

EXPOSÉ XXI

DONNÉES RADICIELLES

par M. DEMAZURE

Cet exposé rassemble, en l'absence de référence convenable, des résultats connus sur les données radicielles (= systèmes de racines « abstraits ») dont la plupart seront utilisés par la suite. 85

Notations. — On désigne par \mathbb{Q}_+ l'ensemble des nombres rationnels positifs (ou nuls); on a $\mathbb{Z} \cap \mathbb{Q}_+ = \mathbb{N}$. Soit V un \mathbb{Q} -espace vectoriel; si A (resp. B) est une partie de \mathbb{Q} (resp. V), on note $A \cdot B$ l'image de $A \otimes B$ par le morphisme $\mathbb{Q} \otimes V \rightarrow V$, autrement dit l'ensemble des combinaisons linéaires d'éléments de B à coefficients dans A . On note $-B = \{-1\}B$. On désigne par $E - F$ l'ensemble des éléments de E qui n'appartiennent pas à F .

1. Généralités

1.1. Définitions, premières propriétés. —

Définition 1.1.1. — Soient M et M^* deux \mathbb{Z} -modules libres de type fini en dualité. On note $V = M \otimes \mathbb{Q}$, $V^* = M^* \otimes \mathbb{Q}$; ce sont deux \mathbb{Q} -espaces vectoriels en dualité. On identifie M (resp. M^*) à une partie de V (resp. V^*). La forme bilinéaire canonique sur $M^* \times M$ (resp. $V^* \times V$) est notée $(\ , \)$.

Soit R une partie *finie* de M . Donnons-nous une application $\alpha \mapsto \alpha^*$ de R dans M^* ; l'ensemble des α^* , $\alpha \in R$, est noté R^* . À chaque $\alpha \in R$, on associe l'endomorphisme s_α (resp. s_α^*) de M et V (resp. M^* et V^*) donné par les formules :

$$\begin{aligned} (1) \quad & s_\alpha(x) = x - (\alpha^*, x)\alpha, & \text{i.e.} \quad & s_\alpha = \text{id} - \alpha^* \otimes \alpha; \\ (1^*) \quad & s_\alpha^*(u) = u - (u, \alpha)\alpha^*, & \text{i.e.} \quad & s_\alpha^* = \text{id} - \alpha \otimes \alpha^*. \end{aligned}$$

On dit que le couple (R, R^*) (plus précisément le couple $(R, R \rightarrow M^*)$) est une *donnée radicielle dans* (M, M^*) , ou que (M, M^*, R, R^*) est une *donnée radicielle*, si les axiomes

⁽⁰⁾version α du 23 mai 2009

suivants sont vérifiés :

(DR I) Pour chaque $\alpha \in R$, on a $(\alpha^*, \alpha) = 2$.

(DR II) Pour chaque $\alpha \in R$, on a $s_\alpha(R) \subseteq R$, $s_\alpha^*(R^*) \subseteq R^*$.

On dit que R est le *système de racines* de la donnée radicielle $\mathcal{R} = (M, M^*, R, R^*)$. Les éléments de R (resp. R^*) sont dits les *racines* (resp. *coracines*) de la donnée radicielle.

Remarque 1.1.2. — L'axiome (DR I) est équivalent à l'une quelconque des propriétés suivantes :

$$\begin{aligned} (2) \quad s_\alpha s_\alpha &= \text{id} & , & & (2^*) \quad s_\alpha^* s_\alpha^* &= \text{id}, \\ (3) \quad s_\alpha(\alpha) &= -\alpha & , & & (3^*) \quad s_\alpha^*(\alpha^*) &= -\alpha^*. \end{aligned}$$

Remarque 1.1.3. — Les axiomes (DR I) et (DR II) entraînent

$$R = -R, \quad R^* = -R^*, \quad 0 \notin R, \quad 0 \notin R^*.$$

87 **Lemme 1.1.4.** — *L'application $R \rightarrow R^*$ est une bijection. Plus généralement, si $\alpha, \beta \in R$ et $(\alpha^*, x) = (\beta^*, x)$ pour tout $x \in R$, alors $\alpha = \beta$.*

En effet, on a alors $s_\beta(\alpha) = \alpha - 2\beta$, $s_\alpha(\beta) = \beta - 2\alpha$. On en déduit aussitôt

$$s_\beta s_\alpha(\alpha) = 2\beta - \alpha = \alpha + 2(\beta - \alpha), \quad s_\beta s_\alpha(\beta - \alpha) = s_\beta(\beta - \alpha) = \beta - \alpha,$$

d'où $(s_\beta s_\alpha)^n(\alpha) = \alpha + 2n(\beta - \alpha) \in R$ par (DR II). Comme R est fini, on a $\beta - \alpha = 0$.

Corollaire 1.1.5. — *L'application inverse $R^* \rightarrow R$ définit une donnée radicielle*

$$\mathcal{R}^* = (M^*, M, R^*, R)$$

dite duale de \mathcal{R} . ⁽¹⁾

Définition 1.1.6. — On note $\Gamma_0(R)$ le sous-groupe de M engendré R . On note $\mathcal{V}(R)$ le sous-espace vectoriel de V engendré par R , c'est-à-dire $\Gamma_0(R) \otimes \mathbb{Q}$. Appliquant ces définitions à \mathcal{R}^* , on construit de même $\Gamma_0(R^*)$ et $\mathcal{V}(R^*)$.

On appelle *rang réductif* de \mathcal{R} le nombre

$$\text{rgred}(\mathcal{R}) = \text{rang}(M) = \dim(V) = \dim(V^*) = \text{rang}(M^*) = \text{rgred}(\mathcal{R}^*).$$

On appelle *rang semi-simple* de \mathcal{R} le nombre

$$\text{rgss}(\mathcal{R}) = \text{rang}(R) = \text{rang}(\Gamma_0(R)) = \dim(\mathcal{V}(R)).$$

On a donc $\text{rgss}(\mathcal{R}) \leq \text{rgred}(\mathcal{R})$.

On verra ci-dessous que $\text{rgss}(\mathcal{R}) = \text{rgss}(\mathcal{R}^*)$, c'est-à-dire que $\mathcal{V}(R)$ et $\mathcal{V}(R^*)$ ont même dimension.

88 **Définition 1.1.7.** — On dit que \mathcal{R} est *semi-simple* (resp. *triviale*) si $\text{rgss}(\mathcal{R}) = \text{rgred}(\mathcal{R})$ (resp. $\text{rgss}(\mathcal{R}) = 0$). Pour que \mathcal{R} soit triviale, il est donc nécessaire et suffisant que R soit vide. La donnée radicielle triviale de rang réductif nul est notée $0 = (\{0\}, \{0\}, \emptyset, \emptyset)$.

⁽¹⁾N.D.E. : On notera que $(\alpha^*)^* = \alpha$.

Définition 1.1.8. — On note $W(\mathcal{R})$ le groupe de transformations de M engendré par les s_α , $\alpha \in R$. On l'appelle le *groupe de Weyl* de \mathcal{R} . On note

$$W^*(\mathcal{R}) = W(\mathcal{R}^*).$$

Alors $W(\mathcal{R})$ opère dans $R, \Gamma_0(R), \mathcal{V}(R), M$ et V . Si $w \in W(\mathcal{R})$ et $x \in M$ (resp. $x \in V$), on a $wx - x \in \Gamma_0(R)$ (resp. $wx - x \in \mathcal{V}(R)$), c'est immédiat sur la formule (1). De même pour $W^*(\mathcal{R})$.

Lemme 1.1.9. — Pour tous $\alpha \in R, x \in V, u \in V^*$, on a

$$(4) \quad (s_\alpha^*(u), s_\alpha(x)) = (u, x).$$

En effet, en faisant le produit scalaire de (1) et (1*), on trouve que le premier membre est égal à $(u, x) + (u, \alpha)(\alpha^*, x)((\alpha^*, \alpha) - 2) = (u, x)$.

Remarque 1.1.10. — Si on suppose $0 \notin R$ et $0 \notin R^*$, alors 1.1.9 équivaut à (DR I).

Corollaire 1.1.11. — Notons $h \mapsto h^\vee$ l'isomorphisme de $GL(M)$ sur $GL(M^*)$ qui associe à h son contragrédient. Alors la formule (4) s'écrit aussi

$$(5) \quad (s_\alpha)^\vee = s_\alpha^*.$$

Corollaire 1.1.12. — L'isomorphisme précédent induit un isomorphisme de $W(\mathcal{R})$ sur $W^*(\mathcal{R})$. 89

Scolie 1.1.13. — En vertu du résultat précédent, nous identifierons W et W^* , et nous considérerons W comme un groupe de transformations de $R, R^*, M, M^*, \Gamma_0(R), \Gamma_0(R^*), V, V^*, \mathcal{V}(R), \mathcal{V}(R^*)$. Nous écrirons s_α pour s_α^* .

1.2. L'application p . —

Lemme 1.2.1. — Soit $p : M \rightarrow M^*$ (resp. $V \rightarrow V^*$) l'application linéaire définie par

$$(6) \quad p(x) = \sum_{u \in R^*} (u, x)u.$$

Notons $\ell(x) = (p(x), x)$. On a les propriétés suivantes :

$$(7) \quad \ell(x) \geq 0, \quad \ell(\alpha) > 0 \quad \text{pour } \alpha \in R.$$

$$(8) \quad \ell(wx) = \ell(x), \quad \text{pour } w \in W.$$

$$(9) \quad (p(x), y) = (p(y), x), \quad \text{pour } x, y \in V.$$

$$(10) \quad \ell(\alpha)\alpha^* = 2p(\alpha), \quad \text{pour } \alpha \in R.$$

Les trois premières relations sont immédiates ⁽²⁾. Démontrons la dernière. On a par (1), pour $u \in V^*$:

$$\begin{aligned} (u, \alpha)^2 \alpha^* &= (u, \alpha) u - (u, \alpha) s_\alpha(u) \\ &= (u, \alpha) u + (u, s_\alpha(\alpha)) s_\alpha(u) \\ &= (u, \alpha) u + (s_\alpha(u), \alpha) s_\alpha(u) \quad (\text{car } s_\alpha^2 = \text{id}). \end{aligned}$$

90 Comme s_α est une permutation de R^* (par (DR II)), il n'y a plus qu'à sommer sur $u \in R^*$ pour conclure.

Scolie 1.2.2. — La relation (10) dit que $\alpha \mapsto \ell(\alpha)\alpha^*$ est la restriction à R d'une application linéaire de M dans M^* . En particulier, on a

$$(-\alpha)^* = -\alpha^*.$$

Corollaire 1.2.3. — *L'application p induit un isomorphisme de $\mathcal{V}(R)$ sur $\mathcal{V}(R^*)$.*

En effet, p envoie $\mathcal{V}(R)$ sur $\mathcal{V}(R^*)$. On a donc

$$\dim(\mathcal{V}(R)) \geq \dim(\mathcal{V}(R^*)).$$

En appliquant cette formule à la donnée radicielle duale, on en déduit

$$\dim(\mathcal{V}(R)) = \dim(\mathcal{V}(R^*)),$$

donc p , étant surjectif, est aussi bijectif.

Corollaire 1.2.4. — *On a $\dim(\mathcal{V}(R)) = \dim(\mathcal{V}(R^*))$, donc*

$$\text{rgss}(\mathcal{R}) = \text{rgss}(\mathcal{R}^*).$$

Corollaire 1.2.5. — *La forme bilinéaire (u, x) est non dégénérée sur $\mathcal{V}(R^*) \times \mathcal{V}(R)$, donc met ces \mathbb{Q} -espaces vectoriels en dualité.*

En effet, si $(u, x) = 0$ pour tout $u \in R^*$, alors $p(x) = 0$.

Corollaire 1.2.6. — *La forme bilinéaire symétrique $(p(x), y)$ est positive non dégénérée sur $\mathcal{V}(R)$.*

91 **Corollaire 1.2.7.** — *W opère fidèlement dans R (et donc dans les autres ensembles de 1.1.13).*

En effet, soit $u \in V^*$. Soit $w \in W$, supposons que $w(\alpha) = \alpha$ pour tout $\alpha \in R$ et prouvons que $w(u) = u$. On a

$$(w(u) - u, \alpha) = (w(u), \alpha) - (u, \alpha) = (u, w^{-1}(\alpha)) - (u, \alpha) = 0.$$

Mais $w(u) - u \in \mathcal{V}(R^*)$. S'il est orthogonal à toutes les racines, il est nul par 1.2.5.

Corollaire 1.2.8. — *Le groupe W est fini.*

⁽²⁾N.D.E. : (8) résulte de (4), (2) et (DR II).

Proposition 1.2.9. — *Les opérations de W respectent la correspondance entre racines et coracines. En d'autres termes, pour $\alpha \in R$ et $w \in W$, on a*

$$w(\alpha^*) = w(\alpha)^*.$$

Il suffit de le vérifier pour $w = s_\beta$, $\beta \in R$, c'est-à-dire de vérifier la formule

$$s_\beta(\alpha^*) = s_\beta(\alpha)^*.$$

Or, $\ell(s_\beta(\alpha)) s_\beta(\alpha)^*/2$ égale :

$$p(s_\beta(\alpha)) = \sum_{u \in R^*} (u, s_\beta(\alpha)) u = \sum_{u \in R^*} (s_\beta(u), \alpha) u = \sum_{u \in R^*} (u, \alpha) s_\beta(u) = s_\beta(p(\alpha));$$

comme $\ell(s_\beta(\alpha)) = \ell(\alpha)$, on obtient $s_\beta(\alpha)^* = s_\beta(2p(\alpha)/\ell(\alpha)) = s_\beta(\alpha^*)$.

