{-1}(x) - \frac{2(s, w^{-1}(x))}{(s,s)} s\right) = x - \frac{2(r,x)}{(r,r)} r = w_r(x)$$

Donc $w_r \in W_0$ et donc $W_0 = W$. □

Pour $w \in W$, notons $n(w) = |\Phi^+ \cap w(\Phi^-)|$ le nombre de racines positives transformées par w en racines négatives.

Lemme I.3.7 : Soit $r \in \Pi$. Alors w_r transforme r en $-r$ mais toute autre racines positive en une racine positive.

Preuve : Soit $s \in \Phi^+$ avec $s \neq r$. Alors $s = \sum\limits_{r_i \in \Pi} \alpha_i r_i$ avec les $\alpha_i \geq 0$. On dispose de $r_i \neq r$ tel que $\alpha_i > 0$/ Le coefficient de r_i dans $w_r(s)$ est donc strictement positif, par conséquent $w_r(s) \in \Phi^+$. □

Lemme I.3.8 : Soit $r \in \Pi$ et $w \in W$. Alors :
(i) $n(w_r w) = n(w) + 1$ si $w^{-1}(r) \in \Phi^+$,
(ii) $n(w_r w) = n(w) - 1$ si $w^{-1}(r) \in \Phi^-$,
(iii) $n(w w_r) = n(w) + 1$ si $w(r) \in \Phi^+$,
(iv)$n(w w_r) = n(w) - 1$ si $w(r) \in \Phi^-$,

Preuve : Par le lemme I.3.7, w_r change le signe de seulement deux racines r et $-r$. Par conséquent $n(w_r w) = n(w) \pm 1$ et $n(w w_r) = n(w) \pm 1$. Or $n(w_r w) = n(w) + 1$ si et seulement si $r \in w(\Phi^+)$, ce qui prouve (i) et (ii). De même $n(w w_r) = n(w) + 1$ si et seulement si $w(r) \in \Phi^+$, ce qui prouve (iii) et (iv). □

Théorème I.3.9 : L'expression de longueur minimale $n(w)$ comme produit des réflexions génératrices du groupe de Weyl est égale au nombre de racines positives transformées par w en racines négatives $n(w)$.

Preuve : Soit w un élément de W tel que $l(w) = k$. Alors $w = w_{r_1} w_{r_2} ... w_{r_k},\ r_i \in \Pi$. Par le lemme

I.3.8 :

$$n(w) \leq n(w_{r_1}w) + 1 \leq n(w_{r_2}w_{r_1}w) + 2 \leq ... \leq k$$

Par conséquent $n(w) \leq l(w)$.
Supposons par l'absurde que $n(w) < k$. Par le lemme I.3.8, on dispose de $j \leq k-1$ tel que :

$$w_{r_1}w_{r_2}...w_{r_j}(r_{j+1}) \in \Phi^-$$

Il suit qu'il existe $i \leq j$ tel que $w_{r_{i+1}}...w_{r_j}(r_{j+1}) \in \Phi^+$ et $w_{r_i}w_{r_{i+1}}...w_{r_j}(r_{j+1}) \in \Phi^-$. Vu que w_{r_i} change seulement le signe de r_i et $-r_i$, on a :

$$w_{r_{i+1}}...w_{r_j}(r_{j+1}) = r_i$$

il suit que $w_{r_i} = w_{r_{i+1}}...w_{r_j}w_{r_{j+1}}...w_{r_{i+1}}$, et donc $w_{r_{i+1}}...w_{r_{j+1}} = w_{r_i}...w_{r_j}$.
On peut désormais utiliser cette relation pour raccourcir l'expression originale de w :

$$\begin{aligned} w &= w_{r_1}...w_{r_k} \\ &= w_{r_1}...w_{r_i}w_{r_i}...w_{r_j}w_{r_{j+2}}...w_{r_k} \\ &= w_{r_1}...w_{r_{i-1}}w_{r_{i+1}}...w_{r_j}w_{r_{j+2}}...w_{r_k} \end{aligned}$$

Par conséquent w s'écrit comme produit de $k-2$ réflexions fondamentales. Contradiction. □

Corollaire I.3.10 : Si $w \in W$ satisfait $w(\Pi) = \Pi$, alors $w = 1$.
Preuve : Si $w(\Pi) = \Pi$, alors $w(\Phi^+) = \Phi^+$ et donc $n(w) = 0$. Donc $l(w) = 0$ et donc $w = 1$. □

Proposition I.3.11 : Si Π est un système fondamental dans Φ. Alors, pour tout $w \in W$, $(w(\Pi)$ est un système fondamental de racines dans Φ. Si Π_1, Π_2 sont deux systèmes fondamentaux dans Φ, il existe un unique $w \in W$ tel que $w(\Pi_1) = \Pi_2$.

Preuve : Soit Φ^+ un système de racines positif contenant Π. Alors $\Phi^+ = \phi \cap \mathfrak{V}^+$ pour un certain ordre total sur $\mathfrak{V}$. $w(\mathfrak{V}^+)$ définit aussi un ordre total sur $\mathfrak{V}$ et les racines positives pour cet ordre sont :

$$w(\Phi^+) = \Phi \cap w(\mathfrak{V}^+)$$

$w(\Pi)$ est donc clairement le système fondamental contenu dans $w(\Phi^+)$.
Soit désormais Π_1, Π_2 deux systèmes fondamentaux. Soient Φ_1+, Φ_2^+ leurs systèmes positifs associés. Raisonnons par récurrence sur $n = \left|\Phi_1^+ \cap \Phi_2^+\right|$. Si $n = 0$, $\Phi_1^+ = \Phi_2^+$, et donc $\Pi_1 = \Pi_2$. Supposons désormais $n > 0$.
$\Pi_1 \cap \Phi_2^-$ est non vide. En effet, si toute racine de Π_1 était dans Φ_2^+, alors $\Phi_1^+ \subset \Phi_2^+$. Soit donc $r \in \Pi_1 \cap \Phi_2$. Alors $w_r(\Phi^+)$ est dans l'ensemble de racines obtenu de Φ_1^+ en remplaçant r par $-r$. Il vient :

$$\left|w_r(\Phi_1^+) \cap \Phi_2^-\right| = n - 1$$

Or $w_r(\Pi_1)$ est le système fondamentale contenu dans $w_r(\Phi_1^+)$ donc, par hypothèse de récurrence, il

existe $w' \in W$ tel que $w'w_r(\Pi_1) = \Pi_2$. Donc $w(\Pi_1) = \Pi_2$ avec $w = w'w_r$.
Prouvons enfin l'unicité. Soit w_1, w_2 envoyant Π_1 sur Π_2. Alors $w_1w_2^{-1}$ fixe Π_1, donc par le corollaire I.3.10 $w_1w_2^{-1} = 1$ soit $w_1 = w_2$. □

Corollaire I.3.12 : Le nombre de systèmes fondamentaux dans Φ est égal à l'ordre de W.

Preuve : Soit Π un système fondamental fixé. Alors $w(\Pi)$ donne exactement chaque système fondamental quand w parcourt W. □

Proposition I.3.13 : Soit Φ^+ un système positif dans Φ et Φ^- le système négatif associé. Alors il existe un unique $w_0 \in W$ tel que $w_0(\Phi^+) = \Phi^-$. De plus, w_0 est d'ordre 2.

Preuve : laissée au lecteur.

I.4 Racines d'une algèbre de Lie simple

Définition I.4.1 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple et $\mathfrak{L} = \mathfrak{H} \oplus \mathfrak{L}_{r_1} \oplus \mathfrak{L}_{r_2} \oplus ... \oplus \mathfrak{L}_{r_k}$ une décomposition de Cartan de $\mathfrak{L}$. Ecrivons, pour tout $i \in [\![1, k]\!]$, $\mathfrak{L}_{r_i} = Vect(e_i)$. On définit, pour $i \in [\![1, k]\!]$ et $h \in \mathfrak{H}$:

$$[he_i] = r_i(h)e_i$$

On vérifie que $r_1, ..., r_k$ sont des formes linéaires sur $\mathfrak{H}$, appelées *racines de* $\mathfrak{L}$.

Remarque I.4.2 : $r_1, ...r_k$ sont des formes linéaires distinctes et non nulles.

Lemme I.4.3 : Soit (.) une forme bilinéaire symétrique sur un $\mathbb{K}$-espace vectoriel E de dimension finie. Supposons que (.) soit *non dégénérée* (i.e sa matrice associée dans une base quelconque est inversible). Soit $u \in \mathcal{L}(E, \mathbb{R})$. Alors il existe un unique $h \in E$ tel que :

$$\forall x \in E, u(x) = (h, x)$$

Proposition I.4.4 : Soit $\mathfrak{L}$ une algèbre de Lie *semi-simple*, c'est à dire une algèbre de Lie vérifiant : pour tout $\mathfrak{H}$ idéal de $\mathfrak{L}$, $[\mathfrak{H}\mathfrak{H}] = 0$. Supposons le corps de base de caractéristique nulle. Alors $\mathfrak{L}$ est semi-simple si et seulement si la forme de Killing est non dégénérée.

Par conséquent, les racines d'une $\mathbb{C}$-algèbre de Lie $\mathfrak{L}$ simple peuvent être identifiées à k vecteurs $r_1, ..., r_k \in \mathfrak{H}$. Nous conserverons ces notations pour la suite.

Proposition I.4.5 : Notons $\Phi = \{r_1, ..., r_k\}$. Alors :
- Φ engendre $\mathfrak{H}$
- $\forall \Psi \subset \phi,\ Vect(\Psi) = \mathfrak{H} \Longrightarrow (\forall r \in \Phi, , r \in Vect_{\mathbb{Q}}(\Psi))$ Ainsi : $\forall r, si \in \Phi, (r, s) \in \mathbb{Q}$

Proposition I.4.6 : Notons $\mathfrak{H}_{\mathbb{R}}$ le sous-ensemble de $\mathfrak{H}$ formé des combinaisons linéaires *réelles* des éléments de Φ. Alors :
(i) $\mathfrak{H}_{\mathbb{R}}$ est un espace vectoriel réel de même dimension que $\mathfrak{H}$

(ii) La restriction de la forme de Killing à $\mathfrak{H}_{\mathbb{R}}$ est un produit scalaire.

Il suit de ce qui précède que nous pouvons munir $\mathfrak{H}_{\mathbb{R}}$ d'une structure euclidienne. Au sens des groupes de Weyl, Φ forme un système de racines. En particulier, $\frac{2(r,s)}{(r,r)}$ est un entier pour tous $r, s \in \Phi$. Interprétons cet entier et supposons r et s linéairement indépendants.
Φ étant fini, on dispose de $p, q \in \mathbb{N}$ tels que : $\forall i \in [\![-p, q]\!]\,, ir + s \in \Phi$ et $-(p+1)r + s, (q+1)r + s \notin \Phi$. Nous appelerons une telle suite finie la *r-chaîne de racines selon s.*

La réflexion w_r selon l'hyperplan orthogonal à r permutant les éléments de Φ intervertit plus précisément chaque r-chaîne de racines. En particulier elle transforme $-pr+s$ en $qr+s$. Par conséquent ces deux vecteurs sont symétriques par rapport au dit hyperplan. Il vient :

$$((-pr + s) + (qr + s), r) = 0$$

D'où $\frac{2(r,s)}{(r,r)} = p - q \in \mathbb{Z}$

Nous aurons besoin dans la suite du lemme suivant :

Lemme I.4.7 : Toute racine $r \in \Phi^+$ peut s'exprimer comme somme de racines fondamentales :

$$r = p_{i_1} + p_{i_2} + ... + p_{i_k}$$

de telle manière que $p_{i_1} + p_{i_2} + ... + p_{i_a}$ soit une racine pour tout $a \leq k$.
Preuve : Soit $r = \sum n_i p_i \in \Phi^+$ une racine. $(r, r) = \sum n_i(r, p_i)$, avec les $n_i \geq 0$. Vu que $(r, r) > 0$, il existe p_i tel que $(r, p_i) > 0$ Supposons que r ne soit pas une racine fondamentale. Alors r, p_i sont linéairement indépendants, et r ne peut pas être le premier terme de la p_i-chaîne de racines selon r, donc $r - p_i$ est une racine. En itérant le processus, le résultat suit. □

I.5 Diagrammes de Dynkin

Proposition I.5.1 : Soient p_i, p_j des racines fondamentales [au sens des groupes de Weyl] du système Φ. La quantité :

$$n_{ij} = \frac{4(p_i, p_j)^2}{(p_i, p_i)(p_j, p_j)} = 4\cos^2\theta_{ij}$$

est un entier naturel. Il suit : $\theta_{ij} \in \left\{\frac{pi}{2}, \frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}\right\}$, $\theta_{ij} = \pi$ étant exclu par indépendance linéaire.

Preuve : Rappelons que $\frac{2(p_i,p_j)}{(p_i,p_i)}$ et $\frac{2(p_i,p_j)}{(p_j,p_j)}$ sont des entiers, donc n_{ij} aussi. Puisque $0 \leq \cos^2\theta_{ij} \leq 1$, on a : $4\cos^2\theta_{ij} = 0, 1, 2, 3$ ou 4. Le résultat suit.

Proposition I.5.2 : Mêmes notations. Soient $r_i, r_j \in \Phi$, $i \neq j$. Alors n_{ij} se factorise en deux entiers naturels non tous deux positifs $k_1 = \frac{2(p_i,p_j)}{(p_i,p_i)}$ et $k_2 = \frac{2(p_j,p_i)}{(p_j,p_j)}$. Par conséquent :
(a) Si $n_{ij} = 1$, $k_1 = k_2 = -1$. Ainsi p_i et p_j ont même norme.
(b) Si $n_{ij} = 2$, $\{k_1, k_2\} = -1, -2$. Ainsi $\frac{\|p_i\|}{\|p_j\|} \in \left\{\sqrt{2}, \frac{1}{\sqrt{2}}\right\}$.

(c) Si $n_{ij} = 2$, $\{k_1, k_2\} = -1, -3$. Ainsi $\frac{\|p_i\|}{\|p_j\|} \in \left\{\sqrt{3}, \frac{1}{\sqrt{3}}\right\}$.
Le cas $n_{ij} = 0$ ne donne aucune information sur les longueurs relatives de p_i et p_j.

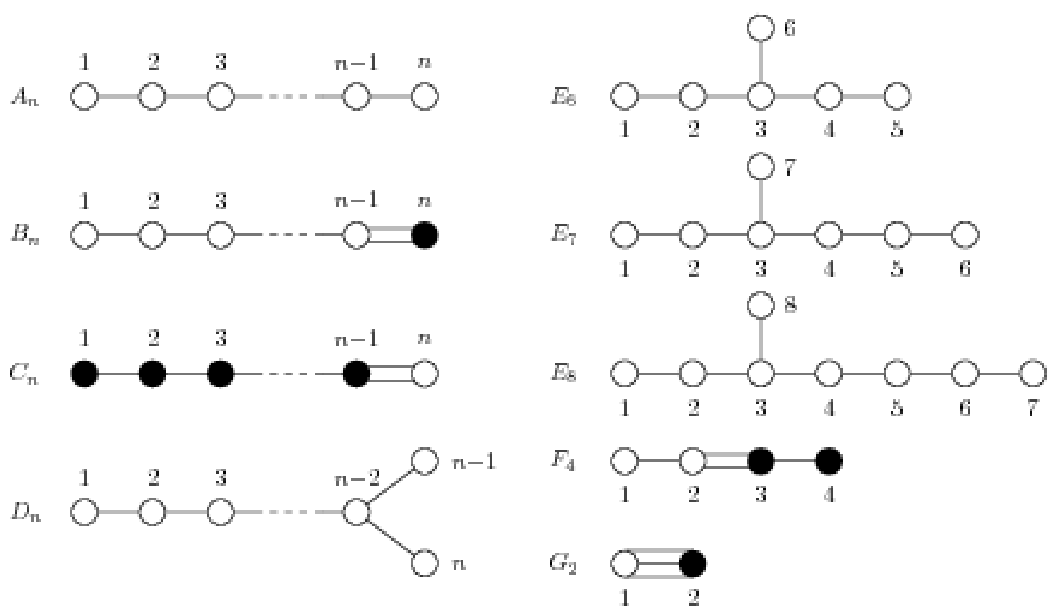
On peut synthétiser le tout sous la proposition suivante :

Proposition I.5.3 : Soient α, β des racines. Alors l'un des cas suivants est réalisé :
(i) α et β sont orthogonaux.
(ii) α et β ont la même norme et forment un angle de $\frac{\pi}{3}$ ou $\frac{2\pi}{3}$.
(iii) α est $\sqrt{2}$ plus long que β ou vice-versa, et α, β forment un angle de $\frac{\pi}{4}$ ou $\frac{3\pi}{4}$.
(iv) α est $\sqrt{3}$ plus long que β ou vice-versa, et α, β forment un angle de $\frac{\pi}{6}$ ou $\frac{5\pi}{6}$.
(v) $\alpha = \pm\beta$

Remarque I.5.4 : Moyennant cela, on observe que toute p_i-chaîne de racines selon p_j a une longueur comprise entre 1 et 4. En effet $\frac{2(p_i,p_j)}{(p_i,p_i)} = p - q$. De ce qui précède, $p - q$ est compris entre 0 et -3. Le même argument montre qu'en fait, toute r-chaîne pour $r \in \Phi$ est de longueur au plus 4. Soit en effet s la première racine d'une r-chaîne. $\frac{2(r,s)}{(r,r)} = p - q$ or $p = 0$ et $p - q$ entre -3 et 0 donc $q \leq 3$.

Définition I.5.5 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple, Φ son système fondamental de racines. Le *diagramme de Dynkin* de $\mathfrak{L}$ est le multigraphe à $|\phi|$ noeuds associés aux racines $p_1, ...p_k \in \Phi$, tel que l'arête $\{i, j\}$ soit de multiplicité n_{ij}.

Au vu de la "rigidité" de la proposition I.5.3, on peut désormais démontrer qu'il existe un nombre fini de diagrammes de Dynkin distincts associés aux algèbres de Lie complexes simples. Ces derniers sont les suivants :



Remarque I.5.6 : Le diagramme de Dynkin ne détermine pas toujours l'algèbre de Lie à isomorphisme près. Considérant le second diagramme, nous dirons qu'il est de type B_n si $\|p_n\| = \frac{1}{\sqrt{2}} \|p_{n_1}\|$, de type C_n sinon.
Il est d'ailleurs possible de récupérer le système de racines entier de l'algèbre à partir du diagramme ; à savoir les longueurs relatives et les angles entre racines fondamentales. Car de la configuration entre racines fondamentales on déduit les réflexions fondamentales w_r, qui engendrent le groupe de Weyl W. Ce dernier agissant transitivement sur Φ, le résultat suit.