Corollaire 1.2.10. — *Si $\alpha \in R$ et $w \in W$, on a*

$$ws_\alpha w^{-1} = s_{w(\alpha)}.$$

92

En effet, $ws_\alpha w^{-1}(x) = x - (\alpha^*, w^{-1}(x)) w(\alpha) = x - (w(\alpha^*), x) w(\alpha)$, et ce dernier terme égale, d'après 1.2.9 :

$$x - (w(\alpha)^*, x) w(\alpha) = s_{w(\alpha)}(x).$$

Corollaire 1.2.11. — ⁽³⁾ *Soit $R' \subseteq R$. Pour que (M, M^*, R', R'^*) soit une donnée radicielle, il faut et il suffit que $\alpha, \beta \in R'$ entraîne $s_\alpha(\beta) \in R'$.*

2. Relations entre deux racines

2.1. Racines proportionnelles. —

Proposition 2.1.1. — *Soient α et β deux racines. Les conditions suivantes sont équivalentes :*

- (i) *Il existe $k \in \mathbb{Q}$ tel que $\alpha = k\beta$.*
- (ii) *$s_\alpha = s_\beta$.*

De plus, sous ces conditions, on a $\alpha^ = k^{-1}\beta^*$ et k est égal à l'un des nombres 1, -1, 2, -2, 1/2, -1/2.*

Supposons d'abord (i). On a d'abord

$$\alpha^* = \ell(\alpha)^{-1} 2p(\alpha) = k^{-2} \ell(\beta)^{-1} 2kp(\beta) = k^{-1} \beta^*.$$

Cela entraîne aussitôt $s_\alpha = s_\beta$. Réciproquement, si on a $s_\alpha = s_\beta$, alors

$$\alpha = s_\alpha(-\alpha) = s_\beta(-\alpha) = (\beta^*, \alpha) \beta - \alpha,$$

d'où $2\alpha = (\beta^*, \alpha) \beta$, avec $(\beta^*, \alpha) \in \mathbb{Z}$, donc (ii) entraîne (i). Enfin, si $\alpha = k\beta$, alors $\alpha^* = k^{-1}\beta^*$, d'où

$$(\alpha^*, \beta) = 2k^{-1}, \quad (\beta^*, \alpha) = 2k,$$

donc $2k$ et $2k^{-1}$ sont des entiers et on a terminé.

93

⁽³⁾N.D.E. : de la proposition 1.2.9.

Application 2.1.2. — Les données radicielles \mathcal{R} telles que $\text{rgss}(\mathcal{R}) = 1$ sont de l'un des deux types suivants :

- (i) Type A_1 : il existe un $\alpha \in M$ tel que les racines soient α et $-\alpha$.
Les coracines sont alors α^* et $-\alpha^*$.
- (ii) Type A'_1 : il existe un $\alpha \in M$ tel que les racines soient α , $-\alpha$, 2α , -2α .
Les coracines sont alors α^* , $-\alpha^*$, $\alpha^*/2$, $-\alpha^*/2$.

Définition 2.1.3. — On dit que $\alpha \in R$ est *indivisible* si $\alpha/2 \notin R$. On dit que \mathcal{R} est *réduite* si toute racine est indivisible.

Pour que \mathcal{R} soit réduite, il faut et il suffit que \mathcal{R}^* le soit. Si α est indivisible et si $w \in W$, alors $w(\alpha)$ est indivisible.

Définition 2.1.4. — Soit $\alpha \in R$. Si α est indivisible, on pose $\text{ind}(\alpha) = \alpha$. Sinon, on pose $\text{ind}(\alpha) = \alpha/2$.

Corollaire 2.1.5. — Si $\alpha \in R$ est indivisible et si $k\alpha \in R$, où $k \in \mathbb{Q}$, alors $k \in \mathbb{Z}$.

Proposition 2.1.6. — Soit \mathcal{R} une donnée radicielle. Alors

$$\text{ind}(\mathcal{R}) = (M, M^*, \text{ind}(R), \text{ind}(R)^*)$$

est une donnée radicielle réduite, et l'on a

$$W(\text{ind}(\mathcal{R})) = W(\mathcal{R}).$$

En effet, $\text{ind}(\mathcal{R})$ est une donnée radicielle par 1.2.11, car le groupe de Weyl permute les racines indivisibles. La seconde assertion résulte de 2.1.1.

94 **Remarque 2.1.7.** — Si \mathcal{R} n'est pas réduite, on a $\text{ind}(R)^* \neq \text{ind}(R^*)$ et donc $\text{ind}(\mathcal{R}^*) \neq \text{ind}(\mathcal{R})^*$.

2.2. Racines orthogonales. —

Lemme 2.2.1. — Soient α et β deux racines. On a

$$(11) \quad \ell(\alpha)(\alpha^*, \beta) = \ell(\beta)(\beta^*, \alpha).$$

Cela résulte aussitôt de 1.2.1, formules (9) et (10).

Corollaire 2.2.2. — Soient $\alpha, \beta \in R$. Les conditions suivantes sont équivalentes :

- (i) $(\alpha^*, \beta) = 0$,
- (ii) $(p(\alpha), \beta) = 0$,
- (iii) $s_\alpha(\beta) = \beta$,
- (iv) $s_\alpha(\beta^*) = \beta^*$,
- (v) $s_\alpha \neq s_\beta$ et s_α et s_β commutent.
- (i bis) $(\beta^*, \alpha) = 0$,
- (iii bis) $s_\beta(\alpha) = \alpha$,
- (iv bis) $s_\beta(\alpha^*) = \alpha^*$,

Toutes les équivalences sont immédiates, sauf celles qui portent sur (v). Montrons que (i) (et (i bis)) entraînent (v). On a

$$s_\alpha s_\beta(x) = x - (\beta^*, x)\beta - (\alpha^*, x)\alpha + (\beta^*, x)(\alpha^*, \beta)\alpha.$$

Si $(\alpha^*, \beta) = 0$, alors $(\beta^*, \alpha) = 0$ et $s_\alpha s_\beta(x) = s_\beta s_\alpha(x)$.

Supposons réciproquement (v). On a alors

$$s_\alpha = s_\beta s_\alpha s_\beta = s_{s_\beta(\alpha)} \quad (\text{par 1.2.10}).$$

Par 2.1, il existe donc $k \in \mathbb{Q}^*$ tel que $\alpha = k s_\beta(\alpha) = k \alpha - k(\beta^*, \alpha) \beta$. Comme $s_\alpha \neq s_\beta$, alors β et α ne sont pas proportionnelles par 2.1.1, donc $(\beta^*, \alpha) = 0$.

Définition 2.2.3. — Deux racines vérifiant les conditions équivalentes de 2.2.2 sont dites *orthogonales*.

Remarque 2.2.4. — Les racines α et β sont orthogonales si et seulement si les coracines α^* et β^* sont orthogonales. 95

Lemme 2.2.5. — Si α et β sont deux racines orthogonales, alors $\alpha + \beta \in R$ si et seulement si $\alpha - \beta \in R$.

En effet $s_\beta(\alpha + \beta) = s_\beta(\alpha) + s_\beta(\beta) = \alpha - \beta$.

Lemme 2.2.6. — Soient α et β deux racines non orthogonales. Si on définit $\ell(\gamma^*)$ pour une coracine γ^* comme ℓ de la racine γ^* de \mathcal{R}^* , on a la relation

$$(12) \quad \ell(\alpha)\ell(\alpha^*) = \ell(\beta)\ell(\beta^*).$$

En effet, multipliant la formule (11) par la formule correspondante pour \mathcal{R}^* , et tenant compte de l'égalité $(\gamma^*)^* = \gamma$ pour tout $s \in R$, on trouve :

$$(\beta^*, \alpha) (\alpha^*, \beta) \ell(\alpha) \ell(\alpha^*) = (\beta^*, \alpha) (\alpha^*, \beta) \ell(\beta) \ell(\beta^*).$$

2.3. Cas général. —

Proposition 2.3.1. — Si α et β sont deux racines quelconques, on a

$$(13) \quad 0 \leq (\alpha^*, \beta)(\beta^*, \alpha) \leq 4.$$

Si α et β ne sont ni proportionnelles, ni orthogonales, on a

$$1 \leq (\alpha^*, \beta)(\beta^*, \alpha) \leq 3.$$

En effet, on a $4(p(\alpha), \beta)^2 = \ell(\alpha)\ell(\beta)(\alpha^*, \beta)(\beta^*, \alpha)$. D'autre part, d'après 1.2.6, la forme bilinéaire symétrique $(p(x), y)$ est positive non dégénérée sur $\mathcal{V}(R)$, d'où $(p(x), y)^2 \leq \ell(x)\ell(y)$.

Corollaire 2.3.2. — Soient α et β deux racines non orthogonales. Si $\ell(\alpha) = \ell(\beta)$, il existe $w \in W$ tel que $w(\alpha) = \beta$.

En effet, si α et β sont proportionnelles, comme $\ell(\alpha) = \ell(\beta)$, on a $\alpha = \beta$ ou $\alpha = -\beta$; en ce cas on prend $w = 1$ ou $w = s_\alpha$. Si α et β ne sont ni proportionnelles, ni orthogonales, on a, d'après la formule (11) et 2.3.1 :

$$(\beta^*, \alpha) = (\alpha^*, \beta) = \pm 1.$$

Si $(\beta^*, \alpha) = (\alpha^*, \beta) = 1$, on prend $w = s_\beta s_\alpha s_\beta$. Si $(\beta^*, \alpha) = (\alpha^*, \beta) = -1$, on prend $w = s_\alpha s_\beta$.

Corollaire 2.3.3. — Si α et β sont deux racines, si $\alpha \neq \beta$ et $(\beta^*, \alpha) > 0$ (resp. si $\alpha \neq -\beta$ et $(\beta^*, \alpha) < 0$), alors $\alpha - \beta$ (resp. $\alpha + \beta$) est une racine.

Le second cas se déduit du premier en changeant β en $-\beta$. Si α et β sont proportionnelles et si $(\beta^*, \alpha) > 0$, alors on a $\beta = \alpha$, $2\beta = \alpha$ ou $\beta = 2\alpha$. Le premier cas est exclu. Dans les autres, on a respectivement $\alpha - \beta = \beta \in \mathbb{R}$ ou $\alpha - \beta = -\alpha \in \mathbb{R}$. Si α et β ne sont pas proportionnelles, (α^*, β) et (β^*, α) sont deux entiers strictement positifs de produit au plus 3. L'un d'eux est donc égal à 1. Si $(\beta^*, \alpha) = 1$, on a $\alpha - \beta = s_\beta(\alpha) \in \mathbb{R}$; si $(\alpha^*, \beta) = 1$, on a $\alpha - \beta = -s_\alpha(\beta) \in \mathbb{R}$.

Lemme 2.3.4. — Soient α et β deux racines non proportionnelles. Si $\beta - \alpha$ n'est pas racine, alors $\beta + k\alpha \in \mathbb{R}$ pour $k = -(\alpha^*, \beta)$, mais pas pour $k = -(\alpha^*, \beta) + 1$.

En effet, on a $\beta - (\alpha^*, \beta)\alpha = s_\alpha(\beta) \in \mathbb{R}$, mais $\beta + (-(\alpha^*, \beta) + 1)\alpha = s_\alpha(\beta - \alpha) \notin \mathbb{R}$.

Proposition 2.3.5. — Soient α et β deux racines non proportionnelles. L'ensemble des entiers k tels que $\beta + k\alpha \in \mathbb{R}$ est un intervalle $[p, q]$ ($p \leq 0$, $q \geq 0$) et on a $p + q = -(\alpha^*, \beta)$.

97 Pour la première assertion, il suffit par exemple de prouver que si $\beta + k\alpha \in \mathbb{R}$, k entier > 0 , alors $\beta + (k - 1)\alpha \in \mathbb{R}$. Si $k = 1$, c'est trivial. Si $k \geq 2$, on a

$$(\alpha^*, \beta + k\alpha) = (\alpha^*, \beta) + 2k \geq -3 + 4 > 0,$$

et on conclut par 2.3.3. Soit donc $[p, q]$ l'intervalle en question. Appliquant 2.3.4 à $\beta + p\alpha$, on trouve

$$q - p = -(\alpha^*, \beta + p\alpha) = -(\alpha^*, \beta) - 2p. \quad (4)$$

Remarque 2.3.6. — La formule précédente contient les énoncés qualitatifs 2.2.5 et 2.3.3.

Compléments 2.3.7. — ⁽⁵⁾ D'après 1.2.1 (9) et 1.2.6, la forme bilinéaire sur $\mathcal{V}(\mathbb{R})$ définie par

$$\langle x, y \rangle = (p(x), y)$$

est symétrique et définie positive. D'après 1.2.1 (10), pour tout $\alpha \in \mathbb{R}$ et $y \in \mathcal{V}(\mathbb{R})$,

$$\langle \alpha, y \rangle = \frac{\ell(\alpha)}{2}(\alpha^*, y),$$

où $\ell(\alpha) = \langle \alpha, \alpha \rangle$. Par conséquent, on déduit de 2.3.3 le corollaire suivant.

Corollaire. — Soient $\alpha \neq \beta$ dans \mathbb{R} . Si $\alpha - \beta \notin \mathbb{R}$, alors $\langle \alpha, \beta \rangle \leq 0$.

⁽⁴⁾N.D.E. : On a corrigé $+2p$ en $-2p$.

⁽⁵⁾N.D.E. : On a ajouté ces compléments, utiles pour la démonstration de 3.1.5.

3. Racines simples, racines positives

3.1. Systèmes de racines simples. —

Lemme 3.1.1. — Soient α et α_i , $i = 1, \dots, n$, des racines. Supposons α distinct des α_i . Si on a une relation

$$\alpha = \sum_{i=1}^n q_i \alpha_i, \quad q_i \in \mathbb{Q}_+,$$

il existe un indice i tel que $q_i \neq 0$, $(\alpha^*, \alpha_i) > 0$, $\alpha - \alpha_i \in \mathbb{R}$.

En effet, on écrit $2 = (\alpha^*, \alpha) = \sum_{i=1}^n q_i (\alpha^*, \alpha_i)$, ce qui prouve les deux premières assertions. La troisième résulte alors de 2.3.3.

Proposition 3.1.2. — Soient α et α_i , $i = 1, \dots, n$, des racines. Si

$$\alpha = \sum_{i=1}^n m_i \alpha_i, \quad m_i \in \mathbb{N}_+,$$

il existe une suite β_1, \dots, β_m de racines prises parmi les α_i (non nécessairement deux à deux distinctes) telle que si l'on note **98**

$$a_p = \sum_{i=1}^p \beta_i, \quad p = 1, \dots, m,$$

on ait $a_p \in \mathbb{R}$ et $a_m = \alpha$.

Raisonnons par récurrence sur l'entier $\sum m_i = m'$. Si α est égal à l'un des α_i , soit α_{i_0} (ce qui est automatique si $m' = 1$), on prend $m = 1$, $\beta_1 = \alpha_{i_0}$. Sinon, on applique le lemme précédent et il existe un indice i tel que $m_i \neq 0$ et que $\alpha - \alpha_i$ soit une racine. On a alors $(m_i - 1) \in \mathbb{N}$ et

$$\alpha - \alpha_i = (m_i - 1) \alpha_i + \sum_{j \neq i} m_j \alpha_j.$$

Il n'y a plus qu'à appliquer l'hypothèse de récurrence à $\alpha - \alpha_i$.

Corollaire 3.1.3. — Soit $\mathbb{R}' \subseteq \mathbb{R}$. Les conditions suivantes sont équivalentes :

- (i) Si $\alpha, \beta \in \mathbb{R}'$ et $\alpha + \beta \in \mathbb{R}$, alors $\alpha + \beta \in \mathbb{R}'$.
- (ii) $\mathbb{N} \cdot \mathbb{R}' \cap \mathbb{R} \subseteq \mathbb{R}'$.