I.6 Théorèmes d'isomorphismes

Définition I.6.1 : • Un système de racines est dit *indécomposable* si :

$$\nexists \Phi_1, \Phi_2 \subset \Phi \mid \Phi_1 \sqcup \Phi_2 = \Phi \text{ et } \forall (r,s) \in \Phi_1 \times \Phi_2, (r,s) = 0$$

• Deux systèmes de racines Φ_1 et Φ_2 sont dits dits équivalents si :

$$\exists \alpha : \Phi_1 \to \Phi_2 \text{ bijective }, \lambda > 0 | \forall (r,s) \in \Phi_1,\ (\alpha(r), \alpha(s)) = \lambda(r,s)$$

Proposition I.6.2 : Le système de racines d'une algèbre de Lie complexe simple est indécomposable.
Preuve : Ceci suit du fait que le diagramme de Dynkin d'une algèbre de Lie simple est connexe.

Théorème I.6.3 : Soit Φ un système de racines indécomposable. Alors il existe une $\mathbb{C}$-algèbre de Lie simple qui a un système de racines équivalent à Φ.

Théorème I.6.4 : *[**Théorème d'isomorphisme**]* Soient $\mathfrak{L}, \mathfrak{L}'$ des $\mathbb{C}$-algèbres de Lie simples de sous-algèbres de Cartan $\mathfrak{H}, \mathfrak{H}'$ de même dimension l. Soient $p_1, ..., p_l$ et $p'_1, ..., p'_l$ les systèmes fondamentaux de racines pour $\mathfrak{L}$ et $\mathfrak{L}'$ et :

$$A_{ij} = \frac{2(p_i, p_j)}{(p_i, p_i)}, \quad A'_{ij} = \frac{2(p'_i, p'_j)}{(p'_i, p'_i)}$$

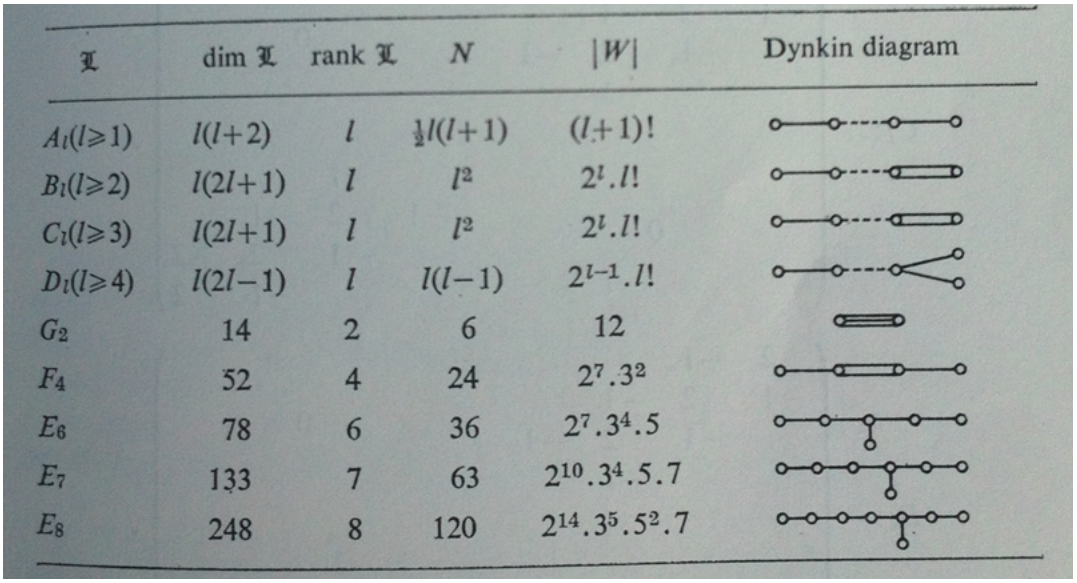
De même, soit :

$$h_{p_i} = \frac{2p_i}{(p_i, p_i)}$$

Choisissons $e_{p_i} \in \mathfrak{L}_{p_i}$, $e_{-p_i} \in \mathfrak{L}_{-p_i}$ tels que $[e_{p_i} e_{-p_i}] = h_{p_i}$. Définissons de même e'_{p_i}, e'_{-p_i} et h'_{p_i}.
Supposons : $\forall (i,j), A_{ij} = A'_{ij}$. Alors il existe un unique isomorphisme $\theta : \mathfrak{L} \to \mathfrak{L}'$ tel que $\forall i,\ \theta(h_{p_i}) = h'_{p_i}$, $\theta(e_{p_i}) = e'_{p_i}$ et $\theta(e_{-p_i}) = e'_{-p_i}$
En particulier, deux $\mathbb{C}$-algèbres de Lie simples aux systèmes de racines équivalents sont isomorphes.

I.7 Description des algèbres de Lie simples

Théorème I.7.1 : On peut désormais exhiber les $\mathbb{C}$-algèbres de Lie simples dans le tableau ci-dessous. On précise, pour chaque algèbre, son *rang*, qui est la dimension commune de ses sous-algèbres de Cartan, le nombre N de racines positives, le cardinal $|W|$ de son groupe de Weyl, et son diagramme de Dynkin.



$\mathfrak{L}$	dim $\mathfrak{L}$	rank $\mathfrak{L}$	N	$\lvert W\rvert$	Dynkin diagram
$A_l(l\geqslant 1)$	$l(l+2)$	l	$\frac{1}{2}l(l+1)$	$(l+1)!$	
$B_l(l\geqslant 2)$	$l(2l+1)$	l	l^2	$2^l.l!$	
$C_l(l\geqslant 3)$	$l(2l+1)$	l	l^2	$2^l.l!$	
$D_l(l\geqslant 4)$	$l(2l-1)$	l	$l(l-1)$	$2^{l-1}.l!$	
G_2	14	2	6	12	
F_4	52	4	24	$2^7.3^2$	
E_6	78	6	36	$2^7.3^4.5$	
E_7	133	7	63	$2^{10}.3^4.5.7$	
E_8	248	8	120	$2^{14}.3^5.5^2.7$	

Remarque I.7.2 : La matrice $(A_{ij})_{i,j}$ définie dans la section VI est appelée *matrice de Cartan de* $\mathfrak{L}$. Le théorème d'isomorphisme nous montre qu'elle caractérise l'algèbre de Lie $\mathfrak{L}$. Les matrices des algèbres de Lie simples sont :

$$A_n = \begin{pmatrix} 2 & -1 & & & & & 0 \\ -1 & 2 & -1 & & & & \\ & -1 & 2 & -1 & & & \\ & & & \ddots & -1 & & \\ & & & -1 & 2 & -1 & \\ & 0 & & & -1 & 2 & -1 \\ & & & & & -1 & 2 \end{pmatrix} \quad B_n = \begin{pmatrix} 2 & -1 & & & & & 0 \\ -1 & 2 & -1 & & & & \\ & -1 & 2 & -1 & & & \\ & & & \ddots & -1 & & \\ & & & -1 & 2 & -1 & \\ & 0 & & & -1 & 2 & -1 \\ & & & & & -2 & 2 \end{pmatrix}$$

$$C_n = \begin{pmatrix} 2 & -1 & & & & & 0 \\ -1 & 2 & -1 & & & & \\ & -1 & 2 & -1 & & & \\ & & & \ddots & -1 & & \\ & & & -1 & 2 & -1 & \\ & 0 & & & -1 & 2 & -2 \\ & & & & & -1 & 2 \end{pmatrix} \quad D_n = \begin{pmatrix} 2 & -1 & & & & & 0 \\ -1 & 2 & -1 & & & & \\ & -1 & 2 & -1 & & & \\ & & & \ddots & -1 & & \\ & & & -1 & 2 & -1 & -1 \\ & 0 & & & -1 & 2 & 0 \\ & & & & -1 & 0 & 2 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} \qquad F_4 = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -2 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

$$E_6 = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix} E_7 = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

$$E_8 = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

Remarque I.7.3 : On peut donner une description des sytèmes de racines indécomposables :

- *type* A_n : Soit $e_0, ..., e_n$ une base orthonormée d'un espace euclidien de dimension $n+1$. Notons $\mathfrak{V}$ le sous-espace des vecteurs du type $\sum_{i=0}^{n} \lambda_i e_i$ avec $\sum_{i=0}^{n} \lambda_i = 0$

Alors l'ensemble $\{e_0 - e_1, e_1 - e_2, ..., e_{n-1} - e_n\}$ forme un système fondamental de racines de type A_n. Le système total de racines est : $\Phi = \left\{e_i - e_j \mid (i,j) \in [\![0,n]\!]^2\ ,\ i \neq j\right\}$

- *type* B_n : Soit $e_1, ..., e_n$ une base orthonormée d'un espace euclidien $\mathfrak{V}$ de dimension n.

L'ensemble $\{e_1 - e_2, e_2 - e_3, ..., e_{n_1} - e_n, e_n\}$ forme un système fondamental de type B_n. Le système complet est $\Phi = \left\{\pm e_i \pm e_j,\ \pm e_i \mid (i,j) \in [\![1,n]\!]^2\ ,\ i \neq j\right\}$

- *type* C_n : Soit $e_1, ..., e_n$ une base orthonormée d'un espace euclidien $\mathfrak{V}$ de dimension n.

L'ensemble $\{e_1 - e_2, e_2 - e_3, ..., e_{n_1} - e_n, 2e_n\}$ forme un système fondamental de type C_n. Le système complet est $\Phi = \left\{\pm e_i \pm e_j,\ \pm 2e_i \mid (i,j) \in [\![1,n]\!]^2\ ,\ i \neq j\right\}$

- *type* D_n : Soit $e_1, ..., e_n$ une base orthonormée d'un espace euclidien $\mathfrak{V}$ de dimension n.

L'ensemble $\{e_1 - e_2, e_2 - e_3, ..., e_{n_2} - e_{n-1}, e_{n-1} - e_n, e_{n_1} + e_n\}$ forme un système fondamental de type C_n. Le système complet est $\Phi = \left\{\pm e_i \pm e_j,\ \mid (i,j) \in [\![1,n]\!]^2\ ,\ i \neq j\right\}$

II Groupes de Chevalley

II.1 Structure multiplicative d'une Algèbre de Lie

Proposition II.1.1 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple et

$$\mathfrak{L} = \mathfrak{H} \oplus \sum_{r \in \Phi} \mathfrak{L}_r$$

une décomposition de Cartan de $\mathfrak{L}$. Notons : $h_r = \frac{2r}{(r,r)}$ la coracine de $r \in \Phi$. Pour chaque $r \in \Phi$, soit e_r un vecteur engendrant $\mathfrak{L}_r$. Si e_r est déjà choisi pour $r \in \Phi^+$, il existe un unique $e_{-r} \in \mathfrak{L}_{-r}$ tel que $[e_r e_{-r}] = h_r$, on le choisit donc tel quel. L'ensemble :

$$\{h_r,\ r \in \Pi; e_r,\ r \in \Phi\}$$

est une base de $\mathfrak{L}$ Les éléments de cette base se multiplient selon les opérations suivantes :
- $\forall r, s \in \Pi,\ [h_r h_s] = 0$
- $\forall r \in \Pi, s \in \Phi,\ [h_r e_s] = A_{rs} e_s$
- $\forall r \in \Phi, [e_r e_{-r}] = h_r$
- $\forall r, s \in \phi,\ r + s \notin \Phi \Longrightarrow [e_r e_s] = 0$

Notation II.1.2 : Si $r, s, r+s \in \Phi$, il suit de $[\mathfrak{L}_r \mathfrak{L}_s] = \mathfrak{L}_{r+s}$ que $[e_r e_s]$ est un multiple scalaire de e_{r+s}. On définit $N_{r,s}$ tel que $[e_r e_s] = N_{r,s} e_{r+s}$. Les scalaires $N_{r,s}$ sont appelés *constantes de structures* de $\mathfrak{L}$

Théorème II.1.3 : Les constantes de structures d'une $\mathbb{C}$-algèbre de Lie simple $\mathfrak{L}$ vérifient les relations suivantes :
(i) $\forall r, s \in \Phi, N_{r,s} = -N_{s,r}$
(ii) $\forall r_1, r_2, r_3 \in \Phi, r_1 + r_2 + r_3 = 0 \Longrightarrow \frac{N_{r_1,r_2}}{(r_3,r_3)} = \frac{N_{r_2,r_3}}{(r_1,r_1)} = \frac{N_{r_3,r_1}}{(r_2,r_2)}$
(iii) $\forall r, s \in \Phi, N_{r,s} N_{-r,-s} = -(p+1)^2$ où p est le plus grand entier tel que $s - pr \in \Phi$
(iv) $\forall r_1, r_2, r_3, r_4 \in \Phi, (r_1 + r_2 + r_3 + r_4 = 0)$ et $(\forall i, j\ r_i \neq -r_j) \Longrightarrow \frac{N_{r_1,r_2} N_{r_3,r_4}}{(r_1+r_2, r_1+r_2)} + \frac{N_{r_2,r_3} N_{r_1,r_4}}{(r_2+r_3, r_2+r_3)} + \frac{N_{r_3,r_1} N_{r_2,r_4}}{(r_3+r_1, r_3+r_1)} = 0$
Preuve : (i) Vu que $[e_r e_s] = -[e_s e_r]$, il est clair que $N_{s,r} = -N_{r,s}$ pour tout $r, s \in \Phi$
(ii) Soient r_1, r_2, r_3 des racines telles que $r_1 + r_2 + r_3 = 0$. Par l'identité de Jacobi :

$$[[e_{r_1} e_{r_2}] e_{r_3}] + [[e_{r_2} e_{r_3}] e_{r_1}] + [[e_{r_3} e_{r_1}] e_{r_2}] = 0$$

Il vient :

$$N_{r_1,r_2}[e_{-r_3} e_{r_3}] + N_{r_2,r_3}[e_{-r_1} e_{r_1}] + N_{r_3,r_1}[e_{-r_2} e_{r_2}] = 0$$

soit :

$$\frac{2N_{r_1,r_2} r_3}{(r_3,r_3)} + \frac{2N_{r_2,r_3} r_1}{(r_1,r_1)} + \frac{2N_{r_3,r_1} r_2}{(r_2,r_2)} = 0$$

Soit, vu que $r_1+r_2+r_3=0$:

$$\left(\frac{N_{r_2,r_3}}{(r_1,r_1)}-\frac{N_{r_1,r_2}}{(r_3,r_3)}\right)r_1+\left(\frac{N_{r_3,r_1}}{(r_2,r_2)}-\frac{N_{r_1,r_2}}{(r_3,r_3)}\right)r_2=0$$

Or r_1, r_2 sont linéairement indépendants, car sinon $r_1=\pm r_2$ et donc $r_3=0$ ou $-2r_1$, contradiction. Par liberté, le résultat suit.
(iv) Soit $r_1,r_2,r_3,r_4\in\Phi$ avec $r_1+r_2+r_3+r_4=0$, et aucune paire n'est égale ou opposée. Par l'identité de Jacobi :

$$[[e_{r_1}e_{r_2}]e_{r_3}]+[[e_{r_2}e_{r_3}]e_{r_1}]+[[e_{r_3}e_{r_1}]e_{r_2}]=0$$

c'est-à-dire :

$$N_{r_1,r_2}N_{r_1+r_2,r_3}+N_{r_2,r_3}N_{r_2+r-3,r_1}+N_{r_3,r_1}N_{r_3+r_1,r_2}=0$$

En utilisant la formule trouvée en (ii) :

$$\frac{N_{r_1+r_2,r_3}}{(r_4,r_4)}=\frac{N_{r_3,r_4}}{(r_1+r_2,r_1+r_2)}$$

et d'autres formules associées par permutation des racines. En remplaçant : $\frac{N_{r_1,r_2}N_{r_3,r_4}}{(r_1+r_2,r_1+r_2)}+\frac{N_{r_2,r_3}N_{r_1,r_4}}{(r_2+r_3,r_2+r_3)}+\frac{N_{r_3,r_1}N_{r_2,r_4}}{(r_3+r_1,r_3+r_1)}=0$ □

Le résultat (iii) est d'un intérêt supérieur. Il suggère que par un choix judicieux des vecteurs e_r, on peut avoir $N_{r,s}=\pm(p+1)$; c'est en effet possible, via le théorème suivant :

Théorème II.1.4 : ***[Théorème de la base de Chevalley]*** Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie et $\mathfrak{L}=\mathfrak{H}\oplus\sum_{r\in\Phi}\mathfrak{L}_r$ une décomposition de Cartan de $\mathfrak{L}$. Alors, pour tout $r\in\Phi$, on peut choisir $e_r\in\mathfrak{L}_r$ tel que :

- $[e_re_{-r}]=h_r$
- $[e_re_s]=\pm(p+1)e_{r+s}$ où p est le plus grand entier tel que $s-pr\in\Phi$

L'ensemble $\{h_r,\ r\in\Pi,\ e_r,\ r\in\Phi\}$ forme une base de $\mathfrak{L}$ appelée *base de Chevalley*.
Preuve : Soit $\mathfrak{L}'=\mathfrak{L}$ une copie de $\mathfrak{L}$ de système fondamental $(p_i')_i$ avec $p_i'=-p_i$. Il est clair que $A'_{ij}=A_{ij}$. Définissons de même $e_{p_i'}=-e_{-p_i}$ et $e_{-p_i'}=-e_{p_i'}$. Alors :

$$[e_{p_i'}e_{-p_i'}]=[e_{p_i}e_{p_i}]=-h_{p_i}=h_{-p_i}=h_{p_i'}$$

Par le théorème d'isomorphisme, on dispose donc de θ automorphisme de $\mathfrak{L}$ tel que :

$$\theta(e_{p_i})=-e_{-p_i}$$
$$\theta(e_{-p_i})=-e_{p_i}$$
$$\theta(h_{p_i})=-h_{p_i}$$

Or θ^2 transforme e_{p_i},e_{-p_i},h_{p_i} en eux-mêmes, donc par unicité de l'isomorphisme, $\theta^2=Id$. Par le lemme I.4.7, chaque racine $r\in\Phi^+$ peut s'écrire sous la forme $r=r_1+r_2+...r_k$ avec $r_1+...+r_a$ racine pour $a\leq k$. Ainsi, $[[e_{r_1}e_{r_2}]...e_{r_k}]\in\mathfrak{L}_r$, colinéaire à e_r, non nul. L'image de cet élément par θ est $[[-e_{-r_1},-e_{-r_2}]...-e_{-r_k}]$, colinéaire à e_{-r}, non nul.

Posons donc $\theta(e_r) = \lambda e_{-r}$. $\theta(e_{-r}) = \lambda^{-1} e_r$ car θ d'ordre 2. Il vient :

$$\theta(\mu e_r) = \mu\lambda e_{-r} = \mu^2\lambda(\mu^{-1} e_{-r})$$

Choisissons $\mu \in \mathbb{C}$ tel que $\mu^2 = \lambda^{-1}$. Alors $\theta(\mu e_r) = -\mu^{-1} e_{-r}$ et $[\mu e_r, \mu^{-1} e_{-r}] = h_r$. Choisissons donc μe_r comme vecteur racine dans $\mathfrak{L}_r$ et $\mu^{-1} e_{-r}$ pour celui de $\mathfrak{L}_{-r}$. Renommons-les e_r, e_{-r}. On a pu donc choisir $e_r \in \mathfrak{L}_r, e_{-r} \in \mathfrak{L}_{-r}$ tel que $[e_r e_{-r}] = h_r$ et $\theta(e_r) = -e_{-r}$.
Vu que $[e_r e_s] = N_{r,s} e_{r+s}$ quand $r, s, r+s \in \Phi$, en appliquant θ :

$$[-e_{-r}, -e_{-s}] = -N_{r,s} e_{-r-s}$$

. Il suit que que $N_{-r,-s} = -N_{r,s}$. Mais $N_{r,s} N_{-r,-s} = -(p+1)^2$, donc $N_{r,s} = \pm(p+1)$

□

Ceci nous permettra de généraliser les structures d'une algèbre de Lie complexe à des algèbres sur un corps quelconque.

II.2 Automorphismes d'algèbres

Définition II.2.1 : Une *dérivation* de $\mathfrak{L}$ est un endomorphisme δ de $\mathfrak{L}$ vérifiant :

$$\forall y, z \in \mathfrak{L},\ \delta([yz]) = [\delta(y), z] + [y, \delta(z)]$$

Proposition II.2.2 : Soit $\mathfrak{L}$ une algèbre de Lie sur un corps $\mathbb{K}$ de caractéristique 0 et δ une dérivation de $\mathfrak{L}$ nilpotente d'indice n. Alors :

$$\exp\delta = 1 + \delta + \frac{\delta^2}{2} + ... + \frac{\delta^{n-1}}{(n-1)!}$$

est un automorphisme de $\mathfrak{L}$.
Preuve : $\exp\delta$ est clairement un endomorphisme bijectif, d'inverse $\exp(-\delta)$. Via la formule de Leibniz :

$$\delta^r[xy] = \sum_{i=0}^{r} \binom{r}{i} [\delta^i x, \delta^{r-i} y]$$
$$\frac{\delta^r}{r!}[xy] = \sum_{i+j=r} \left[\frac{\delta^i}{i!} x, \frac{\delta^j}{j!} y\right]$$

et donc :

$$\begin{aligned}\exp\delta[xy] &= \sum_{r\geq 0} \sum_{i+j=r} \left[\frac{\delta^i}{i!} x, \frac{\delta^j}{j!} y\right] \\ &= \sum_{i\geq 0} \sum_{j\geq 0} \left[\frac{\delta^i}{i!} x, \frac{\delta^j}{j!} y\right] \\ &= [\exp\delta.x, \exp\delta.y]\end{aligned}$$

□

Proposition II.2.3 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple, $\mathfrak{L} = \mathfrak{H} \oplus \sum_{r\in\Phi} \mathfrak{L}_r$ sa décomposition de Cartan, $\{h_r,\ r \in \Pi,\ e_r,\ r \in \Phi\}$ sa base de Chevalley. Alors, pour $r \in \Phi$, l'endomorphisme $ad\ e_r$ est une dérivation nilpotente de $\mathfrak{L}$.
Preuve : • $ad\ e_r.\mathfrak{H} = \mathfrak{L}_r$ • $(ad\ e_r)^2.\mathfrak{H} = 0$ $ad\ e_r.\mathfrak{L}_r = 0$ • $ad\ e_r.\mathfrak{L}_{-r} \subseteq \mathfrak{H}$ $(ad\ e_r)^3.\mathfrak{L}_{-r} = 0$
De plus, si r et s sont deux racines linéairement indépendantes et $q \in \mathbb{N}$ avec $(q+1)r + s \notin \Phi$, $(ad\ e_r)^{q+1}.\mathfrak{L}_s = 0$. Par conséquent $(ad\ e_r)^n = 0$ pour n suffisament grand. □

Notation II.2.4 : Soit $\zeta \in \mathbb{C}$. Alors $ad(\zeta e_r)$ est aussi une dérivation nilpotente de $\mathfrak{L}$. Par conséquent $\exp(\zeta ad.e_r)$ est un automorphisme de $\mathfrak{L}$. Nous notons :

$$x_r(\zeta) = \exp(\zeta ad.e_r)$$

Proposition II.2.5 : L'automorphisme $x_r(\zeta)$ transforme chaque élément de la base de Chevalley en une combinaison linéaire des éléments de la base, les coefficients étant des puissances entières positives de ζ avec des préfacteurs entiers.
Preuve : On a :

$$\begin{aligned} x_r(\zeta).e_r &= e_r \\ x_r(\zeta).e_{-r} &= e_{-r} + \zeta h_r - \zeta^2 e_r \\ x_r(\zeta).h_r &= h_r - 2\zeta e_r \end{aligned}$$

De plus, si r et s sont linéairement indépendants :

$$\begin{aligned} x_r(\zeta).h_s &= h_s - A_{rs}\zeta e_r \\ x_r(\zeta).e_s &= e_s + N_{r,s}\zeta e_{r+s} + \frac{1}{2!}N_{r,s}N_{r,r+s}\zeta^2 e_{2r+s} + ... + \frac{1}{q!}N_{r,s}...N_{r,(q-1)r+s}\zeta^q e_{qr+s} \end{aligned}$$

Posons $M_{r,s,i} = \frac{1}{i!}N_{r,s}...N_{r,(i-1)r+s}$. Il vient :

$$x_r(\zeta).e_s = \sum_{i=0}^{q} M_{r,s,i}\zeta^i e_{ir+s}$$

en définissant $M_{r,s,0} = 1$ et en utilisant le fait que $N_{r,s} = \pm(p+1)$, on voit que :

$$M_{r,s,i} = \pm\frac{(p+1)(p+2)...(p+i)}{i!} = \pm\binom{p+i}{i} \in \mathbb{N}$$

□

Ceci va nous permettre de définir des automorphismes de ce type sur un corps arbitraire.

Proposition II.2.6 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple de base de Chevalley $\{h_r,\ r \in \Pi,\ e_r,\ r \in \Phi\}$. Notons $\mathfrak{L}_\mathbb{Z}$ l'ensemble des combinaisons linéaires de cette base à coefficients dans $\mathbb{Z}$. $\mathfrak{L}_\mathbb{Z}$ est un groupe abélien additif. De la Proposition II.2.5 et du Théorème II.1.4, on vérifie que $\mathfrak{L}_\mathbb{Z}$ est stable par crochet de Lie. $\mathfrak{L}_{\mathbb{Z}}$ est donc une "algèbre de Lie" [2] sur $\mathbb{Z}$.

Soit $\mathbb{K}$ un corps arbitraire. Considérons le produit tensoriel du groupe additif de $\mathbb{K}$ avec celui de $\mathfrak{L}_{\mathbb{Z}}$, et définissons : $\mathfrak{L}_{\mathbb{K}} = \mathbb{K} \otimes \mathfrak{L}_{\mathbb{Z}}$. $\mathfrak{L}_{\mathbb{K}}$ est un groupe abélien additif. Tout élément x de $\mathfrak{L}_{\mathbb{K}}$ peut s'écrire :

$$x = \sum_{r\in\Pi} \lambda_r(1_{\mathbb{K}} \otimes h_r) + \sum_{r\in\Phi} \mu_r(1_{\mathbb{K}} \otimes e_r)$$

où $\lambda_r, \mu_r \in \mathbb{K}$. Ecrivons $\bar{h}_r = 1_{\mathbb{K}} \otimes h_r$ et $\bar{e}_r = 1_{\mathbb{K}} \otimes e_r$. Alors $\mathfrak{L}_{\mathbb{K}}$ est un $\mathbb{K}$-espace vectoriel de base $\left\{\bar{h}_r,\ r \in \Pi,\ \bar{e}_r,\ r \in \Phi\right\}$

Il reste à définir un crochet de Lie sur $\mathfrak{L}_{\mathbb{K}}$.

Proposition II.2.7 : Soient x et y deux éléments de la base de Chevalley de $\mathfrak{L}$. Alors la multiplication sur $\mathfrak{L}_{\mathbb{K}}$ définie par :

$$[1_{\mathbb{K}} \otimes x, 1_{\mathbb{K}} \otimes y] = 1_{\mathbb{K}} \otimes [xy]$$

et étendue par linéarité munit $\mathfrak{L}_{\mathbb{K}}$ d'une structure d'algèbre de Lie. Les constante multiplicatives de $\mathfrak{L}_K$ respectivement à la base $\left\{\bar{h}_r,\ r \in \Pi,\ \bar{e}_r,\ r \in \Phi\right\}$ sont celles de $\mathfrak{L}$ respectivement à $\{h_r,\ r \in \Pi,\ e_r,\ r \in \Phi\}$ interprétées comme éléments du corps premier de $\mathbb{K}$.

On étend désormais les automorphismes de type $x_r(\zeta)$ à $\mathfrak{L}_{\mathbb{K}}$

Définition II.2.8 : Soit $A_r(\zeta)$ la matrice représentant $x_r(\zeta)$ dans la base de Chevalley de $\mathfrak{L}$. On sait que les coefficients de $A_r(\zeta)$ sont de la forme $a\zeta^i$ avec $a \in \mathbb{Z}$ et $i \geq 0$. Soit $t \in \mathbb{K}$ et $\bar{A}_r(t)$ la matrice obtenue par substitution de a avec $a.1_{\mathbb{K}}$ et de ζ avec t. On définit $\bar{x}_r(t)$ comme l'endomorphisme de $\mathfrak{L}_{\mathbb{K}}$ représenté par la matrice $\bar{A}_r(t)$ dans la base $\left\{\bar{h}_r,\ r \in \Pi,\ \bar{e}_r,\ r \in \Phi\right\}$

Proposition II.2.9 : Pour tout $r \in \Phi$ et $t \in \mathbb{K}$, $\bar{x}_r(t)$ est un automorphisme de $\mathfrak{L}_{\mathbb{K}}$.

Dans la suite, ce afin de simplifier les notations, nous noterons h_r pour $\bar{h}_r$, e_r pour $\bar{e}_r$, et ainsi de suite.

Définition II.2.10 : Soit $\mathfrak{L}$ une algèbre de Lie sur le corps $\mathbb{K}$. Le *groupe de Chevalley de type* $\mathfrak{L}$ sur $\mathbb{K}$, noté $\mathfrak{L}(\mathbb{K})$, est le groupe des automorphismes de $\mathfrak{L}$ engendré par les $x_r(t)$ pout $r \in \Phi$ et $t \in \mathbb{K}$.

Proposition II.2.11 : $\mathfrak{L}(\mathbb{K})$ est déterminé à automorphisme près par la $\mathbb{C}$-algèbre de Lie simple et le corps $\mathbb{K}$

Preuve : Montrons que $\mathfrak{L}(\mathbb{K})$ est indépendant du choix de la base de Chevalley de $\mathfrak{L}$.

Soit $\{h_r, r \in \Pi\ ;\ e_r, r \in \Phi\}$ une base de Chevalley de $\mathfrak{L}$. Montrons tout d'abord que toute base de Chevalley de $\mathfrak{L}$ peut être transformé par automorphisme en une autre de la forme $\{h_r, r \in \Pi\ ;\ \pm e_r, r \in \Phi\}$.

Comme deux sous-algèbres de Cartan $\mathfrak{h}$ sont isomorphes, on peut raisonner à $\mathfrak{h}$ fixé. Le théorème d'isomorphisme nous donne aussi que pour deux systèmes fondamentaux de racines, il existe un automorphisme qui transforme l'un en l'autre. De même pour un ensemble de vecteurs e_r donné. Raisonnons donc aussi à Π et $e_r, r \in \Pi$ fixés. Les constantes de structures $N_{r,s}$ étant déterminées au signe près, il

2. appellation abusive, bien entendu, puisque $\mathbb{Z}$ n'est pas un corps...

en est de même pour les $e_r, r \in \Phi$. D'où le résultat préliminaire.
Il est désormais immédiat que le groupe généré par les $x_r(t)$ est indépendant du choix de la base. En effet, si $-e_r$ est choisi au lieu de e_r, on substitue simplement $x_r(t)$ par $x_r(-t)$, son inverse.
Ainsi, le type d'isomorphisme de $\mathfrak{L}(\mathbb{K})$ dépend seulement de $\mathfrak{L}$ et $\mathbb{K}$. □

On s'apercevra par la suite que presque tous les groupes de Chevalley sont simples, et qu'ils contiennent certains groupes simples classiques de matrices. Par exemple, le groupe $A_1(\mathbb{K})$ est isomorphe à $PSL_2(\mathbb{K})$. Toutefois certains groupes classiques de matrices ne sont pas des groupes de Chevalley ; par exemple, les groupes unitaires ou les groupes de matrices orthogonales de second type en dimension paire. Une construction additionnelle à partir des groupes de Chevalley - les "*groupes tordus*" - pourra retrouver la plupart de ceux qui nous échappent. Cette manipulation nous permettra de plus d'obtenir comme groupes tordus certains *groupes exceptionnels*.

On rappelle en guise de préambule les identifications classiques :

Théorème II.2.12 : ***[Ree]*** Soit $\mathbb{K}$ un corps, $n \in \mathbb{N}$. Nous avons les identifications suivantes :
(i) $A_n(\mathbb{K})$ est isomorphe au groupe spécial linéaire $PSL_{n+1}(\mathbb{K})$
(ii) $B_n(\mathbb{K})$ est isomorphe au groupe spécial orthogonal $P\Omega_{2n+1}(\mathbb{K}, f_B)$, où f_B est la forme quadratique $x_0^2 + x_1x_{-1} + x_2x_{-2} + ... + x_nx_{-n}$
(iii) $C_n(\mathbb{K})$ est isomorphe au groupe spécial symplectique $PSp_{2n}(\mathbb{K})$
(iv) $D_n(\mathbb{K})$ est isomorphe au groupe orthogonal $P\Omega_{2n}(\mathbb{K}, f_D)$ où f_D est la forme quadratique $x_1x_{-1} + x_2x_{-2}... + x_nx_{-n}$

Les paragraphes suivants s'intéressent aux propriétés de structure des groupes de Chevalley. Leur progression est en majeure partie ordonnée dans le but de prouver la simplicité de tels groupes.

II.3 Sous-groupes unipotents

Rappel II.3.1 : Soit $G = \mathfrak{L}(\mathbb{K})$ le groupe de Chevalley de type $\mathfrak{L}$ sur $\mathbb{K}$. G est généré par les éléments $x_r(t)$ pour $r \in \Phi$, $t \in \mathbb{K}$. On a : $x_r(t_1).x_r(t_2) = \exp(t_1 ad\ e_r).\exp(t_2 ad\ e_r) = \exp((t_1+t_2) ad\ e_r) = x_r(t_1+t_2)$

Définition II.3.2 : Pour $r \in \Phi$, soit X_r le sous-groupe généré par les éléments $x_r(t)$ pour $t \in \mathbb{K}$. X_r est un sous-groupe de G isomorphe au groupe additif de $\mathbb{K}$. Les X_r sont appelés *sous-groupes de racines* de G.
Soit U le sous-groupe de G généré par les éléments $x_r(t)$ pour $r \in \Phi^+$ et $t \in \mathbb{K}$, et V celui engendré par les $x_r(t)$ pour $r \in \Phi^-$ et $t \in \mathbb{K}$. Alors U et V engendrent clairement G, et U est engendré par les sous-groupes de racines X_r pour $r \in \Phi^+$; de même pour V avec Φ^-.

Définition II.3.3 : On dit qu'un endomorphisme u de $\mathfrak{L}$ est *unipotent* si $(u-1)$ est nilpotent.

Proposition II.3.4 : Soit $u \in U$; alors u est un endomorphisme unipotent.
Preuve : Soit $\mathfrak{L}_{\mathbb{K}} = \mathfrak{H} \oplus \sum\limits_{r\in\Phi} \mathfrak{L}_r$ la décomposition de Cartan de $\mathfrak{L}_{\mathbb{K}}$. On définit $\mathfrak{L}_0 = \mathfrak{H}$ et $\mathfrak{L}_i = \sum\limits_{h(r)=i} \mathfrak{L}_r$ pour $i > 0$. Alors $\mathfrak{L}_{\mathbb{K}} = \sum\limits_i \mathfrak{L}_i$.

Si $r \in \Phi^+$ et $x \in \mathfrak{L}_i$, on montre via la propriété II.2.5 que :

$$x_r(t).x - x \in \sum_{j>i} \mathfrak{L}_j$$

Tout élément de U étant produit d'éléments $x_r(t)$ pour des racines positives r, on a, pour tout $u \in U$, $u.x - x \in \sum_{j>i} \mathfrak{L}_j$. Donc $u - 1$ nilpotent, i.e u unipotent. $\square$

Lemme II.3.5 : Soit $\mathfrak{L}$ une $\mathbb{C}$-algèbre de Lie simple. Soit $y \in \mathfrak{L}$ tel que $ad\ y$ soit nilpotent et θ un automorphisme de $\mathfrak{L}$. Alors :

$$\theta. \exp(ad\ y)\theta^{-1} = \exp(ad\ \theta y)$$

Preuve : Soit $x \in \mathfrak{L}$. Alors :

$$\begin{aligned} \theta. \exp(ad\ y)\theta^{-1}(x) &= \theta \left(\sum_{i=0}^{+\infty} \frac{1}{i!}[y, ...[y, \theta^{-1}(x)]] \right) \\ &= \sum_{i=0}^{+\infty} \frac{1}{i!}[\theta y ...[\theta y, x]] \\ &= \exp(ad\ \theta(y)).x \end{aligned}$$

Il suit que $\theta. \exp(ad\ y)\theta^{-1} = \exp(ad\ \theta y)$. $\square$

Théorème II.3.6 : ***[Formule du commutateur de Chevalley]*** Soit $G = \mathfrak{L}(\mathbb{K})$ un groupe de Chevalley sur un corps arbitraire $\mathbb{K}$ et r, s des racines linéairement indépendantes de $\mathfrak{L}$, u, t des éléments de $\mathbb{K}$. Définissons :

$$[x_s(u), x_r(t)] = x_s(u)^{-1}x_r(t)^{-1}x_s(u)x_r(t)$$

Alors on a :

$$[x_s(u), x_r(t)] = \prod_{i,j>0} x_{ir+js}(C_{ijrs}(-t)^i u^j)$$

où le produit est pris sur toutes les paires d'entiers naturels i, j pour lesquels $ir + js$ est une racine, par ordre croissant avec $i + j$. Les constantes C_{ijrs} sont données par :

$$C_{i1rs} = M_{rsi}$$

$$C_{1jrs} = (-1)^j M_{srj}$$

$$C_{32rs} = \frac{1}{3} M_{r+s,r,2}$$

$$C_{23rs} = -\frac{2}{3} M_{r+s,s,2}$$

Chaque C_{ijrs} est à valeurs dans $\{\pm 1, \pm 2, \pm 3\}$

Remarque II.3.7 : On vérifie que l'on a pas besoin de considérer les paires i, j pour i ou j supérieurs ou égaux à 4. Chaque r-chaîne de racines pour $r \in \Phi$ est en effet de longueur au plus 4.

Rappel II.3.8 : Si Π est le système fondamental de racines associé à un système Φ dans un espace euclidien, h est la *fonction de hauteur* du système Φ qui à $r \in \Phi$ associe sa distance aux générateurs dans Π.