En effet, on clairement (ii) \Rightarrow (i). La réciproque résulte aussitôt de la proposition.

Définition 3.1.4. — Un ensemble de racines vérifiant les conditions de 3.1.3 est dit *clos*.

Proposition 3.1.5. — Soit $S \subseteq \mathbb{R}$ un ensemble de racines. Les conditions suivantes sont équivalentes :

- (i) Les éléments de S sont indivisibles, linéairement indépendants et

$$\mathbb{R} \subseteq \mathbb{Q}_+ \cdot S \cup -\mathbb{Q}_+ \cdot S.$$

(ii) Les éléments de S sont linéairement indépendants et

$$R \subseteq N \cdot S \cup -N \cdot S.$$

(iii) Toute racine s'écrit de manière unique comme une combinaison linéaire des éléments de S , à coefficients entiers tous de même signe.

⁽⁶⁾ On a évidemment (ii) \Rightarrow (iii). Notons $\alpha_1, \dots, \alpha_n$ les éléments (distincts) de S . Prouvons (i) \Rightarrow (ii). Soit $\alpha \in R$. On a donc une écriture unique

$$\varepsilon \alpha = \sum q_i \alpha_i \quad q_i \in \mathbb{Q}_+, \varepsilon = \pm 1.$$

Montrons que les q_i sont entiers. Cela est certainement vrai s'ils sont tous nuls sauf un (cf. 2.1.5). Sinon, α est distinct des α_i et en appliquant 3.1.1, on trouve un i_0 tel que $\alpha' = \varepsilon \alpha - \alpha_{i_0} \in R$ et $q_{i_0} \neq 0$. Cela donne

$$\alpha' = (q_{i_0} - 1) \alpha_{i_0} + \sum_{i \neq i_0} q_i \alpha_i.$$

100 Comme l'un au moins des $q_i, i \neq i_0$ est non nul, (i) entraîne $q_{i_0} - 1 \geq 0$. On recommence l'opération pour α' et au bout d'un nombre fini de pas, on a démontré que les q_i sont entiers.

Montrons (iii) \Rightarrow (i). Montrons que $\alpha_1, \alpha_2, \dots, \alpha_n$ sont linéairement indépendants sur \mathbb{Q} . Dans le cas contraire, on aurait une égalité

$$x = \sum_{i \in I} a_i \alpha_i = \sum_{j \in J} b_j \alpha_j,$$

où I, J sont deux parties disjointes de $\{1, \dots, n\}$, l'une au moins, disons I , étant non vide, et $a_i, b_j \in \mathbb{N}^*$. D'après le corollaire 2.3.7, on a $\langle \alpha_i, \alpha_j \rangle \leq 0$ si $i \in I$ et $j \in J$, d'où $\langle x, x \rangle \leq 0$ et donc $x = 0$. Soit $i_0 \in I$, alors les égalités

$$\alpha_{i_0} = \alpha_{i_0} + \sum_{i \in I} a_i \alpha_i = \alpha_{i_0} + \sum_{j \in J} b_j \alpha_j$$

entraînent (d'après (iii)) $a_i = 0 = b_j$ pour tout i, j , une contradiction. Ceci montre que les éléments de S sont linéairement indépendants sur \mathbb{Q} ; montrons qu'ils sont aussi indivisibles.

Soit donc $\beta \in S$ divisible. On a $\beta/2 \in R$, d'où

$$\beta/2 = \varepsilon \sum_{\alpha \in S} m_\alpha \alpha, \quad m_\alpha \in \mathbb{N}, \varepsilon = \pm 1,$$

donc aussi $\beta = 2\varepsilon \sum_{\alpha} m_\alpha \alpha$, d'où par unicité $m_\alpha = 0$ si $\alpha \neq \beta$ et $2\varepsilon m_\beta = 1$, une contradiction.

Définition 3.1.6. — Un ensemble S de racines vérifiant les conditions de 3.1.5 est dit *système de racines simples*, ou *base de R* .

Si $w \in W$ et si S est un système de racines simples, alors $w(S)$ est un système de racines simples.

⁽⁶⁾N.D.E. : Dans ce qui suit, on a modifié l'ordre et détaillé la preuve de l'implication (iii) \Rightarrow (i).

Remarque 3.1.7. — Cette définition ne fait intervenir que R et non \mathcal{R} , elle ne fait même intervenir en fait que $\text{ind}(R)$.

Remarque 3.1.8. — Si S est un système de racines simples, S est une base du groupe abélien libre $\Gamma_0(R)$. On a donc $\text{Card}(S) = \text{rgss}(\mathcal{R})$.

Remarque 3.1.9. — Les conditions de 3.1.5 sont alors évidemment équivalentes aux suivantes :

- (i') Les éléments de S sont indivisibles, en nombre $\leq \text{rgss}(R)$ et $R \subseteq \mathbb{Q}_+ \cdot S \cup -\mathbb{Q}_+ \cdot S$.
- (ii') On a $\text{Card}(S) \leq \text{rgss}(R)$ et $R \subseteq \mathbb{N} \cdot S \cup -\mathbb{N} \cdot S$.

Corollaire 3.1.10. — Si S est un système de racines simples, alors $\text{ind}(S^*)$ est un système de coracines simples (i.e. un système de racines simples de R^*)

En effet, si $\beta = \sum_{\alpha \in S} a_\alpha \alpha$ ($a_\alpha \in \mathbb{N}$), alors $p(\alpha) = \sum_{\alpha \in S} a_\alpha p(\alpha)$, d'où, d'après 1.2.1 (10) :

$$\beta^* = \sum_{\alpha \in S} a_\alpha \frac{\ell(\alpha)}{\ell(\beta)} \alpha^*,$$

ce qui démontre que $\text{ind}(S^*)$ vérifie (i').

101

(7) D'après 2.1.1, si α^* n'est pas indivisible, alors $\alpha^* = 2u^*$, où $u^* \in \text{ind}(S^*)$ (et $u = 2\alpha$). On en déduit :

Corollaire 3.1.11. — Si S est un système de racines simples et si

$$\beta = \sum_{\alpha \in S} a_\alpha \alpha, \quad a_\alpha \in \mathbb{Z}$$

est l'écriture de β suivant S , alors $2a_\alpha \ell(\alpha)$ est divisible par $\ell(\beta)$ (et même par $2\ell(\beta)$ si α^* est indivisible).

Avant de continuer à énoncer les propriétés des systèmes de racines simples, montrons qu'il en existe.

3.2. Systèmes de racines positives. —

Définition 3.2.1. — Un ensemble $P \subseteq R$ est dit un système de racines positives de \mathcal{R} (ou de R , cf. la remarque 3.2.2), s'il vérifie les conditions suivantes :

- (P 1) $P \cap -P = \emptyset$.
- (P 2) $P \cup -P = R$.
- (P 3) $\mathbb{Q}_+ \cdot P \cap R \subseteq P$.

En particulier, un tel ensemble est clos. On verra plus tard qu'en fait un ensemble clos vérifiant (P 1) et (P 2) vérifie aussi (P 3), donc est un système de racines positives. Si $w \in W$ et si P est un système de racines positives, alors $w(P)$ est un système de racines positives.

Remarque 3.2.2. — Cette définition ne fait intervenir que R . On dira aussi que P est un système de racines positives de R . 102

(7)N.D.E. : On a ajouté la phrase qui suit, et dans 3.1.11 on a remplacé $4a_\alpha \ell(\alpha)$ par $2a_\alpha \ell(\alpha)$.

Remarque 3.2.3. — De (P 1) et (P 2), on tire aussitôt

$$\text{Card}(P) = \text{Card}(R)/2.$$

Il en résulte que si P et P' sont deux systèmes de racines positives et si $P \subseteq P'$, alors $P = P'$.

Remarque 3.2.4. — Si P est un système de racines positives, P^* est un système de coracines positives (i.e. un système de racines positives de R^*).

Cela résulte aussitôt de 1.1.4 et 1.2.2.

Définition 3.2.5. — Soit S un système de racines simples. On pose

$$\mathcal{P}(S) = \mathbb{Q}_+ \cdot S \cap R = \mathbb{N}_+ \cdot S \cap R.$$

Proposition 3.2.6. — Si S est un système de racines simples, $\mathcal{P}(S)$ est un système de racines positives. Si S est un système de racines simples et P un système de racines positives, on a l'équivalence :

$$S \subseteq P \iff P = \mathcal{P}(S).$$

La première assertion est immédiate. Si $S \subseteq P$, alors $\mathcal{P}(S) \subseteq P$ par (P 3), donc $\mathcal{P}(S) = P$ par 3.2.3. Le reste est trivial.

Remarque 3.2.7. — Il existe des systèmes de racines positives : soit \geq une structure d'espace vectoriel totalement ordonné sur $\mathcal{V}(R)$. L'ensemble des racines ≥ 0 pour cette relation d'ordre est un système de racines positives.

103 Théorème 3.2.8. — Soit P un système de racines positives. Il existe un unique système de racines simples $\mathcal{S}(P)$ tel que $\mathcal{S}(P) \subseteq P$, i.e. tel que $P = \mathcal{P}(\mathcal{S}(P))$.

L'unicité résulte aussitôt de :

Lemme 3.2.9. — Soit S un système de racines simples. Alors pour que $\alpha \in \mathcal{P}(S)$ appartienne à S , il faut et il suffit que α ne soit pas somme de deux éléments de $\mathcal{P}(S)$.

Ce lemme résulte aussitôt des définitions et de 3.1.2.

Démontrons maintenant l'existence de $\mathcal{S}(P)$. Considérons l'ensemble des parties T de P telles que $T = \text{ind}(T)$ et que $\mathbb{Q}_+ \cdot T \supseteq P$. Cet ensemble est non vide, car il contient $\text{ind}(P)$. Soit S un élément minimal de cet ensemble pour la relation d'inclusion. Montrons que S est un système de racines simples, c'est-à-dire par 3.1.5 (i), que S est une partie libre de $M \otimes \mathbb{Q}$.

Lemme 3.2.10. — Si $\alpha, \beta \in S$ et $q\alpha + q'\beta \in R$, où $q, q' \in \mathbb{Q}$, alors $qq' \geq 0$.

En effet, si $qq' < 0$, on peut écrire (quitte à échanger α et β)

$$a\alpha - b\beta \in P, \quad a, b \in \mathbb{Q}_+^*,$$

donc il existe par hypothèse une relation

$$a\alpha - b\beta = \sum_{\gamma \in S} c(\gamma)\gamma, \quad c(\gamma) \in \mathbb{Q}_+.$$

Si $a \leq c(\alpha)$, elle s'écrit

$$-\beta = \frac{c(\alpha) - a}{b} \alpha + \sum_{\gamma \neq \alpha} \frac{c(\gamma)}{b} \gamma.$$

Alors, cet élément appartient à $\mathbb{Q}_+ \cdot S \cap R$, qui est contenu dans P d'après (P 3). Mais alors $\beta \in P \cap -P$, ce qui contredit (P 1).

Si, au contraire $a > c(\alpha)$, on écrit

$$(a - c(\alpha)) \alpha = b\beta + \sum_{\gamma \neq \alpha} c(\gamma) \gamma,$$

ce qui prouve que $S \subseteq \mathbb{Q}_+ \cdot (S - \{\alpha\})$, contrairement au caractère minimal de S . 104

Rappelons (cf. 2.3.7) que la forme bilinéaire sur $\mathcal{V}(R)$ définie par $\langle x, y \rangle = (p(x), y)$ est un produit scalaire euclidien ; de plus, pour $\alpha \in R$ on a $\langle \alpha, y \rangle = \ell(\alpha) (\alpha^*, y)/2$, de sorte que $\langle \alpha, y \rangle$ et $\langle \alpha^*, y \rangle$ sont de même signe.

Lemme 3.2.11. — Si $\alpha, \beta \in S$, alors $(\beta^*, \alpha) \leq 0$ et donc $\langle \beta, \alpha \rangle \leq 0$.

En effet, $s_\beta(\alpha) = \alpha - (\beta^*, \alpha) \beta \in R$, d'où $(\beta^*, \alpha) \leq 0$ d'après 3.2.10.

Démontrons maintenant que S est libre. Dans le cas contraire, 3.2.11 entraîne, comme dans la démonstration de 3.1.5, qu'il existe une relation non triviale

$$\sum_{\alpha \in S} m(\alpha) \alpha = 0, \quad m(\alpha) \in \mathbb{N},$$

d'où $-\alpha_0 = (m(\alpha_0) - 1) \alpha_0 + \sum_{\alpha \neq \alpha_0} m(\alpha) \alpha$, si $m(\alpha_0) \geq 1$. Alors, d'après (P 3), α_0 appartient à $P \cap -P$, contredisant (P 1).

Ceci montre que S est une base de R et achève la démonstration du théorème 3.2.8.

Corollaire 3.2.12. — Soient P un système de racines positives, S une base de R et $w \in W$. On a les relations :

$$\begin{aligned} S \subseteq P &\iff P = \mathcal{P}(S) \iff S = \mathcal{S}(P) \\ \mathcal{P}(\text{ind}(S^*)) &= \mathcal{P}(S)^*, & \mathcal{S}(P^*) &= (\text{ind})(\mathcal{S}(P)^*); \\ \mathcal{S}(w(P)) &= w(\mathcal{S}(P)), & \mathcal{P}(w(S)) &= w(\mathcal{P}(S)). \end{aligned}$$

Définition 3.2.13. — Si on a choisi un système de racines simples S , les éléments de $\mathcal{P}(S)$ seront dits positifs. Si on a choisi un système de racines positives P , les éléments de $\mathcal{S}(P)$ seront dits simples. 105

Corollaire 3.2.14. — Soit P un système de racines positives. Soit $\alpha \in P$. Les conditions suivantes sont équivalentes :

- (i) α est simple (i.e. $\alpha \in \mathcal{S}(P)$).
- (ii) α n'est pas somme de deux éléments de P .
- (iii) $P - \{\alpha\}$ est clos (cf. 3.1.4).

L'équivalence de (i) et (ii) résulte aussitôt de 3.2.9. L'équivalence de (ii) et (iii) est immédiate.

Définition 3.2.15. — Soit S un système de racines simples. La somme des coefficients de la décomposition d'une racine α suivant S s'appelle l'ordre de α relativement à S et se note $\text{ord}_S(\alpha)$.

On a les équivalences :

$$\alpha \in \mathcal{P}(S) \iff \text{ord}_S(\alpha) > 0, \quad \alpha \in S \iff \text{ord}_S(\alpha) = 1.$$

Lemme 3.2.16. — Soient S un système de racines simples et $\alpha \in \mathcal{P}(S)$. Il existe une suite $\alpha_i \in S$, $i = 1, \dots, m$, telle que

$$\begin{aligned} \alpha_1 + \alpha_2 + \dots + \alpha_p \in \mathcal{P}(S) \quad \text{pour } p = 1, \dots, m, \\ \alpha_1 + \alpha_2 + \dots + \alpha_m = \alpha. \end{aligned}$$

De plus, pour toute suite α_i vérifiant ces conditions, on a $m = \text{ord}_S(\alpha)$.

Trivial par 3.1.2

106

3.3. Caractérisation et conjugaison des systèmes de racines positives. —

Lemme 3.3.1. — Si $\alpha \in \mathcal{P}(S)$, $\beta \in S$ et si α et β ne sont pas proportionnelles, alors $s_\beta(\alpha) \in \mathcal{P}(S)$.

En effet, $s_\beta(\alpha) = \alpha - (\beta^*, \alpha)\beta$. Comme il y a au moins une racine simple autre que β qui intervient dans la décomposition de α avec un coefficient non nul (donc strictement positif), donc aussi dans la décomposition de $s_\beta(\alpha)$ avec le même coefficient, $s_\beta(\alpha)$ est aussi positive.

Corollaire 3.3.2. — Si $\beta \in S$, la symétrie s_β échange les éléments de $\mathcal{P}(S)$ non proportionnels à β .

Lemme 3.3.3. — Si $\alpha \in \mathcal{P}(S) - S$, α indivisible, il existe $\beta \in S$ tel que $s_\beta(\alpha) \in \mathcal{P}(S)$ et $\text{ord}_S(s_\beta(\alpha)) < \text{ord}_S(\alpha)$.

En effet, d'après 3.1.1 il existe $\beta \in S$ tel que $(\beta^*, \alpha) > 0$. Comme $\alpha \notin S$ et est indivisible, α ne peut être proportionnel à β . Donc, $s_\beta(\alpha) \in \mathcal{P}(S)$, d'après 3.3.1, et l'on a $\text{ord}_S(s_\beta(\alpha)) = \text{ord}_S(\alpha) - (\beta^*, \alpha) < \text{ord}_S(\alpha)$.

Corollaire 3.3.4. — Si $\alpha \in \mathcal{P}(S)$ est indivisible, il existe une suite $\beta_p \in S$, $p = 1, \dots, q$, telle que

$$\alpha_p = s_{\beta_p} \cdots s_{\beta_1}(\alpha) \in \mathcal{P}(S) \quad \text{pour } p = 1, \dots, q,$$

et $\alpha_q \in S$.

Cela résulte de 3.3.3 par récurrence sur $\text{ord}_S(\alpha)$.

Proposition 3.3.5. — Le groupe de Weyl est engendré par les s_α , $\alpha \in S$. Toute racine indivisible est conjuguée d'une racine simple par un élément du groupe de Weyl.

107

La seconde assertion résulte aussitôt de 3.3.4. La première en résulte par 1.2.10 et 2.1.1.

Proposition 3.3.6. — Soit P un système de racines positives. Soit $P' \subseteq R$ vérifiant $(P \ 2)$ et clos. Alors il existe $w \in W$ tel que $w(P) \subseteq P'$.

Énonçons tout de suite les corollaires.

Corollaire 3.3.7. — *Le groupe de Weyl opère transitivement sur l'ensemble des systèmes de racines positives (resp. des systèmes de racines simples).*

Corollaire 3.3.8. — *Pour qu'une partie P de R soit un système de racines positives, il faut et il suffit qu'elle vérifie (P 1) et (P 2) et soit close.*

Corollaire 3.3.9. — *Si on munit $\Gamma_0(\mathbb{R})$ d'une structure de groupe ordonné telle que toute racine soit > 0 ou < 0 , l'ensemble des racines positives pour cette structure d'ordre est un système de racines positives.*

Démontrons maintenant 3.3.6. On peut trouver un $w \in W$ tel que $\text{Card}(w(P) \cap P')$ soit maximum, donc en remplaçant P par $w(P)$, on peut supposer que

$$(*) \quad \text{Card}(P \cap P') \geq \text{Card}(P \cap s_\alpha(P'))$$

pour tout $\alpha \in \mathcal{S}(P) = S$. Prouvons que $P \subseteq P'$. Sinon, P' étant clos, il existe $\alpha \in S$, $\alpha \notin P'$. Mais P' vérifiant (P 2), on a alors $-\alpha \in P'$ (donc $-2\alpha \in P'$ si 2α est racine). Pour tout $\beta \in P \cap P'$, on a $\beta \neq \alpha$; si 2α n'est pas racine, on a alors $s_\alpha(\beta) \in P$ (par 3.3.1), donc

$$s_\alpha(P \cap P') \subseteq P \cap s_\alpha(P');$$

mais $P \cap s_\alpha(P')$ contient aussi $\alpha = s_\alpha(-\alpha)$, ce qui contredit l'inégalité (*). Si 2α est racine, on raisonne de même.

Pour étudier les ensembles de racines vérifiant (P 2) et *clos*, on est donc ramené au cas où ils contiennent un ensemble de racines positives.

Proposition 3.3.10. — *Soient P un système de racines positives et P' une partie close de R contenant P. Si on note $S = \mathcal{S}(P)$ et $T = S \cap -P'$, alors P' est la réunion de P et de l'ensemble des racines qui sont combinaison linéaire à coefficients négatifs des éléments de T.* 108

Démontrons l'assertion par récurrence sur l'ordre d'une racine $\gamma \in P' - P$. Si $\text{ord}_S(\gamma) = -1$, alors $-\gamma \in S$ et $\gamma \in -T$. Si $\text{ord}_S(\gamma) < -1$, il existe, d'après 3.1.2, $\beta \in S$ telle que $-\gamma - \beta \in R$; alors

$$0 < \text{ord}_S(-\gamma - \beta) = \text{ord}_S(-\gamma) - 1 < \text{ord}_S(-\gamma)$$

et la première inégalité montre que $-\gamma - \beta \in P$. Donc, comme $P \cap -P = \emptyset$ et comme $\gamma + \beta$ est la somme de deux racines de P' , c'est un élément de $P' - P$, tel que $\text{ord}_S(\gamma + \beta) > \text{ord}_S(\gamma)$. Donc, par l'hypothèse de récurrence, $\gamma + \beta$ est une combinaison linéaire à coefficients négatifs des éléments de T. Comme $\gamma = (\gamma + \beta) - \beta$, il suffit de vérifier que $\beta \in -P'$. Or $\gamma \in P'$ et $-(\gamma + \beta) \in P \subseteq P'$, de sorte que $-\beta = \gamma - (\gamma + \beta)$ appartient à P' .

Définition 3.3.10.1. — ⁽⁸⁾ On dit qu'une partie R' de R est *symétrique* si $-R' = R'$.

⁽⁸⁾N.D.E. : On a inséré ici cette définition.

Scholie 3.3.11. — Soit P' un ensemble de racines vérifiant (P 2) et *clos*. Il existe un système de racines simples S et une partie T de S tels que

$$P' = R \cap (\mathbb{N} \cdot S \cup -\mathbb{N} \cdot T).$$

Si on note $R_T = \mathbb{Z} \cdot T \cap R$, qui est une partie close et symétrique de R , P' est donc la réunion disjointe de R_T et de la partie close de $\mathcal{P}(S)$ formée des $\alpha \in \mathcal{P}(S) - \mathbb{N} \cdot T$, i.e. des racines positives qui dans la décomposition sur S « contiennent au moins une racine de $S - T$ ».

3.4. Ensembles de racines clos et symétriques. —

Proposition 3.4.1. — Soient $\mathcal{R} = (M, M^*, R, R'^*)$ une donnée radicielle et R' une partie close et symétrique de R . Alors :

- (i) $\mathcal{R}' = (M, M^*, R', R'^*)$ est une donnée radicielle ;
 109 (ii) pour tout système de racines positives P de R , $P' = P \cap R'$ est un système de racines positives de R' ;
 (iii) le groupe de Weyl $W(\mathcal{R}')$ de \mathcal{R}' est le sous-groupe de $W(\mathcal{R})$ engendré par les s_α , pour $\alpha \in R'$.

La première assertion est triviale par 1.2.11, la seconde résulte de 3.3.8, la troisième est évidente.

Corollaire 3.4.2. — Soit $w \in W(\mathcal{R}')$. L'ordre de w est le plus petit entier $n > 0$ tel que $w^n(\alpha') = \alpha'$ pour tout $\alpha' \in R'$.

Il suffit d'appliquer 1.2.7 à la donnée radicielle \mathcal{R}' .

Corollaire 3.4.3. — Soient α et β deux racines non proportionnelles. Soit n le plus petit entier > 0 tel que $(s_\alpha s_\beta)^n(\alpha) = \alpha$ et $(s_\alpha s_\beta)^n(\beta) = \beta$. Alors le sous-groupe $W_{\alpha\beta}$ de W engendré par s_α et s_β est défini par les relations :

$$s_\alpha^2 = 1, \quad s_\beta^2 = 1, \quad (s_\alpha s_\beta)^n = 1.$$

Compte tenu de 3.4.2, il suffit de vérifier :

Lemme 3.4.4. — Soit G le groupe engendré par deux éléments x et y soumis aux relations $x^2 = y^2 = 1$. Tout sous-groupe invariant de G ne contenant ni x ni y est engendré (comme sous-groupe invariant) par un élément de la forme $(xy)^n$, où $n > 0$.

⁽⁹⁾ En effet, tout élément de G s'écrit $(xy)^n$, ou $(yx)^n = (xy)^{-n}$, ou :

$$(a) \quad x(yx)^{2n} \quad \text{ou} \quad y(xy)^{2n+1}$$

$$(b) \quad y(xy)^{2n} \quad \text{ou} \quad x(yx)^{2n+1},$$

où $n \in \mathbb{N}$. Or les éléments du type (a), resp. (b), sont conjugués à x , resp. à y .

⁽⁹⁾N.D.E. : On a corrigé l'original dans ce qui suit.

Remarque 3.4.5. — On calcule immédiatement l'entier n : si on pose

$$(\alpha^*, \beta) = p, \quad (\beta^*, \alpha) = q,$$

on a

$$(s_\alpha s_\beta)(\alpha) = (pq - 1)r - pt, \quad (s_\alpha s_\beta)(\beta) = qr - t.$$

110

L'entier n est donc l'ordre de la matrice

$$\begin{pmatrix} pq - 1 & -p \\ q & -1 \end{pmatrix} \quad (10)$$

Si $pq = 0$, alors $p = q = 0$, d'après 2.2.2, d'où $n = 2$. Sinon, d'après 2.3.1, pq égale 1, 2, ou 3, et l'on trouve, respectivement, $n = 3, 4$ ou 6.

N. B. En écrivant que l'ordre de la matrice précédente est fini, on retrouve l'inégalité (13) de 2.3.1.

Définition 3.4.6. — Soit S un système de racines simples et $S' \subseteq S$. On note

$$R_{S'} = R \cap \mathbb{Q} \cdot S' = R \cap \mathbb{Z} \cdot S'.$$

Lemme 3.4.7. — $R_{S'}$ est clos et symétrique, S' est un système de racines simples de la donnée radicielle $(M, M^*, R_{S'}, R_{S'}^*)$ dont le groupe de Weyl est le sous-groupe $W_{S'}$ de W engendré par les s_α , pour $\alpha \in S'$. On a $S \cap R_{S'} = S'$.

Trivial.

Proposition 3.4.8. — Soit $R' \subseteq R$. Les conditions suivantes sont équivalentes :

- (i) Il existe un sous-espace vectoriel V' de V (ou de $\mathcal{V}(R)$) tel que $R' = R \cap V'$.
- (ii) Il existe un système de racines simples S de R et une partie S' de S telle que $R' = R_{S'}$.

Plus précisément, sous ces conditions, tout système de racines simples S' de (M, M^*, R', R'^*) est contenu dans un système de racines simples S de R et $R' = R_{S'}$. 111

On a évidemment (ii) \Rightarrow (i). Supposons (i) vérifiée : alors R' est clos et symétrique, donc (M, M^*, R', R'^*) est une donnée radicielle. Soient S' un système de racines simples de cette donnée et $P' = \mathcal{P}(S')$. Si $V' = V$, alors S' est un système de racines simples de R et on a terminé. Sinon, il existe $x \in V^*$ tel que

$$(x, V') = \{0\}, \quad (x, \alpha) \neq 0 \quad \text{pour tout } \alpha \in R - R'.$$

Posons $P_x^+ = \{\alpha \in R \mid (x, \alpha) > 0\}$ et $P = P_x^+ \cup P'$. Pour tout $\alpha \in R$, on a les équivalences

$$\begin{aligned} (x, \alpha) > 0 &\iff \alpha \in P_x^+, \\ (x, \alpha) < 0 &\iff \alpha \in -P_x^+, \\ (x, \alpha) = 0 &\iff \alpha \in R'. \end{aligned}$$

Il résulte aussitôt de 3.3.8 que P est un système de racines positives de R . Posons $S = \mathcal{S}(P)$. Il suffit évidemment de prouver $S' \subseteq S$. Sinon soit $\alpha \in S' - S$. Alors, par

⁽¹⁰⁾N.D.E. : Faut-il adopter la convention $Ae_j = \sum_i a_{ij}e_i$, et transposer cette matrice ?

3.2.14, il existe $\beta, \gamma \in P$ tels que $\alpha = \beta + \gamma$. Si $\beta, \gamma \in P_x^+$, on a $\alpha \in P_x^+$, ce qui est absurde car $(x, S') = 0$. Si β ou γ , par exemple β , appartient à P' , alors, comme R' est symétrique et clos, $\gamma = \alpha - \beta$ appartient à $P \cap R' = P'$; mais alors α n'est pas simple dans P' .

Lemme 3.4.9. — *Sous les conditions précédentes, soit $\alpha \in \mathcal{P}(S) - R'$. Pour tout $w \in W_{S'}$, on a $w(\alpha) \in \mathcal{P}(S) - R'$.*

Il suffit en effet de le vérifier pour $w = s_\beta$, $\beta \in S'$, auquel cas cela résulte de 3.3.1 et de ce que $s_\beta(R') = R'$.

112 **Lemme 3.4.10.** — *Soit $w \in W$. Sous les conditions de 3.4.8, les conditions suivantes sont équivalentes :*

- (i) $w \in W_{S'}$.
- (ii) Pour tout $m \in M$, $w(m) - m \in V'$.
- (iii) Pour tout $\alpha \in R$, $w(\alpha) - \alpha \in V'$.