Lemme II.3.9 : L'ordonnancement des racines peut au sein de l'espace euclidien $\mathfrak{V}$ engendré par Φ peut être choisi de tel sorte qu'il soit compatible avec la fonction de hauteur, i.e : $r < s \Longrightarrow h(r) < h(s)$.

Lemme II.3.10 : Soit $r \in \Phi$; Alors $h_r \in \mathfrak{L}_{\mathbb{K}}$ est non nul.

Théorème II.3.11 : Soit $G = \mathfrak{L}(\mathbb{K})$ un groupe de Chevalley, U le sous-groupe de G généré par les X_r pour $r \in \Phi^+$ et U_m le sous-groupe généré par les X_r pour $r \in \Phi^+$ et $h(r) \geq m$ Alors :
(i) U est nilpotent et :

$$U = U_1 \supset U_2 \supset ... \supset U_h \supset 1$$

est une suite centrale pour U, où h est la plus grande hauteur atteinte par une racine de $\mathfrak{L}$
(ii) Tout élément de U s'exprime de manière unique sous la forme $\prod\limits_{r_i \in \Phi^+} x_{r_i}(t_i)$, où le produit est pris sur toutes les racines positives, par ordre croissant.
Les résultats sont similaires pour V en substituant avec des racines négatives
Preuve : • Observons tout d'abord que U_m est normal dans U pour tout $m \geq 1$. En effet, si $s \in \Pi^+$ et $h(s) \geq m$, on a :

$$x_r(t)x_s(u)x_r(t)^{-1} \in U_m$$

pour tout $r \in \Phi^+$ par la formule du commutateur. Donc $x_r(t)U_m x_r(t)^{-1} \subset U_m$. En remplaçant t par $-t$, on voit que : $x_r(t)U_m x_r(t)^{-1} = U_m$. Les $x_r(t)$ générant U pour $t \in \mathbb{K}$ et $r \in \Phi^+$, U_m est normal dans U.
Soit $r, s \in \Phi^+$ avec $h(r) \geq n,\ h(s) \geq m$. Alors :

$$h(ir + js) \geq m + n$$

pour tous $i, j > 0$. Par conséquent :

$$[x_s(u), x_r(t)] \in U_{m+n}$$

via la formule du commutateur. Ceci signifie que les images de $x_r(t)$, $x_s(u)$ par le morphisme naturel commutent dans le groupe U/U_{m+n}. Or les $x_s(u)$ génèrent U_m, et les $x_r(t)$ génèrent U_n. Par conséquent :

$$[U_m, U_n] \subseteq U_{m+n}$$

En particulier, $[U, U_n] \subseteq U_{n+1}$ pour tout n. Par conséquent tout élément de U_n/U_{n+1} commute avec tout élément de U/U_{n+1}, et donc U_n/U_{n+1} est dans le centre de U/U_{n+1}. On dispose donc d'une suite de résolution pour U.
• Tout élément de U est produit d'éléments $x_r(t)$ pour $r \in \Phi^+$. Si dans un tel produit on dispose d'une paire de termes consécutifs $x_r(t), x_s(u)$ avec $r < s$, on utilise la formule :

$$x_s(u)x_r(t) = x_r(t)x_s(u) \prod_{i,j>0} x_{ir+js}(C_{ijrs}(-t)^i u^j)$$

Les termes $x_r(t), x_s(u)$ apparaissent désormais dans leur ordre naturel et les nouveaux termes introduits satisfont $h(ir+js) \geq h(r)+h(s)$. Le processus de réarrangement se termine donc après un nombre finis d'étapes, et tout élément de U s'exprime donc sous la forme :

$$x_{r_1}(t_1)x_{r_2}(t_2)...x_{r_N}(t_N)$$

où $0 < r_1 < r_2 < ... < r_N$ sont les racines positives de$\mathfrak{L}$.

- Prouvons désormais l'unicité. On montre par récurrence descendante sur m que :

$$\prod_{h(s)\geq m} x_s(t_s) = \prod_{h(s)\geq m} x_s(t'_s)$$

implique $t_s = t'_s$, où le produit est pris sur toutes les racines de taille au moins m dans l'ordre croissant. La proposition est triviale si $m = h+1$, où h est la plus grande hauteur atteinte, puisque $U_{h+1} = 1$. Supposons donc le résultat vrai pour $m+1$. Notons :

$$u = \prod_{h(s)\geq m} x_s(t_s) = \prod_{h(s)\geq m} x_s(t'_s)$$

et soit r une racine positive de taille m. Considérons l'élément $u.e_{-r}$ de $\mathfrak{L}_{\mathbb{K}}$. Si $h(s) > m$ et $-r+s \in \Phi$, alors $-r+s \in \Phi^+$, puisque l'ordonnancement des racines est compatible avec la fonction de hauteur. Puisque $h(s) = m$, alors $-r+s$ ne peut pas être une racine, puisqu'elle serait de hauteur 0. Par conséquent :

$$u.e_{-r} = e_{-r} + t_r h_r + x$$

où $x \in \sum\limits_{r\in\Phi^+} \mathfrak{L}_r$. De même :

$$u.e_{-r} = e_{-r} + t'_r h_r + y$$

où $y \in \sum\limits_{r\in\Phi^+} \mathfrak{L}_r$. Mais $\mathfrak{L}_{\mathbb{K}}$ se décompose de la manière :

$$\mathfrak{L}_{\mathbb{K}} = \mathfrak{H} \oplus \sum_{r\in\Phi^+} \mathfrak{L}_r \oplus \sum_{r\in\Phi^-} \mathfrak{L}_r$$

et $h_r \neq 0$ par le Lemme II.3.10. Donc $t_r = t'_r$ et $x = y$. Ainsi :

$$u = \prod_{h(s)=m} x_s(t_s). \prod_{h(s)\geq m+1} x_s(t_s) = \prod_{h(s)=m} x_s(t_s). \prod_{h(s)\geq m+1} x_s(t'_s)$$

Il suit que :

$$\left(\prod_{h(s)=m} x_s(t_s)\right)^{-1} .u = \prod_{h(s)\geq m+1} x_s(t_s) = \prod_{h(s)\geq m+1} x_s(t'_s)$$

Or $t_s = t'_s$ par hypothèse de récurrence, ce qui complète la preuve. □

II.4 Sous-groupes $\langle X_r, X_{-r}\rangle$

Remarque II.4.1 : Dans ce paragraphe, on établit l'existence d'un morphisme du groupe $SL_2(\mathbb{K})$ dans $\langle\ X_r, X_{-r}\ \rangle$ qui permettra d'interpréter l'action de $\langle\ X_r, X_{-r}\ \rangle$ sur certaines sous-modules de $\mathfrak{L}$ comme l'action de $SL_2(\mathbb{C})$ sur un espace de polynômes homogènes à deux variables d'un degré convenable.

Lemme II.4.2 : Soit $\mathbb{K}$ un corps arbitraire. Le groupe $SL_2(\mathbb{K})$ est engendré par les éléments suivants :

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

pour t parcourant $\mathbb{K}$.

Proposition II.4.3 : Il existe un morphisme de $SL_2(\mathbb{C})$ dans le sous-groupe $\langle\ X_r, X_{-r}\ \rangle$ de $G = \mathfrak{L}(\mathbb{C})$ tel que :

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \to x_r(t)$$

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \to x_{-r}(t)$$

Preuve :
Ceci se prouve en montrant que $\langle X_r, X_{-r}\rangle$ agit de la même manière sur $\mathfrak{L}$ que le groupe $SL_2(\mathbb{C})$ sur les sous-espace vectoriels R_q de $\mathbb{C}[x, y]$ formés des polynômes homogènes de degré q, un élément

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

agissant sur R_q par :

$$x \mapsto \alpha x + \gamma y$$
$$y \mapsto \beta x + \delta y$$

et que par conséquent il existe un morphisme envoyant les générateurs de $SL_2(\mathbb{C})$ sur ceux de $\langle X_r, X_{-r}\rangle$.

Il nous reste à généraliser le résultat à un corps $\mathbb{K}$ quelconque :

Théorème II.4.4 : Soit $\mathbb{K}$ un corps quelconque. Alors il existe un morphisme de $SL_2(\mathbb{K})$ dans le sous-groupe $\langle\ X_r, X_{-r}\ \rangle$ de $G = \mathfrak{L}(\mathbb{K})$ tel que :

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \to x_r(t)$$

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \to x_{-r}(t)$$

Nous noterons par la suite Φ_r un tel morphisme. Par commodité, nous admettons les relations présentées dans les résultats qui suivent.

Proposition II.4.5 : Soit $\lambda \in \mathbb{K}$ non nul. Notons :

$$h_r(\lambda) = \Phi_r \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

Alors $h_r(\lambda)$ opère sur la base de Chevalley de $\mathfrak{L}_{\mathbb{K}}$ comme il suit :
- $\forall s \in \Pi,\ h_r(\lambda).h_s = h_s$
- $\forall s \in \Phi,\ h_r(\lambda).e_s = \lambda^{A_{rs}} e_s$

Proposition II.4.6 : Notons :

$$n_r = \Phi_r \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Alors n_r opère sur la base de Chevalley de $\mathfrak{L}_{\mathbb{K}}$ comme il suit :
- $n_r.h_s = h_{w_r(s)}$
- $n_r.e_s = \eta_{r,s} e_{w_r(s)}$, où $\eta_{r,s} = \pm 1$.

Proposition II.4.7 : Les nombres $\eta_{r,s}$ vérifient les propriétés suivantes :
- $\eta_{r,r} = -1$
- $\eta_{r,-r} = -1$
- $\eta_{r,s}\eta_{r,w_r(s)} = (-1)^{A_{rs}}$
- $\eta_{r,s}\eta r, -s = 1$

Proposition II.4.8 : Notons, pour $t \in \mathbb{K}$, :

$$n_r(t) = \Phi_r \begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix}$$

Alors on a les propriétés suivantes :
- $n_r(1) = n_r,\ n_r(-1) = n_r^{-1}$
- $n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t)$
- $h_r(t) = n_r(t)n_r(-1)$

Preuve : Ces résultats suivent des relations correspondantes dans $SL_2(\mathbb{K})$ en utilisant le morphisme Φ_r □

II.5 Sous-groupes diagonal et monomial

Notons H comme le sous-groupe de $G = \mathfrak{L}(\mathbb{K})$ engendré par les éléments de type $h_r(\lambda)$ pour $r \in \Phi$ et $\lambda \in \mathbb{K}$. D'après supra., tout élément de H est un automorphisme de $\mathfrak{L}_{\mathbb{K}}$ qui agit trivialement sur $\mathfrak{H}_{\mathbb{K}}$ et transforme chaque vecteur e_s en un multiple scalaire de lui-même. Les coefficients qui apparaissent de cette manière forme un caractère sur le groupe additif généré par les racines, que l'on s'attache désormais à décrire.

Définition II.5.1 **:** Soit $P = \mathbb{Z}\Phi$ l'ensemble des combinaisons linéaires d'éléments de Φ à coefficients entiers relatifs. P est un groupe abélien libre de base l'ensemble des racines fondamentales $\Pi = \{p_1, ..., p_l\}$. Un morphisme de P dans le groupe multiplicatif $\mathbb{K}^*$ sera appelé $\mathbb{K}$-*caractère de* P.

Les $\mathbb{K}$-caractères de P forment un groupe multiplicatif. De plus, chaque $\mathbb{K}$-caractère χ de P donne lieu à un automorphisme $h(\chi)$ de $\mathfrak{L}_{\mathbb{K}}$ défini par :

$$h(\chi).h_s = h_s, \quad h(\chi).e_s = \chi(s)e_s$$

On note $\tilde{H}$ le sous-groupe des automorphismes de $\mathfrak{L}_{\mathbb{K}}$ engendré par les automorphismes de la forme $h(\chi)$

Exemple II.5.2 **:** Pour $r \in \Phi$, $\lambda \in K^*$, $h_r(\lambda)$ est un automorphisme de $\mathfrak{L}$ dans elle-même. On rappelle que :

$$h_r(\lambda).h_s = h_s, \;\; h_r(\lambda).e_s = \lambda^{A_{rs}} e_s$$

$h_r(\lambda)$ définit donc une application de Φ dans $\mathbb{K}^*$ via $s \mapsto \lambda^{A_{rs}}$. Cette application s'étend en un $\mathbb{K}$-caractère de P. En effet, notons $\chi_{r,\lambda}$ l'application de P dans K^* donnée par :

$$\chi_{r,\lambda}(a) = \lambda^{\frac{2(r,a)}{(r,r)}}$$

Alors $\chi_{r,\lambda}$ est un $\mathbb{K}$-caractère qui prend la valeur $\lambda^{A_{rs}}$ en s.

Proposition II.5.3 **:** Soit $q_1, ..., q_l$ la base de $\mathfrak{H}_{\mathbb{R}}$ duale aux co-racines $h_{p_1}, ..., h_{p_l}$. $q_1, ..., q_l$ sont définies par :

$$(h_{p_i}, q_j) = \delta_{i,j}$$

. La non-singularité de la forme de Killing nous montre que $q_1, ..., q_l$ forme une base de $\mathfrak{H}$. On les appelle *poids fondamentaux* de $\mathfrak{L}$. Par changement de base, toute racine fondamentale p_i est une combinaison linéaire de $q_1, ..., q_l$:

$$p_i = \mu_{i1} q_1 + ... + u_{il} q_l$$

Or $(h_{p_j}, p_i) = \mu_{ij}$. Par conséquent :

$$\mu_{ij} = 2\frac{(p_i, p_j)}{(p_j, p_j)} = A_{ji}$$

et donc les coefficents sont des entiers relatifs.

Proposition II.5.4 **:** On note Q l'ensemble des combinaisons linéaires de $q_1, ..., q_l$ avec des coefficients entiers relatifs. P est un sous-groupe de Q, d'indice fini.

Preuve : Vu que $p_i = \sum_{j=1}^{l} A_{ji} q_j$, on a $|Q : P| = \det(A_{ij})$, via le théorème de la base adaptée, par exemple. D'où le résultat. □

Théorème II.5.5 **:** H est le sous-groupe de G constitué des automorphismes $h(\chi)$ de $\mathfrak{L}_{\mathbb{K}}$ pour lesquels χ est un $\mathbb{K}$-caractère de P pouvant être étendu en un $\mathbb{K}$-caractère de Q.

Preuve : H est engendré par les éléments $\chi_{r,\lambda}$ pour $r \in \Phi$ et $\lambda \in \mathbb{K}^*$. Or, $\chi_{r,\lambda}$ peut être étendu en un

$\mathbb{K}$-caractère de Q via :

$$\chi_{r,\lambda}(a) = \lambda^{\frac{2(r,a)}{(r,r)}}, a \in Q$$

(ceci est bien défini, car $\frac{2(r,a)}{(r,r)} \in \mathbb{Z}$ vu que $\frac{2r}{(r,r)}$ est une co-racine et $a \in Q$). Par conséquent tout élément de H est de la forme $h(\chi)$ pour un χ $\mathbb{K}$-caractère de Q.
Réciproquement, soit χ un $\mathbb{K}$-caractère de Q. Notons $\chi(q_1) = \lambda_1,\ \chi(q_2) = \lambda_2,\ ...,\ \chi(q_l) = \lambda_l$. χ_{p_i,λ_i} prend la valeur λ_i en q_i et la valeur 1 en q_j pour $j \neq i$. En effet :

$$\chi_{p_i,\lambda_i}(q_j) = \lambda_i^{\frac{2(p_i,q_j)}{(p_i,p_i)}} = \lambda^{\delta_{ij}}$$

Il vient que $\chi = \chi_{p_1,\lambda_1}\chi_{p_2,\lambda_2}...\chi_{p_l,\lambda_l}$, d'où $h(\chi) = h(\chi_{p_1,\lambda_1})h(\chi_{p_2,\lambda_2})...h(\chi_{p_l,\lambda_l})$. Donc $h(\chi) \in H$, d'où le résultat. $\square$

On s'intéresse désormais aux relations entre H et les sous-groupes U et V de G. Remarquons tout d'abord que H normalise chaque sous-groupe de racines X_r. En effet :

$$h(\chi)x_r(t)h(\chi)^{-1} = h(\chi)\exp ad\ (te_r)h(\chi)^{-1} = \exp ad\ (\chi(r)te_r)$$

Par conséquent :

$$h(\chi)x_r(t)h(\chi)^{-1} = x_r(\chi(r)t)$$

Et donc $h(\chi)X_rh(\chi)^{-1} = X_r$. Ainsi H normalise U et V. En particulier, UH et VH sont des sous-groupes de G. On pose $B = UH$.