On a évidemment (i) \Rightarrow (ii) \Rightarrow (iii). Prouvons (iii) \Rightarrow (i). Soit donc $w \in W$ tel que $w(\alpha) - \alpha \in V'$ pour tout $\alpha \in R$. Écrivons $w = s_{\alpha_n} \cdots s_{\alpha_1}$, avec $\alpha_i \in S$, et montrons par récurrence sur n que chaque $\alpha_i \in S'$. On peut supposer que $w' = s_{\alpha_{n-1}} \cdots s_{\alpha_1} \in W_{S'}$. On a alors, pour tout $\alpha \in R$,

$$w(\alpha) - \alpha = w'(\alpha) - \alpha - (\alpha_n^*, w'(\alpha)) \alpha_n.$$

Prenant $\alpha = w'^{-1}(\alpha_n)$, on trouve $2\alpha_n \in V'$, d'où $\alpha_n \in S'$, donc $w = s_{\alpha_n} w'$ appartient à $W_{S'}$.

3.5. Remarques diverses. —

Proposition 3.5.1. — *Soit P un système de racines positives. Notons ⁽¹¹⁾*

$$\rho_P = (1/2) \sum_{\alpha \in \text{ind}(P)} \alpha.$$

Alors $(\beta^*, \rho_P) = 1$ pour tout $\beta \in \mathcal{S}(P)$.

En effet, on peut écrire

$$2\rho_P = \beta + \sum_{\substack{\alpha \in \text{ind}(P) \\ \alpha \neq \beta}} \alpha,$$

donc $s_\beta(2\rho_P) = 2\rho_P - 2\beta$, par 3.3.2.

113 **Corollaire 3.5.2.** — *Posons $\rho_P^* = (1/2) \sum_{\alpha^* \in \text{ind}(P^*)} \alpha^*$. Alors :*

- (i) $(\rho_P^*, \alpha) > 0$ pour tout $\alpha \in P$, i.e. (cf. 3.6.8) $\rho_P^* \in \mathcal{C}(P)$.
- (ii) Pour tout $\alpha \in R$, on a $\text{ord}_{\mathcal{S}(P)}(\alpha) = (\rho_P^*, \alpha)$. ⁽¹²⁾

Remarque 3.5.3. — Si $w \in W$, on a $\rho_{w(P)} = w(\rho_P)$ et $\rho_{w(P)}^* = w(\rho_P^*)$.

⁽¹¹⁾N.D.E. : On a remplacé g_P par la notation ρ_P maintenant usuelle, et de même dans 3.5.2 on a remplacé h_P par ρ_P^* .

⁽¹²⁾N.D.E. : à vérifier, si OK préciser (i)...

Proposition 3.5.4. — Soient α et γ deux racines non proportionnelles, α étant supposée indivisible. Il existe un système de racines simples contenant α et une racine β telle que $\gamma = a\alpha + b\beta$, $a, b \in \mathbb{N}$.

En effet, construisons une base de l'espace vectoriel $\mathcal{V}(\mathbb{R})$ contenant $\alpha_1 = \alpha$, $\alpha_2 = \gamma$. Considérons l'ordre lexicographique par rapport à cette base. L'ensemble des racines > 0 étant noté P , il est clair que P est un système de racines positives et que ⁽¹³⁾ le plus petit élément de P non proportionnel à α est simple. Cet élément est de la forme

$$\beta = p\alpha + q\gamma, \quad 0 < q \leq 1.$$

On a donc $\gamma = q^{-1}\beta - q^{-1}p\alpha$, et comme $q^{-1} > 0$, on a $q^{-1} \in \mathbb{N}^*$ et $-q^{-1}p \in \mathbb{N}$.

Faisons enfin deux remarques sur le groupe $\Gamma_0(\mathbb{R})$.

Proposition 3.5.5. — Soient G un groupe abélien et $f : \mathbb{R} \rightarrow G$ une application vérifiant les deux conditions suivantes :

- (i) Si $\alpha \in \mathbb{R}$, $f(-\alpha) = -f(\alpha)$.
- (ii) Si $\alpha, \beta, \alpha + \beta \in \mathbb{R}$, $f(\alpha + \beta) = f(\alpha) + f(\beta)$.

Alors il existe un homomorphisme de groupes unique $\bar{f} : \Gamma_0(\mathbb{R}) \rightarrow G$ tel que $\bar{f}(\alpha) = f(\alpha)$ pour $\alpha \in \mathbb{R}$.

En effet, si S est un système de racines simples de \mathbb{R} , et si $\beta \in \mathbb{R}$ s'écrit $\sum_{\alpha \in S} a(\alpha)\alpha$, 114
il résulte aussitôt de 3.2.16 que $f(\beta) = \sum_{\alpha \in S} a(\alpha)f(\alpha)$. Or S est une base de $\Gamma_0(\mathbb{R})$.

Proposition 3.5.6. — Soit S un système de racines simples. Il existe sur $\Gamma_0(\mathbb{R})$ une structure de groupe totalement ordonné telle que les racines > 0 soient les éléments de $\mathcal{P}(S)$ et que $\alpha \mapsto \text{ord}_S(\alpha)$ soit une fonction croissante.

Soient en effet $\alpha_1, \alpha_2, \dots, \alpha_n$ ($n = \text{rgss}(\mathcal{R})$), les éléments de S . Pour $x \in \Gamma_0(\mathbb{R})$, on a une décomposition

$$x = \sum_{i=1}^n m_i(x)\alpha_i.$$

Il suffit de prendre l'ordre lexicographique relativement aux fonctions $\sum m_i, m_n, m_{n-1}, \dots, m_2$.

Remarque 3.5.7. — Les premières racines sont dans l'ordre :

$$\alpha_1, \alpha_2, \dots, \alpha_n;$$

on a ensuite (si ce sont des racines) $2\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \dots$

⁽¹³⁾N.D.E. : On a modifié l'original, pour tenir compte du cas où 2α serait une racine.

3.6. Chambres de Weyl. —

Lemme 3.6.1. — Soit V un \mathbb{Q} -espace vectoriel de dimension finie. Soient f_i des formes linéaires indépendantes. Posons

$$C = \{x \in V \mid f_i(x) > 0\}.$$

Alors C est une partie convexe maximale de $X = V - \bigcup_i f_i^{-1}(0)$.

Trivial.

115 **Définition 3.6.2.** — Une partie C de V pouvant se décrire par le procédé de 3.6.1 sera appelée (ici) une *chambre* de V .

Définition 3.6.3. — On dit que l'hyperplan H de V est un *mur* de C si $H \cap (\overline{C} - C)$ contient une partie ouverte non vide de H .

Remarque 3.6.4. — Pour une partie convexe, l'adhérence se décrit sans faire appel à la topologie de V : c'est l'ensemble des extrémités de tous les segments ouverts contenus dans la partie donnée.

Lemme 3.6.5. — Sous les conditions de 3.6.1, on a

$$\overline{C} = \{x \in V \mid f_i(x) \geq 0\}.$$

Les murs de C sont les hyperplans $f_i^{-1}(0)$.

C'est clair pour la première assertion. La seconde résulte alors de ce que $\overline{C} - C \subseteq \bigcup_i f_i^{-1}(0)$ et de ce que les $f_i^{-1}(0)$ sont évidemment des murs de C .

Proposition 3.6.6. — Soit C une chambre de V . Si H_i , $i = 1, 2, \dots, n$, sont les murs distincts de C , pour tout système de formes linéaires $\{u_i\}$ tel que $H_i = u_i^{-1}(0)$, il existe des $\varepsilon_i \in \{-1, +1\}$ tels que C soit définie par

$$C = \{x \in V \mid \varepsilon_i u_i(x) > 0\}.$$

Pour tout mur H de C , on a $H \cap C = \emptyset$ et $H \cap \overline{C} = \overline{C}_H$, où C_H est une chambre dans H . Les murs de C_H sont les $H_j \cap H_i$, pour $j \neq i$.

Cela résulte trivialement du lemme.

Définition 3.6.7. — Les C_{H_i} sont les *faces* de C .

Soit maintenant $\mathcal{R} = (M, M^*, R, R^*)$ une donnée radicielle.

Définition 3.6.8. — ⁽¹⁴⁾ Pour tout $\alpha \in R$, on pose

$$\mathcal{H}_\alpha = \{x \in V^* \mid (x, \alpha) = 0\}.$$

116 On note $X = V^* - \bigcup_{\alpha \in R} \mathcal{H}_\alpha$. Pour tout $x \in X$, on pose

$$\mathcal{P}(x) = \{\alpha \in R \mid (x, \alpha) > 0\}.$$

Pour tout système de racines positives P , on note

$$\mathcal{C}(P) = \{x \in V^* \mid (x, \alpha) > 0 \text{ pour tout } \alpha \in P\}.$$

⁽¹⁴⁾N.D.E. : On a ajouté la définition des hyperplans \mathcal{H}_α .

Proposition 3.6.9. — (i) Pour tout $x \in X$, $\mathcal{P}(x)$ est un système de racines positives. Pour tout système de racines positives P , $\mathcal{C}(P)$ est une chambre dans V^* . Les $\mathcal{C}(P)$ sont les parties convexes maximales de X .

(ii) Soit S un système de racines simples. On a

$$\mathcal{C}(\mathcal{P}(S)) = \{x \in V^* \mid (x, \alpha) > 0 \text{ pour tout } \alpha \in S\}.$$

Les murs de $\mathcal{C}(\mathcal{P}(S))$ sont les hyperplans $\mathcal{H}_\alpha = \alpha^{-1}(0)$, pour $\alpha \in S$; ses faces sont les

$$C_\alpha = \{x \in V \mid (x, \alpha) = 0, \quad (x, \beta) > 0 \text{ pour } \beta \in S - \{\alpha\}\}.$$

(iii) On a l'équivalence

$$\mathcal{P}(x) = P \iff x \in \mathcal{C}(P).$$

Il est d'abord clair que $\mathcal{P}(x)$ est un système de racines positives. Comme $x \in \mathcal{C}(\mathcal{P}(x))$, la réunion des $\mathcal{C}(\mathcal{P}(x))$ est X . La propriété (iii) est immédiate; il en résulte que les $\mathcal{C}(P)$ forment une partition de X . La première assertion de (ii) est évidente. Il en résulte aussitôt que $\mathcal{C}(P)$ est une chambre dans V , ce qui prouve le reste de (ii). Il ne reste qu'à remarquer que

$$\bigcup_{\alpha \in R} \alpha^{-1}(0) = \bigcup_{\alpha \in S} s^{-1}(0)$$

⁽¹⁵⁾ pour achever la démonstration de (i) par 3.6.1.

Définition 3.6.10. — Les $\mathcal{C}(P)$ sont appelées les *chambres de Weyl* de la donnée radicielle.

Corollaire 3.6.11. — Les applications $P \mapsto \mathcal{C}(P)$ et $C \mapsto \mathcal{P}(x)$ pour un $x \in C$ quelconque, réalisent une correspondance bijective entre systèmes de racines positives et chambres de Weyl. 117

Cette correspondance est invariante par le groupe de Weyl :

Lemme 3.6.12. — Si $w \in W(\mathcal{R})$, on a $\mathcal{C}(w(P)) = w(\mathcal{C}(P))$.

Corollaire 3.6.13. — Les correspondances $S \leftrightarrow P \leftrightarrow C$ sont des isomorphismes d'espaces homogènes sous $W(\mathcal{R})$.

On verra plus loin que ces espaces homogènes sont *principaux* (5.5).

Remarque 3.6.14. — Si C est une chambre de Weyl, alors $-C$ en est aussi une, dite l'*opposée* de C . Il existe donc un $w_0 \in W$ (et en fait *un seul*, cf. 5.5) tel que $w_0(C) = -C$, on l'appelle la *symétrie* de la donnée radicielle relativement à la chambre de Weyl C , (ou à $\mathcal{P}(C)$ ou à $\mathcal{S}(\mathcal{P}(C))$...)

⁽¹⁵⁾N.D.E. : Correction à faire ici ...

4. Données radicielles réduites de rang semi-simple 2

4.0. ⁽¹⁶⁾ Soit \mathcal{R} une donnée radicielle de rang semi-simple 2. Soit $\{\alpha, \beta\}$ un système de racines simples. Supposons $\ell(\alpha) \leq \ell(\beta)$. On a alors par 2.3.1 et 3.2.1 quatre possibilités :

Type	$\ell(\beta)/\ell(\alpha)$	$\ell(\beta^*)/\ell(\alpha^*)$	(β^*, α)	(α^*, β)
$A_1 \times A_1$	—	—	0	0
A_2	1	1	-1	-1
B_2	2	1/2	-1	-2
G_2	3	1/3	-1	-3

118 Il résulte alors de 3.4.5 que l'ordre de $s_\alpha s_\beta$ est respectivement 2, 3, 4, 6.

Étudions séparément chacun de ces systèmes et donnons la liste des racines indivisibles.

Type $A_1 \times A_1$. Les racines indivisibles sont $\alpha, \beta, -\alpha, -\beta$. Les coracines correspondantes sont $\alpha^*, \beta^*, -\alpha^*, -\beta^*$.

Type A_2 . Les racines indivisibles positives sont comme suit :

racine γ	α	β	$\alpha + \beta$
$\ell(\gamma)/\ell(\alpha)$	1	1	1
coracine γ^*	α^*	β^*	$\alpha^* + \beta^*$
$\ell(\gamma^*)/\ell(\beta^*)$	1	1	1

La demi-somme des racines indivisibles positives est $\rho = \alpha + \beta$.

Type B_2 . Les racines indivisibles positives sont les suivantes :

racine γ	α	β	$\alpha + \beta$	$2\alpha + \beta$
$\ell(\gamma)/\ell(\alpha)$	1	2	1	2
coracine γ^*	α^*	β^*	$2\alpha^* + \beta^*$	$\alpha^* + \beta^*$
$\ell(\gamma^*)/\ell(\beta^*)$	2	1	2	1

La demi-somme des racines indivisibles positives est $\rho = (4\alpha + 3\beta)/2$.

Type G_2 . Les racines indivisibles positives sont les suivantes :

racine γ	α	β	$\alpha + \beta$	$2\alpha + \beta$	$3\alpha + \beta$	$3\alpha + 2\beta$
$\ell(\gamma)/\ell(\alpha)$	1	3	1	1	3	3
coracine γ^*	α^*	β^*	$\alpha^* + 3\beta^*$	$2\alpha^* + 3\beta^*$	$\alpha^* + \beta^*$	$\alpha^* + 2\beta^*$
$\ell(\gamma^*)/\ell(\beta^*)$	3	1	3	3	1	1

119 La demi-somme des racines indivisibles positives est $\rho = 5\alpha + 3\beta$.

⁽¹⁶⁾N.D.E. : On a ajouté la numérotation 4.0, pour références ultérieures.

Proposition 4.1. — Soit n l'ordre de $s_\alpha s_\beta$. Posons $u_0 = 0$ et, pour $p \in \mathbb{N}$,

$$\begin{cases} u_{2p+1} = u_{2p} + (s_\alpha s_\beta)^p(\alpha); \\ u_{2p+2} = u_{2p+1} + (s_\alpha s_\beta)^p s_\alpha(\beta). \end{cases}$$

Alors :

- (i) $u_{k+2n} = u_k$, pour tout $k \in \mathbb{N}$.
- (ii) $u_0 = 0$, $u_1 = \alpha$, $u_{2n-1} = \beta$, $u_{2n} = 0$.
- (iii) Si $1 < k < 2n - 1$, on a $u_k = a_k \alpha + b_k \beta$, avec $a_k, b_k \in \mathbb{N}^*$.

L'assertion (i) résulte de $(s_\alpha s_\beta)^n = 1$ et $u_{2n} = 0$.⁽¹⁷⁾

Prouvons (ii) et (iii). Le calcul donne aussitôt dans les quatre cas les suites de valeurs :⁽¹⁸⁾

$$(A_1 \times A_1) \quad 0, \alpha, \beta + \alpha, \beta, 0.$$

$$(A_2) \quad 0, \alpha, \beta + 2\alpha, 2\beta + 2\alpha, 2\beta + \alpha, \beta, 0.$$

$$(B_2) \quad 0, \alpha, \beta + 3\alpha, 2\beta + 4\alpha, 3\beta + 4\alpha, 3\beta + 3\alpha, 2\beta + \alpha, \beta, 0.$$

$$(G_2) \quad 0, \alpha, \beta + 4\alpha, 2\beta + 6\alpha, 4\beta + 9\alpha, 5\beta + 10\alpha, 6\beta + 10\alpha, 6\beta + 9\alpha, 5\beta + 6\alpha, \\ 4\beta + 4\alpha, 2\beta + \alpha, \beta, 0.$$

Lemme 4.2. —^(*) Posons $w_{2p} = (s_\beta s_\alpha)^p$, $w_{2p+1} = s_\alpha (s_\beta s_\alpha)^p$, de telle sorte que w_0, \dots, w_{2n-1} sont les éléments distincts de W . Soient u_0, \dots, u_{2n-1} les éléments de V définis en 4.1. Pour tout $x \in V^*$, on a

$$w_k(x) - x = n_k \alpha^* + m_k \beta^*, \quad n_k, m_k \in \mathbb{Q},$$

avec $n_k + m_k = -(x, u_k)$.

La démonstration se fait par récurrence sur k . Si $k = 0$, la formule est trivialement vérifiée. Effectuons par exemple le passage de w_{2p} à w_{2p+1} . On a $w_{2p+1} = s_\alpha w_{2p}$, d'où

$$w_{2p+1}(x) - x = s_\alpha w_{2p}(x) - w_{2p}(x) + w_{2p}(x) - x = -(w_{2p}(x), \alpha) \alpha^* + n_{2p} \alpha^* + m_{2p} \beta^*.$$

Donc

$$\begin{aligned} n_{2p+1} + m_{2p+1} &= n_{2p} + m_{2p} - ((s_\beta s_\alpha)^p(x), \alpha) \\ &= -(x, u_{2p}) - (x, (s_\alpha s_\beta)^p(\alpha)) = -(x, u_{2p+1}). \end{aligned}$$

^(*) Les lemmes suivants 4.2 et 4.4 sont utilisés dans la démonstration de 5.1. Il y a actuellement des démonstrations plus simples de 5.1, voir Bourbaki, *Groupes et algèbres de Lie*, Ch. IV.

⁽¹⁷⁾ N.D.E. : L'égalité $u_{2n} = 0$ découle du calcul cas par cas qui suit, ou de l'argument suivant. Notons t la restriction de $s_\alpha s_\beta$ au sous-espace vectoriel engendré par α et β ; alors 1 n'est pas valeur propre de t (sinon, comme $\det(t) = 1$ et $t^n = 1$, on aurait $t = \text{id}$, ce qui n'est pas le cas), donc $t - \text{id}$ est inversible; il en résulte que $u_{2n} = (\text{id} + \dots + t^{n-1})(u_2)$ est nul.

⁽¹⁸⁾ N.D.E. : On a corrigé l'original, pour être en accord avec la convention $\ell(\alpha) \leq \ell(\beta)$ de 4.0.

Corollaire 4.3. — Soit $x \in V^*$. Pour tout $w \in W$, on pose

$$w(x) - x = a_w \alpha + b_w \beta.$$

Si $(x, \alpha) \geq 0$ et $(x, \beta) \geq 0$, alors $a_w + b_w \geq 0$. Si de plus $(x, \alpha) > 0$ (resp. $(x, \beta) > 0$), alors $a_w + b_w > 0$ pour $w \neq 1$, s_β (resp. pour $w \neq 1$, s_α).

Cela résulte aussitôt de 4.1 et 4.2.

Corollaire 4.4. — Soit \mathcal{R} une donnée radicielle quelconque et soit S un système de racines simples. Soient γ une racine positive, α, β deux racines simples, $W_{\alpha\beta}$ le sous-groupe de W engendré par s_α et s_β . Si

$$\text{ord}_S(s_\alpha(\gamma)) < \text{ord}_S(\gamma), \quad \text{ord}_S(s_\beta(\gamma)) \leq \text{ord}_S(\gamma),$$

121 alors, pour tout $w \in W_{\alpha\beta}$, on a $\text{ord}_S(w(\gamma)) \leq \text{ord}_S(\gamma)$; de plus $\text{ord}_S(w(\gamma)) < \text{ord}_S(\gamma)$ si $w \neq 1$, $w \neq s_\beta$.

En effet, considérons la donnée radicielle duale \mathcal{R}^* , puis la donnée (M^*, M, R'^*, R') , où R' est l'ensemble des racines combinaisons linéaires rationnelles de α et de β . Appliquant 4.3 à cette donnée, on trouve le corollaire annoncé.

5. Le groupe de Weyl : générateurs et relations

Soit \mathcal{R} une donnée radicielle. Comme le groupe de Weyl est le même pour cette donnée et pour la donnée réduite correspondante, on peut supposer \mathcal{R} réduite pour étudier le groupe de Weyl.

Soit $S = \{\alpha_1, \dots, \alpha_n\}$ un système de racines simples ($n = \text{rgss}(\mathcal{R})$). Soit n_{ij} l'ordre de l'élément $s_{\alpha_i} s_{\alpha_j}$ de W . En particulier, on a $n_{ii} = 1$ et on a vu en 3.4.2 et 3.4.3 que le sous-groupe W_{ij} de W engendré par s_{α_i} et s_{α_j} était défini par les relations :

$$s_{\alpha_i}^2 = s_{\alpha_j}^2 = (s_{\alpha_i} s_{\alpha_j})^{n_{ij}} = 1.$$

Théorème 5.1. — Le groupe W est le groupe engendré par les éléments s_{α_i} , $i = 1, 2, \dots, n$, soumis aux relations $(s_{\alpha_i} s_{\alpha_j})^{n_{ij}} = 1$.

122 Nous avons déjà vu que le théorème est vrai lorsque $n = 2$; nous nous servirons de cette remarque dans le cours de la démonstration. Introduisons le groupe \overline{W} engendré par des éléments T_i , $i = 1, 2, \dots, n$, soumis aux relations $(T_i T_j)^{n_{ij}} = 1$. On a en particulier $n_{ii} = 1$, d'où $T_i^2 = 1$. Soit $p : \overline{W} \rightarrow W$ le morphisme de groupes qui envoie T_i sur s_{α_i} . On sait que p est surjectif, on va montrer qu'il est injectif.

Lemme 5.2. — On peut définir de manière unique pour chaque $\alpha \in \mathcal{P}(S)$ un élément $T_\alpha \in \overline{W}$ de telle manière que l'on ait les propriétés suivantes :

- (i) $p(T_\alpha) = s_\alpha$,
- (ii) $T_{\alpha_i} = T_i$
- (iii) Si β et α sont deux racines positives telles que $s_{\alpha_i}(\alpha) = \beta$, alors $T_i T_\alpha T_i = T_\beta$.

Remarquons d'abord qu'il résulte de 1.2.10 et 3.3.6 que (i) est une conséquence de (ii) et (iii) et que (ii) et (iii) déterminent parfaitement les T_α . Nous allons faire la construction par récurrence sur $\text{ord}_S(\alpha)$. Si $\text{ord}_S(\alpha) = 1$, alors $\alpha \in S$ et on pose $T_\alpha = T_i$ si $\alpha = \alpha_i$. Considérons l'hypothèse :

(H_p) il existe des T_α , pour $\alpha \in \mathcal{P}(S)$, $\text{ord}_S(\alpha) \leq p$, vérifiant (ii) et la condition (iii) chaque fois que $\text{ord}_S(\alpha) \leq p$, $\text{ord}_S(\beta) \leq p$.

Celle-ci est vérifiée pour $p = 1$: en effet si α et $s_{\alpha_i}(\alpha) = \beta$ sont simples, α_i et α sont orthogonales, donc si l'on note $\alpha_j = \alpha = \beta$, on a $n_{ij} = 2$, d'où

$$T_i T_j T_i = T_j.$$

Supposons $p > 1$ et (H_{p-1}) vérifiée.

A) Construction des T_α pour $\text{ord}_S(\alpha) \leq p$. Il suffit évidemment de le faire pour $\text{ord}_S(\alpha) = p$. Il existe alors $\alpha_i \in S$, avec $s_{\alpha_i}(\alpha) \in \mathcal{P}(S)$, $\text{ord}_S(s_{\alpha_i}(\alpha)) < p$. (3.3.3). On posera alors **123**

$$T_\alpha = T_i T_{s_{\alpha_i}(\alpha)} T_i.$$

Vérifions que T_α ne dépend que de α . Soit donc $\alpha_j \in S$ tel que $s_{\alpha_j}(\alpha) \in \mathcal{P}(S)$ et $\text{ord}_S(s_{\alpha_j}(\alpha)) < p$. Prouvons que

$$(+) \quad T_i T_{s_{\alpha_i}(\alpha)} T_i = T_j T_{s_{\alpha_j}(\alpha)} T_j.$$

Distinguons deux cas.

(1) Supposons α combinaison linéaire de α_i et de α_j . Il en est alors de même de $s_{\alpha_i}(\alpha)$ et $s_{\alpha_j}(\alpha)$ et par (H_{p-1}), $T_{s_{\alpha_i}(\alpha)}$ et $T_{s_{\alpha_j}(\alpha)}$ s'écrivent comme des mots en T_i et T_j . Comme la projection de (+) dans W est vérifiée et que le théorème est vrai pour $n = 2$, donc que p est injectif sur le sous-groupe de \overline{W} engendré par T_i et T_j , (+) est bien vérifiée.

(2) Supposons α non combinaison linéaire de α_i et de α_j . Alors si $w \in W_{\alpha_i \alpha_j}$, les $w(\alpha)$ seront tous positifs (cf. 3.4.9). La relation à vérifier s'écrit aussi

$$(++) \quad (T_i T_j)^{n_{ij}-1} T_{s_{\alpha_i}(\alpha)} (T_j T_i)^{n_{ij}-1} = T_{s_{\alpha_j}(\alpha)}.$$

Or il résulte de 4.4 que les $w(\alpha)$ sont tous d'ordre $< p$ pour $w \in W_{\alpha_i \alpha_j}$ $w \neq 1$. On peut donc appliquer $2(n_{ij} - 1)$ fois l'hypothèse (H_{p-1}) et on a terminé.

B) Vérification de (H_p). Il ne reste plus qu'à vérifier l'assertion suivante : si $\text{ord}_S(\alpha) = p$, $\text{ord}_S(s_{\alpha_i}(\alpha)) < p$, $\text{ord}_S(s_{\alpha_j}(\alpha)) = p$, on a ⁽¹⁹⁾ **124**

$$(+++)$$

$$T_j T_i T_{s_{\alpha_i}(\alpha)} T_i T_j = T_i T_{s_{\alpha_i}(\alpha)} T_i.$$

Cela se fait exactement comme précédemment.

⁽¹⁹⁾N.D.E. : Correction à faire dans ce qui suit ...

Lemme 5.3. — Soit $h \in \overline{W}$. Écrivons-le

$$h = T_{\alpha_1} \cdots T_{\alpha_m}$$

avec les $\alpha_i \in S$, non nécessairement distincts, de telle manière que m soit minimum. Alors

$$p(h)(\alpha_m) \in -\mathcal{P}(S).$$

En effet, comme $p(T_{\alpha_m})(\alpha_m) = s_{\alpha_m}(\alpha_m) = -\alpha_m$, si $p(h)(\alpha_m)$ était positif, il existerait un indice k , $1 \leq k \leq m-1$ tel que

$$u = s_{\alpha_{k+1}} \cdots s_{\alpha_m}(\alpha_m) = -s_{\alpha_{k+1}} \cdots s_{\alpha_{m-1}}(\alpha_m) \in -\mathcal{P}(S),$$

et $s_{\alpha_k}(u) \in \mathcal{P}(S)$. Mais alors on a nécessairement $u = -\alpha_k$ (3.3.1), d'où

$$s_{\alpha_{k+1}} \cdots s_{\alpha_{m-1}}(\alpha_m) = \alpha_k,$$

ce qui entraîne par (iii)

$$T_{\alpha_k} T_{\alpha_{k+1}} \cdots T_{\alpha_{m-1}} T_{\alpha_m} = T_{\alpha_{k+1}} \cdots T_{\alpha_{m-1}},$$

et ceci contredit le caractère minimal de m .

125 Soit maintenant $h \in \overline{W}$ avec $p(h)(\mathcal{P}(S)) \subseteq \mathcal{P}(S)$. Par le lemme 5.3, on a $p(h) = 1$, ce qui démontre le théorème 5.1 et en outre le

Corollaire 5.4. — Si P est un système de racines positives et si $w \in W$ est tel que $w(P) = P$, alors $w = 1$.

Corollaire 5.5. — Le groupe de Weyl opère librement et transitivement dans l'ensemble des système de racines positives (resp. des systèmes de racines simples, resp. des chambres de Weyl).

Choisissons maintenant un système de racines simples S . Posons $P = \mathcal{P}(S)$. Pour tout couple de racines simples $(\alpha, \beta) \in S \times S$, notons $R_{\alpha\beta}$ l'ensemble des racines combinaison linéaire α et de β . Notons $P_{\alpha\beta} = P \cap R_{\alpha\beta}$ et soit $W_{\alpha\beta}$ le groupe de Weyl de $R_{\alpha\beta}$, c'est-à-dire le sous-groupe de W engendré par s_α et s_β .