<u>Lemme II.5.6</u> : $UH \cap V = 1$
Preuve : Soit $\theta \in UH \cap V$, considérons son action sur la base de Chevalley :

$$\theta.h_s = h_s + x, \ \text{où} x \in \sum_{r\in\Phi^-} \mathfrak{L}_r$$

Puisque $\theta \in UH$, on a :

$$x \in \mathfrak{H} \oplus \sum_{r\in\Phi^+} \mathfrak{L}_r$$

Or :

$$\mathfrak{L} = \mathfrak{H} \oplus \sum_{r\in\Phi^+} \mathfrak{L}_r \oplus \sum_{r\in\Phi^-} \mathfrak{L}_r$$

et donc $x = 0$, par conséquent $\theta.h_s = h_s$. Posons désormais $\theta.e_s = e_s + y$. Supposons que $s \in \Phi^+$. Alors :

$$y \in \mathfrak{H} \oplus \sum_{r<s} \mathfrak{L}_r$$

puisque $\theta \in V$. Mais de plus :

$$y \in \sum_{r\geq s} \mathfrak{L}_r$$

puisque $\theta \in UH$. Mais on a la décomposition :

$$\mathfrak{L} = \mathfrak{H} \oplus \sum_{\mathfrak{L}_r} \oplus \sum_{r \geq s} \mathfrak{L}_r$$

Donc $y = 0$ et $\theta.e_s = e_s$. Un argument similaire s'applique si $s \in \Phi^-$. Il suit que $\theta = 1$. □

Corollaire II.5.7 : $UH \cap VH = H$
Preuve : $UH \cap VH = (UH \cap V)H = H$ □

Notons désormais N le sous-groupe de G généré par H et les éléments n_r pour $r \in \Phi$. Afin d'étudier la structure de N, nous avons besoin du lemme suivant caractérisant l'action des n_r sur les sous-groupes de racines :

Lemme II.5.8 : Soit $r, s \in \Phi$. Alors :
(i) $n_r.x_s(t).n_r^{-1} = x_{w_r(s)}(\eta_{r,s}t)$
(ii) $n_r X_s n_r{-}1 = X_{w_r(s)}$
Preuve :

$$\begin{aligned} n_r x_s(t) n_r^{-1} &= n_r \exp ad(te_s) n_r^{-1} \\ &= \exp ad(n_r.te_s) \\ &= \exp ad(\eta_{r,s} te_{w_r(s)}) \\ &= x_{w_r(s)}(\eta_{r,s}t) \end{aligned}$$

en utilisant le Lemme II.3.5 et la Proposition II.4.6. □

La propriété la plus importante du sous-groupe N est celle que nous montrons désormais :

Théorème II.5.9 : Il existe un morphisme de N dans W de noyau H pour lequel $n_r \to w_r$ pour $r \in \Phi$. Ainsi H est un sous-groupe normal de N et N/H est isomorphe à W. Si $n \in N, h(\chi) \in H$, on a :

$$nh(\chi)n^{-1} = h(\chi')$$

où $\chi'(r) = \chi(w^{-1}(r))$, w étant l'image de n par le dit morphisme.
Preuve : Par la proposition II.4.6, n_r opère sur la base de Chevalley de $\mathfrak{L}_{\mathbb{K}}$ par :

$$n_r.h_s = h_{w_r(s)} \ , \ \ n_r.e_s = \eta_{r,s} e_{w_r(s)}$$

Par conséquent, n_r transforme $\mathfrak{L}_s$ en $\mathfrak{L}_{w_r(s)}$, par conséquent n_r permute les $\mathfrak{L}_s$ de la même manière que W permute les racines. De plus, chaque élément de H transforme les espaces $\mathfrak{L}_s$ en lui-même. Il existe donc un morphisme ϕ de N dans W qui envoie n_r sur w_r et contient H dans son noyau.
Montrons désormais que H est un sous-groupe distingué de N. Soit $n \in N$ et $h(\chi) \in H$. On a :

$$\begin{aligned} nh(\chi)n^{-1}.h_s &= nh(\chi).(n^{-1}h_s) = n.(n^{-1}h_s) = h_s \\ nh(\chi)n^{-1}.e_s &= nh(\chi).(\eta e_{w^{-1}(s)}) \end{aligned}$$

Où w est l'image de n par ϕ et $\eta = \pm 1$. Par conséquent :

$$\begin{aligned} nh(\chi)n^{-1}.e_s &= \eta\chi(w^{-1}(s))n.e_{w^{-1}(s)} \\ &= \eta\chi(w^{-1}(s))\eta^{-1}e_s \\ &= \chi'(s)e_s \end{aligned}$$

où $\chi'(s) = \chi(w^{-1}(s))$. On a donc :

$$nh(\chi)n^{-1} = h(\chi')$$

Donc H est distingué dans N.
On dispose donc d'un morphisme de N/H dans W pour lequel n_rH s'envoie sur w_r. Montrons que c'est un isomorphisme. Soit $r, s \in \Phi$. Alors :

$$\begin{aligned} n_r n_s n_r^{-1} &= n_r x_s(1)x_{-s}(-1)x_s(1)n_r^{-1} \text{ par la proposition II.4.8} \\ &= x_{w_r(s)}(\eta_{r,s})x_{w_r(-s)}(-\eta_{r,-s})x_{w_r(s)}(\eta_{r,s}) \text{ par le Lemme II.5.8} \\ &= x_{w_r(s)}(\eta_{r,s})x_{-w_r(s)}(-\eta_{r,s}^{-1})x_{w_r(s)}(\eta_{r,s}) \text{ par la Proposition II.4.7} \\ &= n_{w_r(s)}(\eta_{r,s}) \\ &= h_{w_r(s)}(\eta_{r,s})n_{w_r(s)}, \text{ toujours par Prop. II.4.8} \end{aligned}$$

Puisque $h_{w_r(s)}(\eta_{r,s}) \in H$, on a :

$$n_rH.n_sH.(n_rH)^{-1} = n_{w_r(s)}H$$

Or $n_r^2 = h(-1) \in H$, donc $(n_rH)^2 = H$. Or, rappelons que W est un groupe libre défini par les générateurs $w_r, r \in \Phi$, quotienté par les relations $w_r^2 = 1$ et $w_r w_s w_r^{-1} = w_{w_r(s)}$. Par conséquent, il existe un morphisme de W dans N/H pour lequel w_r s'envoie sur n_rH. Vu que c'est l'application réciproque de ϕ, c'est un isomorphisme. Par conséquent N/H est isomorphe à W. □

Corollaire II.5.10 : (i) $N \cap \tilde{H} = H$
(ii) $U \cap N = 1$
(iii) $UH \cap N = H$
Preuve : (i) Soit $n \in N \cap \tilde{H}$. Vu que $n \in \tilde{H}$, on a $n.\mathfrak{L}_s = \mathfrak{L}_s$ pour tout $s \in \Phi$. Donc n est dans le noyau du morphisme envoyant N sur W, par conséquent $n \in H$.
(ii) Soit $\theta \in U \cap N$. On a $\theta.e_s = \lambda e_{w(s)}$ où $\lambda \in \mathbb{K}^*$ et $w \in W$ image de θ par le morphisme de N vers W. Or, on peut écrire $\theta.e_s = e_s + x$ avec $x \in \mathfrak{H} \oplus \sum_{r>s} \mathfrak{L}_r$ puisque $\theta \in U$.
Il suit que $x = 0$, $\lambda = 1$ et $w(s) = s$). Ceci est valide pour tout $s \in \Phi$, par conséquent $w = 1$. Ainsi $\theta \in H$. Or $U \cap H = 1$, donc $\theta = 1$ et $U \cap N = 1$.
(iii) $UH \cap N = (U \cap N)H = H$ □

II.6 Paire (B, N) d'un groupe

Définition II.6.1 : Une paire de sous-groupes B, N d'un groupe G est appelée une paire (B, N) si les axiomes suivants sons satisfaits :
(i) G est engendré par B et N.
(ii) $B \cap N$ est un sous-groupe normal de N.
(iii) Le groupe $W = N/B \cap N$ est engendré par un ensemble d'éléments $w_i, i \in I$, vérifiant $w_i^2 = 1$
(iv) Si $n_i \in N$ s'envoie sur w_i via la projection canonique de N dans W, et si n est un élément quelconque de N :

$$Bn_iB.BnB \subseteq Bn_inB \cup BnB$$

(v) Si n_i est défini comme ci-dessus, alors $n_iBn_i \neq B$

Proposition II.6.2 : Le groupe de Chevalley $G = \mathfrak{L}(\mathbb{K})$ dispose d'une paire (B, N).

Preuve : On montre que les sous-groupes de G précédemment dénommés B et N satisfont les axiomes ci-dessus. On sait que $B \cap N = H$, que H est normal dans N et que N/H est isomorphe au groupe de Weyl W. Le groupe de Weyl est engendré par les réflexions fondamentales $W_r, r \in \Pi$, on prend ces dernières comme les involutions génératrices de l'axiome 3. On peut montrer :

$$\forall r \in \Pi, Bn_rB.BnB \subseteq Bn_rnB \cup BnB$$

Si $r \in \Pi$, $X_r \subseteq B$ mais $n_rX_rn_r$ n'est pas dans B. Donc $n_rBn_r \neq B$. Enfin, G est engendré par B et N.
En effet, G est engendré par les sous-groupes X_r, et chaque racine r est de la forme w_{r_i} pour un certain $w \in W$ et $r_i \in \Pi$. Soit n élément de N s'envoyant sur $w \in W$ par le morphisme. Alors :

$$X_r = X_{w(ri)} = nX_{r_i}n^{-1}$$

par le lemme II.5.8. Donc X_r est dans le sous-groupe généré par B et N. Ainsi, G admet une paire (B, N).

Proposition II.6.3 : Soir G un groupe avec une paire (B, N). Alors :
(i) $G = BNB$
(ii) Pour tout sous-ensemble J de I, soit W_J le sous-groupe de W engendré par les éléments w_j pour $j \in J$, et N_J le sous-groupe de N s'envoyant sur W_J via la projection canonique. Alors $P_J = BN_JB$ est un sous-groupe de G.
Preuve : Prouvons (ii) : BN_JB est stable par inversion, montrons qu'il l'est par multiplication. Soit $n \in N_J$. Ecrivons $n = n_1n_2...n_k$ où chaque n_i s'envoie sur un générateur w_i dans W. Alors :

$$\begin{aligned} nBN_JB &= n_1n_2...n_KBN_JB \\ &\subseteq n_1n_2...n_{k-1}BN_JB \subseteq ... \subseteq BN_JB \end{aligned}$$

en répétant l'axiome II.6.1 (iv). Donc :

$$N_J B N_J B \subseteq B N_J B$$

il suit que $BN_JB.BN_JB \subseteq BN_JB$, donc BN_JB est un sous-groupe de G.
Prenons désormais J=I. Alors BNB est un sous-groupe de G contenant N et B, qui engendrent G, donc $G = BNB$ □

Proposition II.6.4 : Soit G un groupe avec une paire (B, N). Soit n, n' des éléments de N. Alors $BnB = Bn'B$ si et seulement si n et n' s'envoie sur le même élément de W.
Preuve : Chaque élément de W est produit de générateurs $w_i, i \in I$. Soit $l(w)$ sa distance aux dits générateurs. Supposons $BnB = Bn'B$, avec n, n' s'envoyant sur w, w'. Sans perte de généralités, $l(w) \leq l(w')$. Montrons que $w = w'$ par récurrence sur $l(w)$.
Si $l(w) = 0$, $w = 1$ et $BNB = B$. Donc $Bn'B = B$ et donc $n' \in B \cap N$ d'où $w' = 1$. Supposos désormais $l(w) > 0$. Alors $w = w_i w''$ où $i \in I$ et $l(w'') = l(w) - 1$. Soient n_i, n'' des éléments de n s'envoyant sur w_i, w''. Alors :

$$n_i n'' B \in Bn'B$$

Par l'axiome II.6.1 (iv), $n''B \subseteq n_i Bn'B \subseteq Bn_i n'B \cup Bn'B$, d'où $Bn''B = Bn_i n'B$ ou $Bn''B = Bn'B$. Par hypothèse de récurrence, $w'' = w_i w'$ ou $w'' = w'$. Le second cas est impossible car $l(w'') < l(w')$. Donc $w'' = w_i w'$, soit $w' = w_i w'' = w$. □

Proposition II.6.5 : Soit G un groupe avec une paire (B, N) et $w_i, i \in I$ un des générateurs de W. Soit $w \in W$ tel que $l(w_i w) \geq l(w)$. Soit n_i, n des antécédents dans N. Alors $Bn_iB.BnB \subseteq Bn_i nB$.
Preuve : Raisonnons par récurrence sur $l(w)$. Si $l(w) = 0$, $w = 1$ et le résultat est clair. Supposons $l(w) > 0$. Alors $w = w'w_j$ avec $l(w') = l(w) - 1$.
Raisonnons par l'absurde ; Alors, par l'axiome II.6.A (iv), $Bn_iB.BnB \cap BnB \neq \emptyset$. Soit $n', n_j \in N$ s'envoyant sur w_j, w'. Alors :

$$n_i Bn \cap BnB \neq \emptyset$$

et donc $n_i Bn' \cap BnBn_j \neq \emptyset$. Vu que $l(w_i w') \geq l(w')$, par hypothèse de récurrence :

$$n_i Bn' \subseteq Bn_i n'B$$

et donc $Bn_i n'B \cap BnBn_j \neq \emptyset$. Il suit de BN (iv) que $BnB.Bn_jB \subseteq Bnn_jB \cup BnB$. Donc $Bn_i n'B$ intersecte Bnn_jB ou BnB. Par la Proposition II.6.4, $w_i w' = ww_j$ ou $w_i w' = w$. Le premier cas donne $w_i w' = w'$ soit $w' = 1$ ce qui contredit BN (v). Le second donne $w_i w = w'$, qui implique $l(w_i w) \leq l(w)$, contradiction. □

Proposition II.6.6 : Reprenons les hypothèses supra. Alors, si $l(w_i w) \leq l(w)$, $Bn_iB.BnB \cap BnB \neq \emptyset$.
Preuve : Par BN (iv), $n_i B_i \subseteq B \cup Bn_i B$. Vu que $n_i Bn_i \neq B$, $n_i Bn_i \cap Bn_i B \neq \emptyset$. Donc $n_i B \cap Bn_i Bn_i \neq \emptyset$, d'où à fortiori $n_i Bn \cap Bn_i Bn_i n \neq \emptyset$
Vu que $l(w_i.w_i w) \geq l(w_i w)$, alors par la Proposition II.6.5 $n_i Bn_i B \subseteq BnB$. Donc $n_i Bn$ intersecte

BnB et le résultat suit. $\square$

<u>Corollaire II.6.7</u> : Si $l(w_i w) < l(w)$, $n_i \in BnBn^{-1}B$

<u>Proposition II.6.8</u> : Soit G un groupe avec une paire (B,N) et $n \in N$ s'envoyant sur $w \in W$. Ecrivons $w = w_{i_1}w_{i_2}...w_{i_k}$ où $l(w) = k$. Soit $J = \{i_1, i_2, ..., i_k\}$. Alors les trois sous-groupes de G suivants sont égaux :
(i) $\langle B, n\rangle$
(ii) $\langle B, nBn^{-1}\rangle$
(iii) $P_J = BN_JB$
Preuve : On a $n = n_{i_1}n_{i_2}...n_{i_k}$ où $n_{i_\alpha} \in N$ correspond à $w_{i_\alpha} \in W$. Chaque n_{i_α} est dans N_J, donc $n \in N_J$. On a donc les inclusions :

$$\langle B, nBn^{-1}\rangle \subseteq \langle B, n\rangle \subseteq P_J$$

Or P_J, est généré par B et les éléments $n_{i_1}, ..., n_{i_k}$. Puisque $l(w_{i_1}w) < l(w)$, on a, par le corollaire II.6.7, $n_{i_1} \in \langle B, nBn^{-1}\rangle$. Puisque $l(w_{i_2}w_{i_1}w) < l(w_{i_1}w)$, on a :

$$n_{i_2} \in \langle B, n_{i_1}nBn^{-1}n_{i_1}^{-1}\rangle \subseteq \langle B, nBn^{-1}\rangle$$

par un argument similaire, chacun des n_{i_k} est dans $\langle B, nBn^{-1}\rangle$. Donc P_J est inclus dans $\langle B, nBn^{-1}\rangle$ et le résultat suit. $\square$

<u>Proposition II.6.9</u> : Soit G un sous-groupe avec une paire (B,N). Alors les sous-groupes P_J sont les seuls sous-groupes de G contenant B.
Preuve : Soit M un sous-groupe de G contenant B. M peut s'écrire comme union d'ensemble du type BnB. Il suit de la Proposition II.6.3 que chacun de ces ensembles contient un élément de N. Par conséquent M est engendré par B et un certain ensemble d'éléments de N. Soit $n_\alpha \in N$. Par la Proposition II.6.8, $\langle B, n_\alpha\rangle = P_{J_\alpha}$, pour un bon choix de $J_\alpha \subset I$. M est donc engendré par des P_{J_α} pour une famille de (J_α). Il suit que $M = P_J$ pour $J = \bigcup J_\alpha$. $\square$

<u>Théorème II.6.10</u> : Soit G un groupe avec une paire (B,N). Alors tout sous-groupe P_J de G est égal à son normalisateur. De Plus, deux sous-groupes distincts P_J, P_I, ne peuvent pas être conjugués dans G.
Preuve : Le normalisateur $\mathfrak{n}(P_J)$ est engendré par B et des éléments de N. Soit $n \in N \cap \mathfrak{n}(P_J)$. Alors :

$$\left\langle\ B, n\ \right\rangle = \left\langle\ B, nBn^{-1}\ \right\rangle \subseteq P_J$$

par la proposition II.6.8. Ainsi $n \in P_J$, et donc $P_J = \mathfrak{n}(P_J)$.
Supposons désormais que P_J et P_K sont conjugués dans G. Ecrivons $gP_Jg^{-1} = P_K$ avec $g = bnb'$. Alors $nP_Jn^{-1} = P_K$. Donc :

$$\left\langle\ B, n\ \right\rangle = \left\langle\ B, nBn^{-1}\ \right\rangle \subseteq P_K$$

Toujours par II.6.8. Donc $n \in P_K$, et donc $P_K = P_J$. Deux sous-groupes distincts P_J, P_K sont donc non conjugués. $\square$

Théorème II.6.11 : Soit G un groupe avec une paire (B, N). Alors les sous-groupes P_J, pour des sous-ensembles J, K de I distincts, sont distincts. De plus, on a : $P_J \cap P_K = P_{J\cap K}$

Preuve : Il est nécessaire de montrer dans un premier temps que les éléments w_i pour $i \in I$ forment un système minimal de générateurs de W. Supposons par l'absurde que l'on dispose d'un $j \in I$ tel que W soit engendré par les $w_i,\ i \in I \setminus j$. Alors G admet une paire (B, N) avec I remplacé par $I \setminus j$, les axiomes BN 1-5 étant vérifiés. Soit $w_j = w_{i_1}w_{i_2}...w_{i_k},\ i_\alpha \in I \setminus j$ une expression de longueur minimale de w_j en fonction des autres générateurs. Soit n_j un élément de N correspondant à w_j. Ecrivons $J = i_1, i_2, ..., i_k$. Par la proposition II.6.8, on a $\langle\ B, n_j\ \rangle = BN_JB$. Or, $BN_JB = B \cup Bn_jB$. Par la proposition II.6.4, ceci implique $W = \{1, w_j\}$, contradiction. Donc les w_i forment un ensemble minimal de générateurs.

Soit J, K des sous-ensembles de I. $P_J \cap P_K$ est un sous-groupe de G contenant B, donc $P_J \cap P_K = P_L$ pour un sous-ensemble $L \subset I$ par Proposition II.6.9. On a $P_{J\cap K} \subseteq P_L$. Raisonnons par l'absurde et supposons $P_{J\cap K} \neq P_L$. Alors $L \not\subset J \cap K$, supposons donc sans perte de généralités $L \not\subset J$.

On sait que $P_L \subset P_J$ et donc $N_L \subset N_J$ par II.6.4 toujours. Ainsi $W_L \subset W_J$. Soit $i \in I \setminus J$. Alors $w_i \in W_L$, et donc $w_o \in W_J$. Mais cela veut dire que w_i s'exprime en fonction des générateurs restants de W, contradiction. Ainsi $P_J \cap P_K = P_{J\cap K}$. $\square$

II.7 Simplicité des groupes de Chevalley

Théorème II.7.1 : Soit G un groupe avec une paire (B, N) satisfaisant les conditions suivantes :

(i) $G = D(G)$

(ii) B est résoluble

(iii) $\bigcap gBg^{-1} = 1$

(iv) L'ensemble I ne peut pas être décomposé en deux sous-ensembles J, K non vides, complémentaires, tel que w_j commute avec w_k pour tout $j \in J, k \in K$.

Alors G est un groupe simple.