Théorème 5.6 (Tits). — Soient α et β deux racines simples et soit $w \in W$ tel que $w(\alpha) = \beta$. Il existe une suite de racines simples $\alpha_0, \dots, \alpha_m$ et une suite w_0, \dots, w_{m-1} d'éléments de W vérifiant les conditions suivantes :

- (i) On a $\alpha_0 = \alpha$, $\alpha_m = \beta$.
- (ii) On a $w = w_{m-1}w_{m-2} \cdots w_0$.
- (iii) On a $w_i(\alpha_i) = \alpha_{i+1}$, pour $0 \leq i \leq m-1$.
- (iv) Pour tout i , $0 \leq i \leq m-1$, tel que $\alpha_i \neq \alpha_{i+1}$, on a $w_i \in W_{\alpha_i\alpha_{i+1}}$.
- (v) Pour tout i , $0 \leq i \leq m-1$, tel que $\alpha_i = \alpha_{i+1}$, il existe une racine simple β_i telle que $w_i \in W_{\alpha_i\beta_i}$.

126 Posons ⁽²⁰⁾

$$M(w) = \text{Card}(P \cap w^{-1}(-P)) = \text{Card}\{\alpha \in P \mid w(\alpha) \in -P\}.$$

Si $M(w) = 0$, alors $w(P) = P$ donc $w = 1$ par 5.4 et le théorème est trivial ($m = 0$, les assertions (iii) à (v) sont vides). Raisonnons par récurrence sur $M(w)$. Si $M(w) > 0$, il existe $\beta_0 \in S$ tel que $w(\beta_0) \in -P$. Posons $\alpha_0 = \alpha$. Considérons l'ensemble

$$A = w^{-1}(P) \cap R_{\alpha_0\beta_0}.$$

C'est un système de racines positives de $R_{\alpha_0\beta_0}$. Il existe donc $w_0 \in W_{\alpha_0\beta_0}$ tel que

$$w_0^{-1}(P_{\alpha_0\beta_0}) = A.$$

Posons $w' = ww_0^{-1}$. Par 3.4.9, on a aussitôt

$$P - P_{\alpha_0\beta_0} = w_0(P - P_{\alpha_0\beta_0}),$$

d'où

$$(1) \quad (P - P_{\alpha_0\beta_0}) \cap w^{-1}(-P) = w_0((P - P_{\alpha_0\beta_0}) \cap w'^{-1}(-P)).$$

D'autre part,

$$(2) \quad \beta_0 \in P_{\alpha_0\beta_0} \cap w^{-1}(-P),$$

et, comme $w_0(R_{\alpha_0,\beta_0}) = R_{\alpha_0,\beta_0}$, on a $w_0(-A) = R_{\alpha_0,\beta_0} \cap w'^{-1}(-P)$, d'où

$$(2') \quad P_{\alpha_0\beta_0} \cap w'^{-1}(-P) = P_{\alpha_0\beta_0} \cap w_0(-A) = P_{\alpha_0\beta_0} \cap -P_{\alpha_0\beta_0} = \emptyset.$$

Il résulte de (1), (2) et (2') que $M(w') < M(w)$.

Posons $\alpha_1 = w_0(\alpha_0)$, montrons que $\alpha_1 \in S$, c'est-à-dire $\alpha_0 \in w_0^{-1}(S)$. On sait que $w(\alpha_0) \in S$, donc que $\alpha_0 \in w^{-1}(S)$, donc aussi que $\alpha_0 \in w^{-1}(S) \cap R_{\alpha_0\beta_0}$, donc que α_0 est une racine simple de $A = w^{-1}(P) \cap R_{\alpha_0\beta_0} = w_0^{-1}(P_{\alpha_0\beta_0})$, donc appartient à

$$w_0^{-1}(S \cap P_{\alpha_0\beta_0}) = w_0^{-1}(\{\alpha_0, \beta_0\})$$

(voir 3.4.8). Donc $\alpha_1 = w_0(\alpha_0)$ égale α_0 ou β_0 . Si $\alpha_1 \neq \alpha_0$, on a $\alpha_1 = \beta_0$ et $w_0 \in W_{\alpha_0,\alpha_1}$.

Enfin, on a $\beta = w'(\alpha_1)$, avec $M(w') < M(w)$ et on conclut par récurrence.

6. Morphismes de données radicielles

127

6.1. Définition. — Soient $\mathcal{R} = (M, M^*, R, R)$ et $\mathcal{R}' = (M', M'^*, R', R'^*)$ deux données radicielles. Soit $f : M' \rightarrow M$ une application linéaire et ${}^t f : M^* \rightarrow M'^*$ l'application transposée.

Définition 6.1.1. — On dit que f est un *morphisme* de \mathcal{R}' dans \mathcal{R} et on note $f : \mathcal{R}' \rightarrow \mathcal{R}$, si f induit une bijection de R' sur R et ${}^t f$ une bijection de R^* sur R'^* .

⁽²⁰⁾N.D.E. : Dans ce qui suit, on a détaillé l'original, et l'on a corrigé l'égalité (1).

Alors ${}^t f$ est un morphisme des données radicielles duales :

$${}^t f : \mathcal{R}^* \longrightarrow \mathcal{R}'^*.$$

On voit facilement que si f est un morphisme de \mathcal{R}' dans \mathcal{R} , et si on note $\alpha = f(\alpha')$ pour $\alpha' \in \mathcal{R}'$, on a $\alpha'^* = {}^t f(\alpha^*)$. En effet, on voit immédiatement que si on note p et p' les applications de 1.2.1 respectives à \mathcal{R} et \mathcal{R}' , on a $p' = {}^t f \circ p \circ f$, et l'assertion cherchée en résulte aussitôt. Nous laissons au lecteur le soin de démontrer les énoncés qui suivent et qui sont presque tous triviaux.

Proposition 6.1.2. — Soit $f : \mathcal{R}' \rightarrow \mathcal{R}$ un morphisme de données radicielles. Si $\alpha' \in \mathcal{R}'$ et $\alpha = f(\alpha')$, alors $\alpha'^* = {}^t f(\alpha^*)$. De plus, f induit des isomorphismes :

$$\mathcal{R}' \xrightarrow{\sim} \mathcal{R}, \quad \Gamma_0(\mathcal{R}') \xrightarrow{\sim} \Gamma_0(\mathcal{R}), \quad \mathcal{V}(\mathcal{R}') \xrightarrow{\sim} \mathcal{V}(\mathcal{R}),$$

et ${}^t f$ induit des isomorphismes :

$$\mathcal{R}^* \xrightarrow{\sim} \mathcal{R}'^*, \quad \Gamma_0(\mathcal{R}^*) \xrightarrow{\sim} \Gamma_0(\mathcal{R}'^*), \quad \mathcal{V}(\mathcal{R}^*) \xrightarrow{\sim} \mathcal{V}(\mathcal{R}'^*),$$

128 le dernier étant le transposé du morphisme correspondant induit par f . L'application $s_{\alpha'} \mapsto s_{f(\alpha')}$ se prolonge en un isomorphisme $W(\mathcal{R}') \xrightarrow{\sim} W(\mathcal{R})$ compatible avec les opérations de ces deux groupes dans les ensembles de 1.1.13.

Proposition 6.1.3. — Les applications

$$S' \mapsto f(S'), \quad P' \mapsto f(P'), \quad C' \mapsto ({}^t f \otimes \mathbb{R})^{-1}(C')$$

définissent des correspondances bijectives entre systèmes de racines simples, systèmes de racines positives et chambres de Weyl pour \mathcal{R}' et \mathcal{R} . Ces correspondances sont compatibles avec l'action des groupes de Weyl et avec les correspondances

$$\mathcal{S}(P) \leftrightarrow P \leftrightarrow \mathcal{C}(P).$$

Lemme 6.1.4. — Les morphismes se composent. Pour que le morphisme $f : \mathcal{R}' \rightarrow \mathcal{R}$ soit un isomorphisme, il faut et il suffit que $f : M' \rightarrow M$ soit bijectif.

6.2. Isogénies. —

Définition 6.2.1. — Un morphisme $f : \mathcal{R}' \rightarrow \mathcal{R}$ de données radicielles est dit une *isogénie* si $f : M' \rightarrow M$ est injectif de conoyau fini.

Si f est une isogénie, alors ${}^t f$ est une isogénie.

Définition 6.2.2. — Soit $f : \mathcal{R}' \rightarrow \mathcal{R}$ une isogénie. On pose $K(f) = \text{Coker}(M' \xrightarrow{f} M)$.

Lemme 6.2.3. — On a un accouplement naturel

$$K(f) \times K({}^t f) \rightarrow \mathbb{Q}/\mathbb{Z},$$

qui met ces deux groupes finis en dualité.

C'est classique.

129 **Lemme 6.2.4.** — Si $f : \mathcal{R}' \rightarrow \mathcal{R}$ est un morphisme, alors $\text{rgss}(\mathcal{R}') = \text{rgss}(\mathcal{R})$. Si de plus f est une isogénie, on a aussi $\text{rgred}(\mathcal{R}') = \text{rgred}(\mathcal{R})$.

Trivial.

Lemme 6.2.5. — *Tout morphisme de données radicielles semi-simples est une isogénie.*

Cela résulte aussitôt du fait que f doit induire un isomorphisme de $V' = \mathcal{V}(R')$ sur $V = \mathcal{V}(R)$.

Si \mathcal{R}' et \mathcal{R} sont semi-simples, toute isogénie $f : \mathcal{R}' \rightarrow \mathcal{R}$ définit un diagramme commutatif :

$$\begin{array}{ccc} \Gamma_0(R') & \xrightarrow{\sim} & \Gamma_0(R) \\ \downarrow & & \downarrow \\ M' & \xrightarrow{f} & M. \end{array}$$

Si $M = \Gamma_0(R)$, alors f est nécessairement un isomorphisme.

Définition 6.2.6. — Une donnée radicielle est dite *adjointe* (resp. *simplement connexe*) si $M = \Gamma_0(R)$, resp. $M^* = \Gamma_0(R^*)$.

Une donnée radicielle adjointe ou simplement connexe est donc semi-simple. \mathcal{R} est adjointe (resp. simplement connexe) si et seulement si \mathcal{R}^* est simplement (resp. adjointe). En vertu du résultat précédent, on a :

Proposition 6.2.7. — *Soit \mathcal{R} une donnée radicielle semi-simple. Les conditions suivantes sont équivalentes :*

- (i) \mathcal{R} est adjointe (resp. simplement connexe).
- (ii) Toute isogénie $\mathcal{R}' \rightarrow \mathcal{R}$ (resp. $\mathcal{R} \rightarrow \mathcal{R}'$) est un isomorphisme.

Proposition 6.2.8. — *Soit \mathcal{R} une donnée radicielle adjointe (resp. simplement connexe). Toute racine (resp. coracine) indivisible est un élément indivisible de M (resp. M^*).*

En effet, toute racine indivisible fait partie d'une base de $\Gamma_0(R)$, par 3.3.5.

130

6.3. Radical et coradical. — Soit \mathcal{R} une donnée radicielle. Posons

$$N = \{x \in M \mid (\alpha^*, x) = 0 \text{ pour tout } \alpha^* \in R^*\};$$

$$N^* = M^* / \mathcal{V}(R^*) \cap M^*.$$

Lemme 6.3.1. — *Considérons les morphismes canoniques :*

$$N \longrightarrow M, \quad M^* \longrightarrow N^*.$$

Ils sont transposés l'un de l'autre et N^ s'identifie au dual de N .*

C'est immédiat, compte tenu de 1.2.5.

Définition 6.3.2. — On appelle *coradical* de \mathcal{R} et on note $\text{corad}(\mathcal{R})$ la donnée radicielle triviale

$$\text{corad}(\mathcal{R}) = (N, N^*, \emptyset, \emptyset).$$

Si on pose $\mathcal{R}^0 = (M, M^*, \emptyset, \emptyset)$ (c'est une donnée radicielle triviale), on a donc un morphisme

$$\text{corad}(\mathcal{R}) \longrightarrow \mathcal{R}^0.$$

Définition 6.3.3. — On appelle *radical* de \mathcal{R} et on note $\text{rad}(\mathcal{R})$ la donnée radicielle triviale :

$$\text{rad}(\mathcal{R}) = \text{corad}(\mathcal{R}^*)^*. \quad (21)$$

On a donc un diagramme

$$\begin{array}{ccc} \text{corad}(\mathcal{R}) & \xrightarrow{\quad} & \text{rad}(\mathcal{R}) \\ & \searrow & \nearrow \\ & \mathcal{R}^0 & \end{array},$$

131 dont le transposé est le diagramme correspondant pour \mathcal{R}^* .

Lemme 6.3.4. — *Le morphisme canonique $u : \text{corad}(\mathcal{R}) \rightarrow \text{rad}(\mathcal{R})$ est une isogénie.*

Définition 6.3.5. — On pose $N(\mathcal{R}) = K(u) = M / [(\mathcal{V}(\mathcal{R}) \cap M) + \bigcap_{\alpha \in R} \text{Ker}(\alpha^*)]$.

On a un accouplement canonique

$$N(\mathcal{R}) \times N(\mathcal{R}^*) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Lemme 6.3.6. — *On a*

$$\text{rgred}(\text{rad}(\mathcal{R})) = \text{rgred}(\text{corad}(\mathcal{R})) = \text{rgred}(\mathcal{R}) - \text{rgss}(\mathcal{R}).$$

Les conditions suivantes sont équivalentes :

- (i) \mathcal{R} est semi-simple,
- (ii) $\text{rad}(\mathcal{R}) = 0$,
- (iii) $\text{corad}(\mathcal{R}) = 0$.

6.4. Produits de données radicielles. —

Définition 6.4.1. — Soient $\mathcal{R} = (M, M^*, R, R^*)$ et $\mathcal{R}' = (M', M'^*, R', R'^*)$ deux données radicielles. On appelle donnée radicielle produit de \mathcal{R} et de \mathcal{R}' et on note $\mathcal{R}'' = \mathcal{R} \times \mathcal{R}'$ la donnée radicielle (M'', M''^*, R'', R''^*) où $M'' = M \times M'$, $M''^* = M^* \times M'^*$, $R'' = R \times 0 \cup 0 \times R'$, $R''^* = R^* \times 0 \cup 0 \times R'^*$, l'application $\alpha \mapsto \alpha^*$ étant l'application évidente.

⁽²¹⁾N.D.E. : Expliciter ceci...