Preuve : Soit G_1 un sous-groupe normal de G. Alors G_1B est un sous-groupe de G contenant B, donc $G_1B = P_J$ pour un certain sous-ensemble par la proposition II.6.9. Posons $K = I \setminus J$. Soit $j \in J, k \in K$ et $n_j, n_k \in N$ correspondant à w_i, w_k par le morphisme canonique. Si l est la fonction de longueur donnant la plus courte distance aux générateurs d'un élément, $l(w_jw_k) > l(w_k)$. Par Proposition II.6.5 on a :

$$Bn_jB.Bn_kB \subseteq Bn_jn_kB$$

Or $G_1B = P_J = BN_JB$, et donc $Bn_jB \cap G_1 \neq \emptyset$. G_1 étant un sous-groupe normal de G, ceci implique : $n_kBn_jBn_k \cap G_1 \neq \emptyset$. Mais :

$$n_kBn_jBn_k \subseteq n_kBn_j.n_kB \subseteq Bn_k.n_jB \cap Bn_k.n_j.n_kB$$

par l'axiome 4 des paires (B,N). Et donc :

$$Bn_j.n_kB \cap G_1 \neq \emptyset \text{ ou } Bn_j.n_k.n_kB \cup G_1 \neq \emptyset$$

La dernière condition impliquerait que $n_j.n_k \in N$, où $n_k \in N_J$ et $w_k \in W_J$. Ceci contredit le fait, montré dans la preuve du Théorème II.6.11, que les éléments w_i forme un ensemble minimal de générateurs pour W. Ainsi :

$$Bn_j.n_kB \cap G_1 \neq \emptyset$$

Ce qui veut dire que $n_k.n_j.n_k \in N_J$ et $w_kw_jw_k \in W$. Donc :

$$w_kw_jw_k \in W \cap W_{j,k} = W_j$$

Donc $w_kw_jw_k$ vaut 1 ou w_j. Le premier cas implique $w_j = 1$, ce qui est impossible. Donc $w_kw_jw_k = w_j$. Donc pour tout $j \in J, k \in \mathbb{K}$, $w_kw_j = w_jw_k$. Comme I ne se décompose pas en deux sous-ensembles complémentaires, non vides vérifiant cela, J ou K est vide.
Supposons que K est vide. Alors $J = I$ et $G_1B = G$. Donc :

$$G/G_1 = G_1B/G_1 \simeq B/G_1 \cap B$$

Or B est résoluble donc G/G_1 est résoluble aussi. Mais le fait que G coïncide avec son groupe dérivé implique que la suite de résolution de G n'a pas de facteur non trivial. Donc $G_1 = G$
Supposons désormais que J est vide. Alors $G_1B = B$ et donc G_1 est contenu dans B. Comme G_1 est normal dans G on a :

$$G_1 \subseteq \bigcap_{g\in G} gBg^{-1} = 1$$

Donc $G_1 = 1$. Ainsi, G est simple.

Nous aurons besoin du petit lemme utilitaire suivant :

Lemme II.7.2 : (i) Soit $r \in \Phi$ et $t \in \mathbb{K}^*$. Alors il existe un $\mathbb{K}$-caractère de Q tel que $\chi(r) = t^2$.
(ii) Il existe un $\mathbb{K}$-caractère de Q tel que $\chi(r) = t$, sauf si $\mathfrak{L} = A_1$ ou $\mathfrak{L} = C_l$ et r est une racine longue
Preuve : (i) On rappelle que l'on définit le $\mathbb{K}$-caractère $\chi_{r,t}$ par :

$$\forall a \in Q,\ \chi_{r,t}(a) = t^{\frac{2(r,a)}{(r,r)}}$$

Il vient : $\chi_{r,t}(r) = t^2$.
(ii) laissée au lecteur. $\square$

Théorème II.7.3 : (i) Soit $\mathfrak{L}$ une algèbre de Lie simple sur $\mathbb{C}$ et $\mathbb{K}$ un corps arbitraire. Alors le groupe de Chevalley $G = \mathfrak{L}(\mathbb{K})$ est simple, exception faite de $A_1(\mathbb{F}_2)$, $A_1(\mathbb{F}_3)$, $B_2(\mathbb{F}_2)$, $G_2(\mathbb{F}_2)$.
(ii) Tout groupe de Chevalley a un centre trivial.
Preuve : On rappelle que B est le produit semi-direct de U par H. H est un groupe abélien et U est nilpotent d'après le théorème II.3.11. On vérifie donc que B est résoluble. De plus, l'ensemble de générateurs distingués w_i de W ne peut pas être décomposé en deux sous-ensembles qui commutent vu que $\mathfrak{L}$ est simple (Proposition I.6.2). Il suffit donc de prouver :

$$G = D(G) \text{ et } \cap_{g\in G}\ gBg^{-1} = 1$$

Montrons tout d'abord que G n'a pas de sous-groupe normal non trivial contenu dans B. Soit G_1 un tel sous-groupe. Par la proposition I.3.13, le groupe de Weyl W contient un élément w_0 qui transforme toute racine positive en une racine négative. Soit n_0 un élément correspondant de N. Alors :

$$n_0 U n_0^{-1} = V$$

et donc $n_0 U H n_0^{-1} = VH$. Or G_1 est contenu dans UH, donc aussi dans VH puisqu'il est normal. Donc $G_1 \subseteq H$ par le corollaire II.5.7. Or H normalise U, i.e $[U, H] \subseteq U$, et on a $[U, G_1] \subseteq U \cap G_1 \subseteq U \cap H = 1$. Donc tout élément de G_1 commute avec tout élément de U. Soit $h(\chi) \in G_1$. Alors $h(\chi)x_r(1)h(\chi)^{-1} = x_r(\chi(r) = x_r(1)$ pour tout $r \in \Phi^+$. Il suit que $\chi(r) = 1$ pour tout $r \in \Phi^+$. Donc $\chi = 1$ et $h(\chi) = 1$. Donc $G_1 = 1$. On a donc prouvé $\cap_{g \in G} gBg^{-1} = 1$.
Montrons désormais que le centre Z de G est trivial. La méthode utilisée au Théorème II.7.1 nous montre que :

$$G = ZB \text{ ou } Z \subset \cap_{g \in G} gBg^{-1}$$

Si $G = ZB$ alors B est normal dans G. Or B est son propre normalisateur d'après Théorème II.6.10 , donc $ZB = B$. Ainsi $Z \subset B$ et comme Z est normal :

$$Z \subset \cap_{g \in G} gBg^{-1}$$

et donc $Z = 1$. Il reste à prouver que $G = D(G)$.
• Supposons tout d'abord que $\mathbb{K}$ a au moins 4 éléments. Alors on dispose de $t \in \mathbb{K}^*$ tel que $t^2 \neq 1$. Par le lemme II.7.2, on dispose pour chaque $r \in \Phi$ d'un $\mathbb{K}$-caractère χ de Q tel que $\chi(r) \neq 1$. Alors $h(\chi) \in H$ et on a :

$$h(\chi)x_r(t)h(\chi)^{-1} = x_r(\chi(r)t)$$

Il suit que $x_r((\chi(r) - 1)t) \in D(G)$ pour tout $t \in K$. Soit $u \in K$, prenons :

$$t = \frac{u}{\chi(r) - 1}$$

Alors $x_r(u) \in D(G)$. Les éléments $x_r(u)$ engendrant G pour $r \in \Phi$ et $u \in \mathbb{K}$, on a $G = D(G)$.

• Supposons que $\mathbb{K} = \mathbb{F}_3$. Si $\mathfrak{L}$ n'est pas de type A_1 ou C_l, on dispose pour tout $r \in \Phi$, par le lemme II.7.2, d'un $\mathbb{K}$-caractère χ de Q tel que $\chi(r) \neq 1$. Alors $G = D(G)$ comme ci-dessus. Supposons désormais $G = C_l(3)$ avec $l \geq 2$. G est généré par les X_r pour $r \in \Phi$. X_r et $X_{w(r)}$ étant conjugués dans G par le lemme II.5.8, et donc équivalents modulo $D(G)$, le groupe $G/D(G)$ est généré par les images des sous-groupes X_r et il suffit de choisir une racine de chaque orbite de Φ sous l'action de W, autrement dit une racine de chaque longueur. Si r est une racine courte de C_l, on dispose d'un $\mathbb{K}$-caractère χ tel que $\chi(r) \neq 1$. Donc X_r est inclus dans $D(G)$. Soit s la racine longue de C_l et r la racine qui lui est liée dans le diagramme de Dynkin. Alors :

$$[x_s(1), x_r(1)] = x_{r+s}(\pm 1)x_{2r+s}(\pm 1)$$

par la formule du commutateur. Or $r + s$ est une racine courte, et $2r + s$ une racine longue. Donc

$X_{r+s} \subseteq D(G)$ et $x_{r+s}(\pm 1)x_{2r+s}(\pm 1) \in D(G)$. Il suit que $X_{2r+s} \subseteq D(G)$ et donc $D(G) = G$.

- Supposons que $\mathbb{K} = \mathbb{F}_2$. Si toutes les racines de $\mathfrak{L}$ ont la même longueur, $G/D(G)$ est engendré par l'image de $x_r(1)$ pour n'importe quelle racine $r \in \Phi$. Si $\mathfrak{L} \neq A_1$, on peut choisir $r, s \in \Phi$ tel que $r + s \in \Phi$. On a donc :

$$[x_s(1), x_r(1)] = x_{r+s}(1)$$

par la formule du commutateur. Donc $x_{r+s}(1) \in D(G)$ et donc $D(G) = G$.
Supposons désormais qu'il y a deux racines de longueurs différentes. Alors $G/D(G)$ est généré par $x_r(1), x_s(1)$, où r, s sont des racines de longueurs différentes. Supposons sans perte de généralités que r est courte, s longue et que $r + s \in \Phi$. Supposons de plus que les noeuds correspondant à r, s dans le diagramme de Dynkin sont joints par un double lien, i.e $\mathfrak{L} \neq B_2$. Alors le diagramme dispose de deux noeuds joints par un lien simple. Soit r_1, r_2 les racines fondamentales correspondantes. Alors :

$$[X_{r_2}(1), x_{r_1}(1)] = x_{r_1+r_2}(1)$$

et donc $x_{r_1+r_2}(1) \in D(G)$. Si $r_1 + r_2$ est une racine courte, ceci implique que tous les sous-groupes X_r correspondant aux racines courtes sont dans $D(G)$. Donc $x_{r+s}(1) \in D(G)$. Mais alors $x_{2r+s}(1) \in D(G)$ et $D(G)$ contient donc aussi les sous-groupes X_r associés aux racines longues. D'où $D(G) = G$. Un argument similaire s'applique si $r_1 + r_2$ est une racine longue.
Les seuls groupes de Chevalley non couverts dans la preuve ce-dessus sont $A_1(2)$, $A_1(3)$, $B_2(2)$ et $G_2(2)$, le théorème est donc prouvé. $\square$

Les 4 groupes mentionnés ci-dessus ne sont en réalité pas simples. $A_1(2)$ est d'ordre 6 et isomorphe à $\mathfrak{S}_3$. $A_1(3)$ est d'ordre 12 et isomorphe au groupe alterné $\mathfrak{A}_4$. $B_2(2)$ est d'ordre 720 et isomorphe à $\mathfrak{S}_6$. Enfin, $G_2(2)$ est d'ordre 12096 et dispose d'un sous-groupe simple d'indice 2 isomorphe au groupe spécial unitaire $PSU_3(\mathbb{F}_9)$

III Groupes tordus simples

On a déjà prouvé que les groupes de Chevalley de type A_l, B_l, C_l, D_l s'identifiaient à certains groupes classiques ; mais ceux-ci ne sont pas intégralement représentés, (comme par exemple les groupes unitaires). L'objectif de cette section est de construire d'autres groupes simples à partir des groupes de Chevalley, en les "tordant". On obtiendra aussi de nouveaux groupes simples exceptionnels.

Idée : On obtiendra ces groupes comme sous-groupes de Chevalley $G = \mathfrak{L}(\mathbb{K})$. Les groupes tordus apparaissent dans le cas où le diagramme de Dynkin admet une symétrie non triviale. On montrera que ceux-ci sont aussi des groupes avec une paire (B, N), et que le groupe de Weyl W^1 de cette paire est un groupe de réflexions, sous-groupe du groupe de Weyl W de G. On commencera par construire ce groupe.

III.1 Le sous-groupe W^1

On rappelle que W opère sur l'espace euclidien $\mathfrak{V}$ engendré par le système de racines. On considère ρ une symétrie non triviale du diagramme de Dynkin. Alors il existe une unique isométrie τ de $\mathfrak{V}$ telle que $\tau(r)$ est un multiple strictement positif de $\rho(r)$, pour toute racine fondamentale, telle que :

$\tau(r) = \rho(r)$ si toutes les racines ont la même longueur

$$\tau(r) = \begin{cases} \frac{1}{\sqrt{2}}\rho(r) & \text{si r est courte, et de type } B_l \text{ ou } F_4 \\ \sqrt{2}\rho(r) & \text{si r est long.} \end{cases}$$

$$\tau(r) = \begin{cases} \frac{1}{\sqrt{3}}\rho(r) & \text{si r est courte, et de type } G_4 \\ \sqrt{3}\rho(r) & \text{si r est long.} \end{cases}$$

L'ordre de τ, en tant qu'isométrie, est l'ordre de ρ comme permutation du système fondamental de racines.

On note $\mathfrak{V}^1$ l'ensemble des points fixes de τ. Pour $v \in \mathfrak{V}$, on note v^1 la projection de v sur le sous espace $\mathfrak{V}^1$. On remarque qu'alors v^1 et la moyenne de v sous l'orbite de τ, car on a ;

$$(v, x) = (\tau(v), x) = (\tau^2(v), x) = \dots$$

On a de plus $\forall r \in \Pi$,

$$\tau w_r \tau^{-1} = w_{\rho(r)}$$

Comme les réflexions du groupe fondamental engendrent le groupe de Weyl W, on a que $\tau W \tau^{-1} = W$.

Définition III.1.1 : On note W^1 le groupe des éléments de W qui commutent avec τ.

Lemme III.1.2 : W^1 agit fidèlement sur $\mathfrak{V}^1$, l'action étant l'application des isométries. *Cela permet d'identifier les éléments de W^1 par leur action.*

Preuve : Prenons maintenant $w \in W^1$ différent de l'identité. Alors comme w est d'ordre fini, il existe une racine positive r telle que $w(r)$ soit une racine négative. On a alors $r^1 > 0$ car appliquer τ conserve la positivité, et par commutativité, $w(r^1) = w(r)^1 < 0$. Donc w n'est pas l'identité sur $\mathfrak{V}^1$. CQFD.

Montrons maintenant que W est généré par les éléments d'ordre 2. On procède en deux étapes.

Proposition III.1.3 : Soit J une orbite de Π par ρ. Notons W_J le sous groupe de W généré par les $w_j, j \in J$. Notons w_0^J l'élément de W_J (qu'on obtient facilement par produit), qui transforme chaque racine positive en une racine négative. Alors w_0^J est dans W^1, et W^1 est engendré par tous ceux-ci.

Preuve : Comme τ préserve les signes, il est direct que w_0^J est dans W^1. Prenons maintenant $w \neq 1 \in W^1$. D'après la preuve précédente il existe $r \in \Pi$ telle que $w(r) \in \phi^-$. Prenons J l'orbite selon ρ contenant r. Alors $w(s) \in \phi^- \ \forall\ s \in J$. Or w_0^J change le signe de toutes les racines dans ϕ_J, mais aucune dans son complémentaire. Ainsi $l(ww_0^J) = l(w) - l(w_0^J)$. Par récurrence sur $l(w)$, W^1 est généré par les w_0^J.

Montrons maintenant que les w_0^J restreints à $\mathfrak{V}^1$ sont des réflexions.

<u>Lemme III.1.4</u> : w_0^J coincide avec w_{r^1} sur $\mathfrak{V}^1$ pour r quelconque dans J.
Preuve : En effet, on sait déjà que deux racines fondamentales dans le même orbite de ρ ont des projections qui sont positivement multiples de toutes les autres. De plus, on sait que $w_0^J(r^1) = w_0^J(r)^1$ et que $w_0^J(r) \in \phi_J^-$ pour r racine positive dans ϕ_J. $w_0^J(r^1)$ est ainsi multiple négatif de r^1 ; comme c'est une isométrie elle vaut $w_0^J(r^1) = -r^1$. On vérifie de plus que sur l'orthogonal de r^1 dans $\mathfrak{V}^1$, w_0^J est l'identité. On a donc le résultat. CQFD

Corollaire : Les réflexions $w_{r^1}, \forall r \in \Pi$, engendrent le groupe W^1 des isométries de $\mathfrak{V}^1$.

III.2 Le système ϕ^1

On note ϕ^1 l'ensemble des r^1, pour $r \in \Phi$; et on note Π^1 l'ensemble des r^1, pour $r \in \Pi$.

Lemme III.2.1 : Les ensembles $w(\Phi_J^+)$ forment une partition de Φ lorsque J parcourt les orbites selon ρ et w les éléments de W^1.

Preuve : Commençons par prouver que chaque racine est dans un $w(\Phi_J^+)$. Prenons w_0 l'élement qui transforme toute racine positive en négative. On a comme précédemment $w_0 \in W^1$. Prenons maintenant $r \in \Phi^+$, donc $w_0(r) \in \Phi^-$. Par les preuves de la sous-section précédente, $w_0 = w_0^{J_1} \dots w_0^{J_k}$ avec J_i des ρ-orbites de Π. Il existe un entier i tel que :

$$w_0^{J_{i+1}} \dots w_0^{J_k}(r) \in \Phi^+$$

$$w_0^{J_i} \dots w_0^{J_k}(r) \in \Phi^-$$

Il vient donc que $r \in w_0^{J_k} \dots w_0^{J_{i+1}}(\Phi_{J_i}^+)$ et $-r \in w_0^{J_k} \dots w_0^{J_i}(\Phi_{J_i}^+)$. Chaque racine est donc au moins dans un de ces ensembles. D'autre part, si r, s sont des racines dans Φ_J^+, on a vu que r^1 était un multiple positif de s^1. En faisant agir $w \in W^1$, on voit que $w(r^1) = w(r)^1$ est un multiple positif de $w(s^1) = w(s)^1$.

Supposons maintenant que $r, s \in \Phi$ et que r^1 est un multiple positif de s^1. On a montré que $r \in w(\Phi_J^+)$ pour un bon élément w de W^1 et bon sous-ensemble J de Π. Ainsi $w^{-1}(r) \in \Phi_J^+$ et alors $w^{-1}(r)^1$ est un élément positif qui est une combinaison linéaire de racines dans J. Or, pour un certain $\lambda > 0$,

$$w^{-1}(r)^1 = w^{-1}(r^1) = w^{-1}(\lambda s^1) = \lambda w^{-1}(s)^1$$

et donc $w^{-1}(s)^1$ est un vecteur positif qui est une combinaison linéaire de racines dans J. Il en va de même pour $w^{-1}(s)$ car J est une ρ-orbite. D'où $w^{-1}(s) \in \Phi_J^+$ et $s \in w(\Phi_J^+)$. Ainsi, s est contenu dans chacun des sous-ensembles contenant r. On en déduit que ces ensembles recouvrent Φ, et que soit ils coïncident, soit ils n'ont aucun élément en commun.

Proposition III.2.2 :

1. ϕ^1 engendre $\mathfrak{V}^1$.
2. Chaque élément de ϕ^1 est une combinaison linéaire d'éléments de Π^1, dont tous les coefficients sont soit tous positifs, soit tous négatifs.
3. On peut obtenir une base de $\mathfrak{V}^1$ en prenant un élément de Π^1 dans chaque ensemble de multiples positifs.
4. Si $r^1 \in \phi^1$, alors il existe un élément de W^1 coincidant avec w_{r^1} sur $\mathfrak{V}^1$.
5. Si $r^1, s^1 \in \phi^1$, alors $w_{r^1}(s^1) \in \phi^1$.

C'est donc, au dernier axiome près, un système de racines dont W^1 est le groupe de Weyl.

III.3 Structure de W^1

On va ici décrire la structure de W^1 dans les différents cas possibles. Soient $r_1, \dots, r_k$ un ensemble de racines, dont les ρ-orbites sont deux-à-deux disjointes. Alors $r_1^1, \dots, r_k^1$ sont linéairement indépendants dans $\mathfrak{V}^1$; et W^1 est engendré par $w^1_{r_1}, \dots, w^1_{r_k}$. En considérant les angles entre les $r_1^1, \dots, r_k^1$, on essayera de relier W^1 à un groupe de Weyl de rang k.

<u>Type A_l</u>

On numérote les racines fondamentales $p_1, \dots p_l$.

— Supposons que $l = 2k-1$ soit impair. Les vecteurs $r_1^1, \dots, r_k^1$ s'écrivent alors

$$\frac{1}{2}(p_1 + p_{2k-1}), \dots, \frac{1}{2}(p_k + p_{k+1}), p_k$$

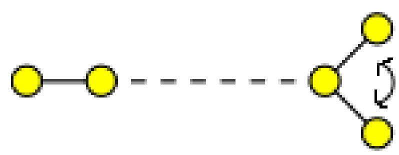
Ils forment un système fondamental de type C_k. W^1 est ainsi isomorphe à $W(C_k)$.

— Supposons $l = 2k$. Les vecteurs $r_1^1, \dots, r_k^1$ s'écrivent alors

$$\frac{1}{2}(p_1 + p_{2k-1}), \dots, \frac{1}{2}(p_k + p_{k+1})$$

Ils forment un système fondamental de type B_k. W^1 est alors isomorphe à $W(B_k)$.

<u>Type D_l</u>

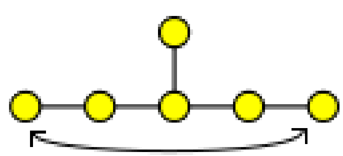


Les vecteurs $r_1^1, \dots, r_k^1$ s'écrivent alors

$$p_1, p_2, \dots, p_{l-2}, \frac{1}{2}(p_{l-1} + p_l)$$

Ils forment un système fondamental de type B_{l-1}.

<u>Type E_6</u>

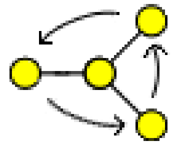


Les vecteurs $r_1^1, \dots, r_k^1$ s'écrivent alors

$$\frac{1}{2}(p_1 + p_6), \dots, \frac{1}{2}(p_2 + p_5), p_3, p_4$$

Ils forment un système fondamental de type F_4.

Type D_4

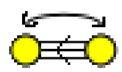


La symétrie est ici d'ordre 3. Les vecteurs $r_1^1, \dots, r_k^1$ s'écrivent alors

$$p_1, \frac{1}{3}(p_2 + p_3 + p_4)$$

Ils forment un système fondamental de type G_2.

Type G_2

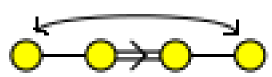


Ici, $k = 1$ donc W est isomorphe à $W(A_1)$, un groupe cyclique d'ordre 2.

Type B_2

On a encore $k = 1$, donc W est isomorphe à $W(A_1)$, un groupe cyclique d'ordre 2.

Type F_4



La situation est ici plus complexe : on prend p_1, p_2 le racines fondamentales longues, et p_3, p_4 les courtes.
Les vecteurs $r_1^1, \dots, r_k^1$ peuvent alors s'écrire :

$$\frac{1}{2}(p_1 + \sqrt{2}p_4), \frac{1}{2}(p_2 + \sqrt{2}p_3)$$

On calcule un angle de $\theta = \frac{7\pi}{8}$ entre les deux. Dans ce cas, W n'est pas isomorphe à un groupe de Chevalley, mais au groupe dièdral d'ordre 16.

III.4 Définition des groupes tordus

Soit G le groupe de Chevalley de $\mathfrak{L}(\mathbb{K})$ et soit ρ une symétrie non-triviale du diagramme de Dynkin de $\mathfrak{L}$. Supposons que K est un corps parfait de caractéristique 2 si $\mathfrak{L} = B_2$ ou F_4, et parfait de caractéristique 3 si $\mathfrak{L} = G_2$. On admet l'existence d'un automorphisme de graphe g de G tel que $g(X_r) = X_{\rho(r)}$; celui-ci commute avec tout automorphisme de corps f.

On écrira maintenant $\rho(r) = \bar{r}$.

Proposition III.4.1 **:** Soit g l'automorphisme de graphe correspondant à ρ et soit f un automorphisme de corps non trivial tel que $\sigma = g \cdot f$ a un ordre fini qui divise celui de ρ. Alors on a

$$\sigma(U) = U, \sigma(V) = V, \sigma(H) = H, \sigma(N) = N$$

et σ agit sur $N/H \cong W$ selon la formule $\sigma(w_r) = w_{\rho(r)}$ pour $r \in \Pi$.

On notera $f(t) = \bar{t}$ si toutes les racines ont la même longueur, et $f(t) = t^\theta$ sinon. De plus $\lambda(r)$ est un entier qui vaut 1 si la racine r est courte, et 2 ou 3 si la racine est longue.

Définition III.4.2 **:**

1. U^1 est l'ensemble des éléments x de U tels que $\sigma(x) = x$.
2. V^1 est l'ensemble des éléments x de V tels que $\sigma(x) = x$.
3. G^1 est le sous-groupe de G engendré par U^1 et V^1.
4. H^1 est l'intersection de G^1 et H.
5. N^1 est l'intersection de G^1 et N.

On montrera que G^1 est (presque) toujours un groupe simple, et que le rôle joué par les sous-groupes définis précédemment est analogue au rôle joué par les sous groupes originaux sur G. On remarque que même si tous les éléments de G^1 sont fixés par σ, G^1 n'est pas forcément le sous groupe des éléments fixés par σ.

Enfin, l'action de σ su W est la même que celle de transformation selon τ déterminée par ρ. Ainsi, le sous-groupe W^1 des éléments de W fixant σ est simplement le sous groupe défini au début de cette partie. On montrera que W^1 joue le rôle du groupe de Weyl de G^1

III.5 Existence d'une paire (B, N) chez les groupes tordus

On a vu que les ensembles $w(\Phi_J^+)$ formaient une partition de Φ lorsque J parcourt les orbites selon ρ et w les éléments de W^1. Nous allons nous intéresser plus en détails aux classes d'équivalences.

Les racines dans la classe d'équivalence $w(\Phi_J^+)$ sont les racines positives dans le système $w(\Phi_J)$ par rapport au système fondamental $w(J)$. Le "type" de ce système de racine est le même que celui de J.

Les différents types en question s'obtiennent à travers l'étude des diagrammes de Dynkin :

Si $\mathfrak{L} = A_{2k-1}, D_l$ ou E_6, chaque ρ-orbite J est de type A_1 ou $A_1 \times A_1$.

Si $\mathfrak{L} = A_{2k}$, J est de type $A_1 \times A_1$. ou A_2.

Si $\mathfrak{L} = D_4$, J est de type A_1 ou $A_1 \times A_1 \times A_1$.

Si $\mathfrak{L} = B_2$, J est de type B^2.

Si $\mathfrak{L} = G_2$, J est de type G_2.

Enfin, si $\mathfrak{L} = F_4$, J est de type $A_1 \times A_1 \times A_1$ ou A_1.

Chaque classe d'équivalence peut donc être vue comme un système positif parmi ces 6 types.

Lemme III.5.1 : Soit S une des classes d'équivalence définie précédemment. Posons X_S le sous groupe engendré par les X_r, pour $r \in S$. On a alors

$$X_S = \prod_{r \in S} X_r$$

De plus $\sigma(X_S) = X_S$, et le sous groupe X_S^1 des éléments de X_S qui fixent σ n'est pas réduit à 1.
Preuve : On a vu que S est un système positif, pour une certaine relation d'ordre, d'un système de racine contenu dans Φ. Le sous-groupe X_S joue alors le rôle de U en tant que sous-système de Φ ; on retrouve ainsi la factorisation.
La preuve du dernier résultat est surtout affaire de technicité, on l'a donc omise.

Proposition III.5.2 :

1. Pour tout $w \in W^1$, $\exists n_w \in N^1$ tel que n_w corresponde à w pour l'homomorphisme naturel de N à W.
2. $N^1/H^1 \cong W^1$
3. Chaque élément de G^1 a une unique expression $g = u'hn_w u$ où $u' \in U^1$, $h \in H^1, w \in W^1, n_w \in N^1$ et $u \in (U_w^-)^1$ l'ensemble des éléments de U_w^- fixant σ.

Théorème III.5.3 : Les sous-groupes B^1, N^1 forment une (B, N) paire dans G^1.
Preuve : Vérifions les conditions 1 à 5.

1. On a que $G^1 = B^1N^1B^1$, donc N^1 et B^1 engendrent G^1.
2. On a $B^1 \cap N^1 = G^1 \cap B \cap N = G^1 \cap H = H^1$, qui est donc distingué dans N^1.
3. $N^1/B^1 \cap N^1$ est isomorphe à W^1, donc engendré par les w_0^J d'ordre 2.

4. Montrons maintenant que $n(w_0^J)B^1n(w_0^J)^{-1} \neq B^1$. Notons S la classe d'équivalence Φ_J^+ de Φ. Il existe alors $x \in X_S^1 \neq 1$. Or

$$n(w_0^J)xn(w_0^J)^{-1} \in n(w_0^J)X_S^1n(w_0^J)^{-1} = X_{-S}^1$$

On voit que $n(w_0^J)xn(w_0^J)^{-1}$ est un élément $\neq 1$ de V^1, qui n'est donc pas dans B^1 car $B^1 \cap V^1 = 1$.
5. Enfin, on doit montrer que $B^1n(w_0^J)B^1 \cdot B^1nB^1 \subseteq B^1n(w_0^J)B^1 \cup B^1nB^1$ pour tout $n \in N^1$ et toutes les ρ-orbites J de Π. Les w_0^J peuvent s'exprimer comme un produit de réflexions sur les racines de J :

$$w_0^J = w_{r_1} \dots w_{r_k} \qquad r_i \in J$$

On a d'après des résultats sur les paires B, N des groupes de Chevalley :

$$Bn(w_{r_i})B \cdot BnB \subseteq Bn(w_{r_i})nB \cup BnB$$

En appliquant de façon répétée cette identité, on obtient que $B^1n(w_0^J)B^1 \cdot B^1nB^1$ est dans une union d'ensemble $Bn(w)B$ où w est un élément de la forme $w_{s_1} \dots w_{s_h}$, et $(s_1, \dots, s_h)$ est extrait de $(r_1, \dots, r_k)$. Par la proposition précédente, $G^1 \cap Bn(w)B \prec B^1n_wB^1$ si $w \in W^1$, et est vide sinon. Ainsi $B^1n(w_0^J)B^1$ est dans une union d'ensembles de la forme $B^1n(w)B^1$, avec $w \in W^1 \cap W_J$. Cependant, les seuls éléments de cette intersection sont 1 et w_0^J, puisque chaque élément non trivial de cette intersection transforme les racines de J en racine négative. D'où le résultat.

Proposition III.5.4 **:** G^1 est engendré par les sous-groupes $X^1_{\Phi^+_J}$, $X^1_{\Phi^-_J}$ où J parcourt les ρ orbites de Π.

III.6 Propriétés des groupes tordus

Nous avons défini les groupes tordus ; nous allons maintenant chercher à prouver leur simplicité, à calculer leur ordre et montrer qu'on peut en identifier quelques uns avec des groupes classiques. Supposons que G^1 soit un groupe tordu construit comme sous groupe du groupe de Chevalley $\mathfrak{L}(\mathbb{K})$, et supposons que le corps $\mathbb{K}$ est fini. On admettra les résultats suivants :

Proposition III.6.1 **:** *(admis)*

Si $\mathfrak{L}$ est de type A_l, pour $l \geq 2$, alors $\mathbb{K}$ admet un automorphisme d'ordre 2, et doit donc être $\mathbb{F}_{q^2}$, où q est une puissance de nombre premier. On a le même résultat si $\mathfrak{L}$ est de type D_l ou E_6.

Si $\mathfrak{L}$ est de type D_4, et que l'automorphisme de graphe utilisé dans la construction est d'ordre 3, alors $\mathbb{K} = \mathbb{F}_{q^3}$.

Si $\mathfrak{L}$ est de type B_2 ou F_4, alors $\mathbb{K}$ est un corps de caractéristique 2 admettant un automorphisme tel que $2\theta^2 = 1$.

Enfin, si $\mathfrak{L}$ est de type G_2, $\mathbb{K}$ est un corps de caractéristique 3 admettant un automorphisme θ tel que $3\theta^2 = 1$.

Rappelons que pour un corps fini $\mathbb{K} = \mathbb{F}_{p^n}$, où p est premier, les automorphismes de corps sont engendrés par l'endomorphisme de Frobenius $x \mapsto x^p$. On identifie ici θ à la puissance à laquelle elle élève chaque terme.

Lemme III.6.2 **:** Soit p un nombre premier. Si θ est un automorphisme de $\mathbb{F}_{p^n}$, avec $p\theta^2 = 1$ alors $n = 2m+1$ est impair et $\theta = p^m$.

Preuve : En effet, on a $\forall \lambda \in \mathbb{K}, \lambda^\theta = \lambda^{p^r}$. Par hypothèse, on a donc $\lambda = \lambda^{p^{2r+1}}$, donc $\mathbb{K}$ est inclus dans $\mathbb{F}_{p^{2r+1}}$. Ainsi $n = 2m+1$ est impair et divise $2r+1$. On peut donc écrire $2r+1 = (2m+1)(2s+1) \iff r = s(2m+1)+m$, et il vient :

$$\lambda^{p^r} = \lambda^{p^{s(2m+1)+m}} = (\lambda^{p^{(2m+1)s}})^{p^m} = \lambda^{p^m}$$

D'où le résultat.

On en déduit que si $\mathfrak{L}$ est de type B_2 or F_4, alors $\mathbb{K} = \mathbb{F}_{2^{2m+1}}$ pour un certain m, et si $\mathfrak{L}$ est de type G_2 alors $\mathbb{K} = \mathbb{F}_{3^{2m+1}}$.

On notera maintenant $G^1 = {}^i\mathfrak{L}(\mathbb{K})$ les groupes tordus, où i est l'ordre de la symétrie qu'on a considérée. De façon exhaustive, on notera donc :

$$^2A_l(q^2)\,(l \geq 2) \quad ^2D_l(q^2)\,(l \geq 4)$$

$$^2E_6(q^2) \qquad ^3D_4(q^3) \qquad ^2B_2(2^{2m+1}) \qquad ^2G_2(3^{2m+1}) \qquad ^2F_4(2^{2m+1}).$$

Proposition III.6.3 : Soit S une classe d'équivalence de Φ. Alors

1. Si $S = \{r\}$ est de type A_1 alors X_S^1 consiste en les éléments $x_r(t)$, avec $t = \bar{t}$.
2. Si $S = \{r, \bar{r}\}$ est de type $A_1 \times A_1$ avec r et $\bar{r}$ de même taille, X_S^1 consiste en les éléments $x_r(t)x_{\bar{r}}(\bar{t})$ pour tout $t \in \mathbb{K}$.
3. Si $S = \{r, \bar{r}, \bar{\bar{r}}\}$ est de type $A_1 \times A_1 \times A_1$, alors X_S^1 est constitué des éléments $x_r(t)x_{\bar{r}}(\bar{t})x_{\bar{\bar{r}}}(\bar{\bar{t}})$ pour tout $t \in \mathbb{K}$.
4. Si $S = \{r, \bar{r}, r + \bar{r}\}$, alors X_S^1 est constitué des éléments $x_r(t)x_{\bar{r}}(\bar{t})x_{r\bar{r}}(u)$, pour tout $t \in \mathbb{K}$ et $u + \bar{u} = -N_{r\bar{r}}t\bar{t}$.

Preuve : 1. Est vrai par définition.
2. Comme $\sigma \cdot x_r(t)x_{\bar{r}}(u) = x_{\bar{r}}(\bar{t})x_r(\bar{u}) = x_r(\bar{u})x_{\bar{r}}(\bar{t})$, les éléments fixant σ sont ceux pour qui $u = \bar{t}$.
3. et 4. se prouvent de la même manière.

III.7 Simplicité des groupes tordus

On montre ici que les groupes tordus sont simples, exceptés quelques-uns sur de petits corps.

Théorème III.7.1 : Tous les groupes tordus sont simples, sauf ${}^2A_2(2^2), {}^2B_2(2), {}^2G_2(3)$ et ${}^2F_4(2)$.
Preuve : On va chercher à utiliser le théorème de simplicité sur les groupes contenant une paire (B, N). Voyons tous les critères :

1. B^1 est résoluble car c'est un sous-groupe de B, qui est lui-même résoluble.
2. Soit G_1^1 un sous-groupe distingué de G^1 inclus dans B^1. Il est alors contenu dans U^1H^1 et dans son conjugué V^1H^1, donc dans H^1. Comme dans la preuve originelle de la simplicité des groupes de Chevalley, on a que tout élément de G^1 commute avec chaque élément de U^1, et chaque élément de V^1. Prenons donc $h(\chi) \in G_1^1$. Comme $h(\chi)x_r(t)h(\chi)^{-1} = x_r(\chi(r)t)$, on a par un lemme précédent que $\chi(r) = 1$ pour tout $r \in \Phi$. En effet, chaque racine r est dans une classe d'équivalence S, et il y a donc un élément dans X_S^1 faisant intervenir r. Donc $G_1^1 = 1$. On a donc $\bigcap_{g \in G^1} gB^1g^{-1} = 1$
3. Le groupe de Weyl de la paire (B^1, N^1) est W^1, et on prend I l'ensemble des générateurs distincts de W^1 composés des w_0^J, où J parcourt les orbites de ρ. On a vu précédemment que soit ces élements forment l'ensemble des réflexions fondamentales d'un groupe de Weyl indécomposable, soit $|I| = 2$ et les deux éléments engendrent le groupe dihédral d'ordre 16. Dans les deux cas, on ne peut pas décomposer I en deux sous-ensemble qui laissent ses éléments commuter.

4. Il reste donc à prouver que $G^1 = D(G^1)$. Ce n'est pas chose facile... On va en fait montrer que $D(G^1)$ contient X_S^1 pour toute classe d'équivalence de Φ, ce qui est une condition suffisante. La preuve consiste à disjoindre les cas, chacun étant très technique ; on se contentera de montrer celui où toutes les racines sont de même taille. Les classes d'équivalence S de Φ sont alors de type A_1, $A_1 \times A_1$, $A_1 \times A_1 \times A_1$ ou A_2. Prenons $h(\chi)$ un élément de H^1. On utilise les relations suivantes, qui découlent de la formule du commutateur :

<u>Si $S = \{r\}$ est de type A_1 :</u>

$$h(\chi)x_r(t)h(\chi)^{-1} = x_r(\chi(r)t)$$

Si $S = \{r, \bar{r}\}$ est de type $A_1 \times A_1$:

$$h(\chi)x_r(t)x_{\bar{r}}(\bar{t})h(\chi)^{-1} = x_r(\chi(r)t))x_{\bar{r}}(\chi(\bar{r})\bar{t})$$

Si $S = \{r, \bar{r}, \bar{\bar{r}}\}$ est de type $A_1 \times A_1 \times A_1$:

$$h(\chi)x_r(t)x_{\bar{r}}(\bar{t})x_{\bar{\bar{r}}}(\bar{\bar{t}})h(\chi)^{-1} = x_r(\chi(r)t))x_{\bar{r}}(\chi(\bar{r})\bar{t})x_{\bar{\bar{r}}}(\chi(\bar{\bar{r}})\bar{\bar{t}})$$

Si $S = \{r, \bar{r}, r + \bar{r}\}$ est de type A_2 et que $u + \bar{u} = -N_{r\bar{r}}t\bar{t}$:

$$h(\chi)x_r(t)x_{\bar{r}}(\bar{t})x_{r+\bar{r}}(u)h(\chi)^{-1} = x_r(\chi(r)t))x_{\bar{r}}(\chi(\bar{r})\bar{t})x_{r+\bar{r}}(\chi(r+\bar{r})u)$$

Cela étant dit, on sait d'après la partie sur les groupes de Chevalley, qu'on peut trouver, quelle que soit r racine de Φ et $t \neq 0 \in \mathbb{K}$, un $\mathbb{K}$ caractère χ de Q telle que $\chi(r) = t^2$. En fait, comme les exceptions A_1 et C_l ne sont pas dans les cas ici considérés, on peut trouver un caractère χ de Q tel que $\chi(r) = t$. Si $r = \bar{r}$, on peut trouver, pour tout t non nul dans $\mathbb{K}_0$ le sous-corps de $\mathbb{K}$ laissant σ invariant, un $\mathbb{K}$ caractère conjugué de Q tel que $\chi(r) = t$. *(Un caractère conjugué est tel que $\chi(\bar{r}) = \overline{\chi(r)}$)*
Si $S = \{r\}$ est de type A_1 et que $\mathbb{K}_0 \neq \mathbb{F}_2$, on peut choisir un caractère χ conjugué de Q tel que $\chi(r) \neq 1$. Alors $x_r((\chi(r) - 1)t) = [h(\chi), x_r(t)]$ d'après la relation précédente. Ainsi, en prenant $t = \frac{u}{\chi(r)-1}$, on a $x_r(u) \in D(G^1)$, et donc $X_S^1 \subseteq D(G^1)$. De la même façon, on obtient le résultat pour S de type $A_1 \times A_1$ ou $A_1 \times A_1 \times A_1$, même si $\mathbb{K}_0 = \mathbb{F}_2$.
Si S est de type A_2, les relations précédentes montrent que :

$$x_r((\chi(r) - 1)t)x_{\bar{r}}((\chi(\bar{r}) - 1)\bar{t})x_{r+\bar{r}}((\chi(r + \bar{r}) - 1)u + N_{r\bar{r}}(\chi(\bar{r}) - 1)t\bar{t})$$

est dans $D(G^1)$.
Si $\mathbb{K}_0 \neq \mathbb{F}_2$, on peut choisir un $\mathbb{K}$ caractère de Q tel que $\chi(r + \bar{r}) \neq 1$. En effet, si $\chi(r) = \lambda$, alors $\chi(\bar{r}) = \bar{\lambda}$ et $\chi(r + \bar{r}) = \lambda\bar{\lambda}$. Si $\chi(r + \bar{r}) = 1 \forall\lambda$, alors $\lambda\bar{\lambda} = 1 \forall\lambda \neq 0$. Dans $\mathbb{K}_0$, on a donc $\lambda^2 = 1$. Notons $\mathbb{K}_0 = \mathbb{F}_q$. Alors $\bar{\lambda} = \lambda^q$ et $\lambda^{q+1} = 1\ \forall\lambda \neq 0 \in \mathbb{K}$. Donc tous les éléments non nuls de $\mathbb{K}_0$ sont égaux à 1, ce qui implique que $\mathbb{K}_0 = \mathbb{F}_2$, ce qui est une contradiction.
Prenons maintenant t_1, u_1 dans $\mathbb{K}$ tels que $u_1 + \bar{u_1} = -N_{r\bar{r}}t_1\bar{t_1}$. Choisissons un caractère conjugué χ de Q tel que $\chi(r + \bar{r}) \neq 1$ définissons $t = \frac{t_1}{\chi(r)-1}$, $u = \frac{u_1}{\chi(r+\bar{r})-10} - \frac{N_{r\bar{r}}(\chi(\bar{r})-1)t\bar{t}}{\chi(r+\bar{r})-1}$. Il vient alors $u + \bar{u} = -N_{r\bar{r}}t\bar{t}$ et $\chi_r(t_1)\chi_{\bar{r}}(\bar{t_1})\chi_{r+\bar{r}}(u_1)$ est dans $D(G^1)$. Ainsi $X_S^1 \subseteq D(G^1)$.
Dans le cas où $\mathbb{K}_0 = \mathbb{F}_2$ et des racines de même longueur, on contourne le problème en définissant x_S suivant le type de S :

Si S de type A_1, $x_S(t) = x_r(t)$, c'est un morphisme.

Si S de type $A_1 \times A_1$, $x_S(t) = x_r(t)x_{\bar{r}}(\bar{t})$. C'est un morphisme.

Si S de type $A_1 \times A_1$, $x_S(t) = x_r(t)x_{\bar{r}}(\bar{t})x_{\bar{\bar{r}}}(\bar{\bar{t}})$. C'est un morphisme.

Si S de type A_2, $x_S(t, u) = x_r t x_{\bar{r}}(\bar{t})x_{r+\bar{r}}(u)$ qui vérifie $x_S(t_1, u_1)x_S(t_2, u_2) = x_S(t_1 + t_2, u_1 + u_2 - N_{r+\bar{r}}\bar{t_1}t_2)$

D'autre part les classes d'équivalences s'identifient une-à-une avec les éléments de système de racines de groupe de Weyl W^1. On a déjà vu que ce système de racine était de type :

$$\begin{aligned} C_k &\text{ si } G^1 = {}^2A_{2k-1} \\ B_k &\text{ si } G^1 = {}^2A_{2k} \\ B_{l-1} &\text{ si } G^1 = {}^2D_l \\ F_4 &\text{ si } G^1 = {}^2E_6 \\ G_2 &\text{ si } G^1 = {}^3D_4 \end{aligned}$$

Dans tous les cas sauf $G^1 = {}^2A_2$, W^1 n'a pas toutes ses racines de même longueur, et deux classes d'équivalence correspondent à des racines de même longueur si et seulement si elles sont de même type. On sait de plus que W^1 opère transitivement sur les racines d'une longueur donnée, et comme $n_w X_S^1 n_w^{-1} = X^1_{w(S)}$, $w \in W^1$ on remarque que G^1 opère transitivement par conjugaison sur les sous-groupes X_S^1 d'un type donné. Il est ainsi suffisant de montrer qu'un sous-groupe de chaque type est inclus dans $D(G^1)$.
Supposons que le diagramme de Dynkin de W^1 a un double lien. Soient S_1, S_2 les deux classes d'équivalence correspondant aux racines fondamentales liées par ce lien. Si $G^1 \neq {}^2A_2$, ces classes sont de type A_1 et $A_1 \times A_1$. Notons alors $S_1 = \{r, \bar{r}\},\ S_2 = \{s\}$. On peut obtenir la relation de commutation :

$$[x_{S_2}(u), x_{S_1}(t)] = x_{S_3}(tu)x_{S_4}(t\bar{t}u)$$

avec $S_3 = \{r+s, \bar{r}+s\}$ et $S_4 = \{r+\bar{r}+s\}$ ainsi $x_{S_3}(tu)x_{S_4}(t\bar{t}u) \in D(G^1)\ \forall t\ \in \mathbb{K}, \forall u \in \mathbb{K}_0$ Or $x_{S_3}(tu) \in D(G^1)$ comme S_3 est de type $A_1 \times A_1$. Donc $X^1_{S_4} \subseteq D(G^1)$. D'où le résultat.
Si $G^1 = {}^2A_2$, les classes d'équivalence sont de type $A_1 \times A_1$ et A_2. En prenant $S_1 = \{r, \bar{r}\}$ et $S_2 = \{s, \bar{s}, s+\bar{s}\}$, on obtient le résultat de façon similaire. De la même manière si $G^1 = {}^3D_4$.

III.8 Identification avec des groupes classiques

On montre ici que ${}^2A_l(q^2)$ et ${}^2D_l(q^2)$ sont isomorphes à certains groupes classiques.

Théorème III.8.1 : ${}^2A_l$ est isomorphe au groupe unitaire $PSU_{l+1}(\mathbb{K}, F)$ qui laisse invariant la forme hermitienne :

$$f = \epsilon(\bar{x_0}x_l - \bar{x_1}x_{l-1} + \bar{x_2}x_{l-2} - \dots)$$

avec matrice

$$A = \epsilon \begin{pmatrix} & & & & & 1 \\ & & & & -1 & \\ & & & 1 & & \\ & & -1 & & & \\ & \cdot & & & & \\ \cdot & & & & & \\ \cdot & & & & & \end{pmatrix}$$

Ici, ϵ est défini comme valant 1 si l est pair et comme étant un élément de $\mathbb{K}$ tel que $\bar{\epsilon} = -\epsilon$.

Preuve : En effet, on sait qu'il existe un automorphisme de l'algèbre de Lie $\mathfrak{L}$ tel que $e_r \mapsto e_{\bar{r}}$ et $h_r \mapsto h_r$, pour $r \in \Pi$ ou $-r \in \Pi$. En passant au corps $\mathbb{K}$, on obtient un automorphisme de $\mathfrak{L}_{\mathbb{K}}$. Si nous le combinons ensuite avec l'automorphisme $t \mapsto \bar{t}$ de $\mathbb{K}$, on obtient un "semi-automorphisme" ψ tel que :

$$\psi(h_r) = h_{\bar{r}}, \qquad \psi(e_r) = e_{\bar{r}} \qquad r \in \pm\Pi$$

$$\psi(\lambda x + \mu y) = \bar{\lambda}\psi(x) + \bar{\mu}\psi(y), \qquad \lambda, \mu \in \mathbb{K}; x, y \in \mathfrak{L}_{\mathbb{K}}$$

Considérons l'application $\theta \mapsto \psi\theta\psi^{-1}$ où θ est un élément du groupe de Chevalley $G = \mathfrak{L}(\mathbb{K})$. C'est un automorphisme, et on a pour $r \in \pm\Pi$:

$$\begin{aligned}\psi x_r(t)\psi^{-1} &= \psi \exp(\mathrm{ad}\ te_r)\psi^{-1} \\ &= \exp \mathrm{ad}(\psi \cdot te_r) = x_{\bar{r}}(\bar{t})\end{aligned}$$

On en déduit que la fonction est un automorphisme de G. Cependant, on constante aussi que la fonction coïncide sur les générateurs $x_r(t)$ avec σ, donc lui est égal. Les éléments fixant σ sont donc ceux qui commutent avec ψ.
Dans notre cas, $\mathfrak{L}_{\mathbb{K}}$ peut-être pris comme étant l'algèbre de Lie des matrices $(l+1) \times (l+1)$ de trace nulle ; les racines fondamentales comme $E_{i,i+1}$ pour $i = 0, 1, \ldots l-1$ et les co-racines fondamentales $E_{i,i} - E_{i+1,i+1}$ sur les mêmes i.
L'automorphisme de $\mathfrak{L}_{\mathbb{K}}$ donné par la symétrie du diagramme de Dynkin agit de la façon suivante :

$$E_{i,i+1} \mapsto E_{l-i-1,l-i}$$

$$E_{i,i} - E_{i+1,i+1} \mapsto E_{l-i-1,l-i-1} - E_{l-i,l-i}$$

On vérifie maintenant que l'automorphisme de $\mathfrak{L}_{\mathbb{K}}$: $M \mapsto -A^{-1t}MA$ coïncide avec le précédent sur les vecteurs fondamentaux ; ce sont donc les mêmes. Le semi-automorphisme ψ défini précédemment s'écrit donc :

$$\psi : M \mapsto -A^{-1t}\bar{M}A$$

On a aussi vu que G consistait en les automorphismes de $\mathfrak{L}_{\mathbb{K}}$ donnés par :

$$M \mapsto TMT^{-1}, T \in SL_{l+1}(\mathbb{K})$$

Repérons ceux qui commutent avec ψ. Si c'est le cas, on obtient que :

$${}^t\bar{T}ATA^{-1} = \lambda I$$

, avec $\lambda \in \mathbb{K}$. On a donc ${}^t\bar{T}AT = \lambda A$.
Supposons que T est une matrice triangulaire supérieure ou inférieure de diagonale remplie de 1. On obtient en comparant les coefficients, dans les deux cas, que $\lambda = 1$. Ainsi les matrices T amenant les éléments de U^1 *(resp. V^1)* sont précisément les matrices T triangulaires supérieures de diagonale remplie de 1 de $SU_{l+1}(\mathbb{K}, f)$ *(resp. inférieures)*. Toutefois, ces éléments l'engendrent : ainsi G^1 consiste en toutes les transformations $M \mapsto TM{}^tT$ avec $T \in SU_{l+1}(\mathbb{K}, f)$. D'où G^1 est isomorphe à $PSU_{l+1}(K, f)$

Théorème III.8.2 : ${}^2D_l(\mathbb{K})$ est isomorphe au groupe orthogonal $P\Omega_{2l}(\mathbb{K}_0, f)$, où $\mathbb{K}_0$ est le sous-corps fixant σ dans la définition de ${}^2D_l$, et f est la forme quadratique :

$$x_1x_{-1} + x_2x_{-2} + \cdots + x_{l-1}x_{-(l-1)} + (x_l - \alpha x_{-l})(x_l - \bar{\alpha}x_{-l})$$

où α est un générateur de $\mathbb{K}$ par rapport à $\mathbb{K}_0$. *Remarquons que la forme quadratique f est définie sur $\mathbb{K}_0$. Elle est d'indice $l-1$ en tant que forme sur $\mathbb{K}_0$, et d'indice l en tant que forme sur $\mathbb{K}$.*
Preuve : On a déjà vu que $D_l(\mathbb{K})$ était isomorphe au groupe orthogonal $P\Omega_{2l}(K, f_D)$, où f_D est la forme :

$$y_1y_{-1} + \cdots + y_ly_{-l}$$

Posons la matrice de f_D :

$$A = \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix}$$

Le groupe $\Omega_{2l}(\mathbb{K}, f_D)$ est le sous-groupe dérivé de $O_{2l}(\mathbb{K}, f_D)$. Il est engendré par les matrices $\exp(te_r)$, avec $r \in \pm\Pi$ et $t \in \mathbb{K}$, et toutes ses matrices T satisfont l'identité ${}^tAT = A$. Si on utilise la représentation matricielle déjà évoquée dans l'identification des groupes de Chevalley, les matrices $\exp(te_r)$ pour $r \in \Pi$ sont :

$$I + t(e_{12} - e{-}2e_{-1}), \ldots I + t(e_{l-1,l} - e{-}le_{-(l-1)}), I + t(e_{l-1,-l} - e{-}le_{-(l-1)})$$

Considérons maintenant l'application :

$$\exp(te_r) \mapsto \exp(te_{\bar{r}}), \quad r \in \pm\Pi$$

qui est en fait la conjugaison par la matrice

$$\begin{pmatrix} I_l & & & \\ & 0 & (0) & 1 \\ & (0) & I_{l-2} & (0) \\ & 1 & (0) & 0 \end{pmatrix}$$

(qui dans une base idoine, s'écrit

$$B = \begin{pmatrix} I_{2l-2} & 0 \\ 0 & B_0 \end{pmatrix}$$

avec

$$B_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix})$$

L'application $\exp(te_r) \mapsto \exp(\bar{t}e_{\bar{r}})$ s'écrit matriciellement :

$$T \mapsto B^{-1}\bar{T}B$$

On va considérer les matrices fixant cette application. Ce sont celles de $\Omega_{2l}(\mathbb{K}, f_D)$ qui satisfont $BT = \bar{T}B$. Procèdons au changement de base tel que les coordonnées $y_1, \ldots y_l, y_{-1}, \ldots y_{-l}$ deviennent

$x_1, \dots x_l, x_{-1}, \dots x_{-l}$ avec

$$\begin{aligned} \text{pour } i \neq \pm l, \quad & y_i = x_i \\ & y_l = x_l - \alpha x_{-l} \\ & y_{-l} = x_l - \bar{\alpha} x_{-l} \end{aligned}$$

Alors la matrice de la forme quadratique f_D par rapport à cette nouvelle base est ${}^t SAS$, avec

$$S = \begin{pmatrix} I_{2l-2} & 0 \\ 0 & S_0 \end{pmatrix}$$

$$A = \begin{pmatrix} \begin{matrix} 0 & I_{l-1} \\ I_{l-1} & 0 \end{matrix} & (0) \\ (0) & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{pmatrix}$$

$$S_0 = \begin{pmatrix} 1 & -\alpha \\ 1 & -\bar{\alpha} \end{pmatrix}$$

Remarquons que M vérifie ${}^t M({}^t SAS)M = {}^t SAS$ si et seulement si $T := SMS^{-1}$ vérifie ${}^t TAT = A$. On considère ainsi naturellement le sous-groupe conjugué $S^{-1}\Omega_{2l}(\mathbb{K}, f_D)S$ et on va donc chercher quelles matrices M de ce sous-groupe correspondent aux matrices $T \in \Omega_{2l}(\mathbb{K}, f_D)$ telle que $BT = \bar{T}B$. Soit

$$M = \begin{array}{cc} \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} & \begin{matrix} 2l-2 \\ 2 \end{matrix} \end{array}$$

Or $B_0 S_0 = \bar{S_0}$, donc par produit, il vient que $BT = \bar{T}B$ lorsque

$$M_{11} = \bar{M_{11}} \qquad M_{12} = \bar{M_{12}} \qquad M_{21} = \bar{M_{21}} \qquad M_{22} = \bar{M_{22}}$$

Ainsi, le sous-groupe des éléments T fixant σ est $S\Omega_{2l}(\mathbb{K}_0, f)S^{-1}$. Comme G est isomorphe à $P\Omega_{2l}(\mathbb{K}, f_D)$, il vient que G^1 est isomorphe à $P\Omega_{2l}(\mathbb{K}_0, f)$.

Références

[1] R. Carter, Simple groups of Lie type, 1972

[2] Jean-Pierre Serre, Algèbres de Lie Semi-Simples Complexes, 1966

[3] N.Bourbaki, Groupes et algèbres de Lie, Chapitres 7-8, 1968

[4] Terence Tao, "Notes on the classification of complex Lie algebras" `https://terrytao.wordpress.com/2013/04/27/notes-on-the-classification-of-complex-lie-algebras`