Proposition 6.4.2. — *Sous les conditions précédentes on a des isomorphismes canoniques*

$$\begin{aligned}\Gamma_0(\mathcal{R}'') &\simeq \Gamma_0(\mathcal{R}) \times \Gamma_0(\mathcal{R}'), & \mathcal{V}(\mathcal{R}'') &\simeq \mathcal{V}(\mathcal{R}) \times \mathcal{V}(\mathcal{R}'), \\ W(\mathcal{R}'') &\simeq W(\mathcal{R}) \times W(\mathcal{R}'),\end{aligned}$$

etc., et des relations

$$\begin{aligned}\text{rgred}(\mathcal{R}'') &= \text{rgred}(\mathcal{R}) + \text{rgred}(\mathcal{R}'), \\ \text{rgss}(\mathcal{R}'') &= \text{rgss}(\mathcal{R}) + \text{rgss}(\mathcal{R}').\end{aligned}$$

132

On a également un isomorphisme canonique de données radicielles

$$(\mathcal{R} \times \mathcal{R}')^* \simeq \mathcal{R}^* \times \mathcal{R}'^*.$$

Les définitions précédentes se généralisent aussitôt à un produit de plusieurs facteurs. On a aussitôt :

Proposition 6.4.3. — *Soit $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_n$ un produit de données radicielles. Les conditions suivantes sont équivalentes :*

- (i) \mathcal{R} est semi-simple (resp. simplement connexe, resp. adjointe, resp. réduite).
- (ii) Chaque \mathcal{R}_i est semi-simple (resp. simplement connexe, resp. adjointe, resp. réduite).

Considérons le cas particulier suivant : soit \mathcal{R}_0 une donnée radicielle triviale et \mathcal{R}_1 une donnée radicielle semi-simple. On a alors un diagramme commutatif

$$\begin{array}{ccc} & \mathcal{R}_0 \times \mathcal{R}_1 & \\ \nearrow & & \searrow \\ \mathcal{R}_1 & \xrightarrow{\text{id}} & \mathcal{R}_1. \end{array}$$

Lemme 6.4.4. — *On a des isomorphismes canoniques*

$$\begin{array}{ccc} \text{corad}(\mathcal{R}_0 \times \mathcal{R}_1) & \xrightarrow{\sim} & \text{rad}(\mathcal{R}_0 \times \mathcal{R}_1) \\ & \searrow \cong & \nearrow \cong \\ & \mathcal{R}_0 & \end{array} .$$

En particulier, $N(\mathcal{R}_0 \times \mathcal{R}_1) = 0$.

Nous verrons plus tard que si réciproquement $N(\mathcal{R}) = 0$, alors la donnée radicielle \mathcal{R} est produit d'une donnée semi-simple par une donnée triviale.

6.5. Données radicielles induites et coinduites. — Soit $\mathcal{R} = (M, M^*, R, R^*)$ une donnée radicielle. Soit $N \subseteq M$ un sous-groupe contenant les racines, i.e. tel que

$$\Gamma_0(R) \subseteq N \subseteq M.$$

L'application linéaire canonique $i_N : N \rightarrow M$ donne par transposition une application linéaire

$${}^t i_N : M^* \longrightarrow N^*.$$

Posons $R_N = R$ et $R_N^* = {}^t i_N(R^*)$.

Lemme 6.5.1. — $\mathcal{R}_N = (N, N^*, R_N, R_N^*)$ est une donnée radicielle, et i_N un morphisme.

Montrons d'abord que ${}^t i_N$ induit un isomorphisme de R^* sur R_N^* . Si $\alpha, \beta \in R$ et ${}^t i_N(\alpha^*) = {}^t i_N(\beta^*)$, on a $(\alpha^*, x) = (\beta^*, x)$ pour tout $x \in N$, en particulier pour $x \in R$, ce qui donne $\alpha = \beta$ par 1.1.4. Le reste s'en déduit sans difficultés.

Définition 6.5.2. — \mathcal{R}_N est dite la donnée radicielle *induite* par \mathcal{R} sur N .

Lemme 6.5.3. — Soit $f : \mathcal{R}' \rightarrow \mathcal{R}$ un morphisme. Posons $N = f(M') \subseteq M$. Alors f se factorise de manière unique par i_N .

En particulier, les *isogénies* $\mathcal{R}' \rightarrow \mathcal{R}$, à isomorphisme près, correspondent *biunivoquement* aux *sous-groupes d'indice fini* de $M/\Gamma_0(R)$, ce qui précise 6.2.7

Soit maintenant N^* un sous-groupe de M^* contenant R^* . On définit la donnée *coinduite* par \mathcal{R} sur N^* par

$$\mathcal{R}^{N^*} = (\mathcal{R}_{N^*}^*)^*,$$

134 et on a un morphisme canonique :

$$p^{N^*} : \mathcal{R} \longrightarrow \mathcal{R}^{N^*}.$$

Lemme 6.5.4. — Soit $f : \mathcal{R}' \rightarrow \mathcal{R}$ un morphisme. Il existe des sous-groupes $N \subseteq M$ et $N^* \subseteq M^*$ tels que f se factorise en

$$\begin{array}{ccc} \mathcal{R}' & \xrightarrow{f} & \mathcal{R} \\ p^{N^*} \downarrow & & \uparrow i_N \\ \mathcal{R}'^{N^*} & \xrightarrow[\sim]{f_0} & \mathcal{R}_N \end{array}$$

où f_0 est un isomorphisme.

En effet, on prend $N = f(M')$ comme dans 6.5.3. Le morphisme $M' \rightarrow N$ obtenu est surjectif, donc son transposé injectif. On prend l'image de ce dernier comme N^* .

Traisons maintenant certains cas particuliers. Si on prend $N = \Gamma_0(R)$, on notera $\mathcal{R}_N = \text{ad}(\mathcal{R})$. Si on prend $N = \mathcal{V}(R) \cap M$, on notera $\mathcal{R}_N = \text{ss}(\mathcal{R})$. On a donc un diagramme :

$$\text{ad}(\mathcal{R}) \longrightarrow \text{ss}(\mathcal{R}) \longrightarrow \mathcal{R}.$$

Posons $\text{dér}(\mathcal{R}) = \text{ss}(\mathcal{R}^*)^*$ et $\text{sc}(\mathcal{R}) = \text{ad}(\mathcal{R}^*)^*$; par dualité, on obtient un diagramme :

$$\mathcal{R} \longrightarrow \text{dér}(\mathcal{R}) \longrightarrow \text{sc}(\mathcal{R}).$$

Proposition 6.5.5. — (i) Dans le diagramme

$$\begin{array}{ccccccc} \text{ad}(\mathcal{R}) & \longrightarrow & \text{ss}(\mathcal{R}) & \longrightarrow & \text{dér}(\mathcal{R}) & \longrightarrow & \text{sc}(\mathcal{R}) \\ & & \searrow & & \nearrow & & \\ & & & \mathcal{R} & & & \end{array}$$

les quatre données de la première ligne sont semi-simples et les trois morphismes des isogénies.

(ii) $\text{ad}(\mathcal{R})$ est une donnée adjointe. \mathcal{R} est adjointe si et seulement si $\text{ad}(\mathcal{R}) \rightarrow \mathcal{R}$ est un isomorphisme. 135

(iii) $\text{sc}(\mathcal{R})$ est une donnée simplement connexe. \mathcal{R} est simplement connexe si et seulement si $\mathcal{R} \rightarrow \text{sc}(\mathcal{R})$ est un isomorphisme.

(iv) Les conditions suivantes sont équivalentes :

- \mathcal{R} est semi-simple,
- $\text{ss}(\mathcal{R}) \rightarrow \mathcal{R}$ est un isomorphisme,
- $\mathcal{R} \rightarrow \text{dér}(\mathcal{R})$ est un isomorphisme.

Arrêtons-nous un instant sur le morphisme $\text{ss}(\mathcal{R}) \rightarrow \text{dér}(\mathcal{R})$. En se reportant à la construction de $\text{ss}(\mathcal{R})$ et de $\text{dér}(\mathcal{R})$, il est aisé de démontrer le

Lemme 6.5.6. — Soit $h : \text{ss}(\mathcal{R}) \rightarrow \text{dér}(\mathcal{R})$ l'isogénie canonique. On a $K(h) \simeq N(\mathcal{R})$.

6.5.7. — Considérons d'autres cas particuliers de données induites. Posons

$$N = \{x \in M \mid (\alpha^*, x) = 0 \text{ pour } \alpha \in R\} \times \Gamma_0(R);$$

on sait que la somme est directe par 1.2.5. Il en résulte que la donnée radicielle \mathcal{R}_N s'identifie au produit $\text{ad}(\mathcal{R}) \times \text{corad}(\mathcal{R})$.

On peut faire de même en remplaçant $\Gamma_0(R)$ par $\mathcal{V}(R) \cap M$, puis dualiser ces deux constructions. On obtient ainsi un diagramme de données radicielles :

$$\begin{array}{cccccccc} \text{ad}(\mathcal{R}) & \longrightarrow & \text{ss}(\mathcal{R}) & \longrightarrow & \text{dér}(\mathcal{R}) & \longrightarrow & \text{sc}(\mathcal{R}) & \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ \text{ad}(\mathcal{R}) \times \text{corad}(\mathcal{R}) & \longrightarrow & \text{ss}(\mathcal{R}) \times \text{corad}(\mathcal{R}) & \longrightarrow & \mathcal{R} & \longrightarrow & \text{dér}(\mathcal{R}) \times \text{rad}(\mathcal{R}) & \longrightarrow & \text{sc}(\mathcal{R}) \times \text{rad}(\mathcal{R}) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \text{ad}(\mathcal{R}) & \longrightarrow & \text{ss}(\mathcal{R}) & \longrightarrow & \text{dér}(\mathcal{R}) & \longrightarrow & \text{sc}(\mathcal{R}); & \end{array}$$

qui est commutatif, comme on le vérifie aussitôt. Ce diagramme est auto-dual en un sens évident. Les morphismes horizontaux sont des isogénies. Les composés des flèches verticales sont l'identité. 136

Lemme 6.5.8. — Soient h_1 et h_2 les isogénies canoniques :

$$\text{ss}(\mathcal{R}) \times \text{corad}(\mathcal{R}) \xrightarrow{h_1} \mathcal{R} \xrightarrow{h_2} \text{dér}(\mathcal{R}) \times \text{rad}(\mathcal{R}).$$

On a $K(h_1) \simeq K(h_2) \simeq N(\mathcal{R})$.

C'est trivial sur les définitions.

Corollaire 6.5.9. — Soit \mathcal{R} une donnée radicielle. Les conditions suivantes sont équivalentes :

- (i) $N(\mathcal{R}) = 0$, i.e. $\text{corad}(\mathcal{R}) \rightarrow \text{rad}(\mathcal{R})$ est un isomorphisme.
- (ii) $h : \text{ss}(\mathcal{R}) \rightarrow \text{dér}(\mathcal{R})$ est un isomorphisme.
- (iii) $h_1 : \text{ss}(\mathcal{R}) \times \text{corad}(\mathcal{R}) \rightarrow \mathcal{R}$ est un isomorphisme.
- (iv) $h_2 : \mathcal{R} \rightarrow \text{dér}(\mathcal{R}) \times \text{rad}(\mathcal{R})$ est un isomorphisme.
- (v) \mathcal{R} est le produit d'une donnée semi-simple et d'une donnée triviale.

Énonçons également une conséquence triviale des remarques précédentes :

Corollaire 6.5.10. — Pour toute donnée radicielle \mathcal{R} , il existe des isogénies

$$\text{ad}(\mathcal{R}) \times \mathcal{R}_0 \longrightarrow \mathcal{R} \longrightarrow \text{sc}(\mathcal{R}) \times \mathcal{R}_0,$$

où \mathcal{R}_0 est « la » donnée radicielle triviale de rang $\text{rgred}(\mathcal{R}) - \text{rgss}(\mathcal{R})$.

Signalons enfin un résultat qui peut être utile :

Lemme 6.5.11. — Soient \mathcal{R} une donnée radicielle, S un système de racines simples, S' une partie de S , considérons la donnée radicielle (cf. 3.4.7)

$$\mathcal{R}_{S'} = (M, M^*, R_{S'}, R_{S'}^*).$$

- 137
- (i) Si \mathcal{R} est simplement connexe, alors $\text{dér}(\mathcal{R}_{S'})$ est simplement connexe.
 - (ii) Si \mathcal{R} est adjointe, alors $\text{ss}(\mathcal{R}_{S'})$ est adjointe.

Les deux assertions sont évidemment équivalentes par dualité. La seconde se ramène à vérifier la formule :

$$M \cap \mathcal{V}(R_{S'}) = \Gamma_0(R_{S'});$$

or, si $M = \Gamma_0(R)$, les deux membres sont égaux au sous-groupe de M engendré par S' .

6.6. Poids. —

Définition 6.6.1. — Soit \mathcal{R} une donnée radicielle. On pose

$$\Gamma(\mathcal{R}) = \{x \in V(R) \mid (\alpha^*, x) \in \mathbb{Z} \text{ pour tout } \alpha^* \in R^*\}.$$

Les éléments de $\Gamma(\mathcal{R})$ sont appelés les *poids* de \mathcal{R} . Les poids de \mathcal{R}^* sont appelés les *copoids* de \mathcal{R} .

On a $\Gamma_0(R) \subseteq \Gamma(\mathcal{R})$ et $\Gamma(\mathcal{R})$ est stable sous $W(\mathcal{R})$.

Lemme 6.6.2. — L'application bilinéaire $V^* \times V \rightarrow \mathbb{Q}$ induit une dualité $\Gamma_0(\mathcal{R}^*) \times \Gamma(\mathcal{R}) \rightarrow \mathbb{Z}$.

Trivial.

Corollaire 6.6.3. — Soit $S^* = (\alpha_1^*, \dots, \alpha_n^*)$ un système de coracines simples. Soient $p_i, i = 1, 2, \dots, n$, les éléments de $\mathcal{V}(\mathbb{R})$ définis par

$$(\alpha_i^*, p_j) = \delta_{ij},$$

(d'où $s_{\alpha_i}(p_i) = p_i - \alpha_i$ et $s_{\alpha_i}(p_j) = p_j$ pour $i \neq j$) (*). Alors $\Gamma(\mathcal{R})$ est le groupe abélien libre engendré par les p_i . 138

Les p_i sont appelés les *poids fondamentaux* correspondant au système de coracines simples S^* .

Corollaire 6.6.4. — Pour tout $\alpha^* \in S^*$, on a donc $(\alpha^*, \sum_i p_i) = 1$, donc $\sum_i p_i = \rho_P$ (cf. 3.5.1), où $P = \mathcal{P}(\text{ind}(S))$.

Corollaire 6.6.5. — Pour tout $x \in \mathcal{V}(\mathbb{R})$, on a $x = \sum_i (\alpha_i^*, x) p_i$.

Remarquons que $\mathbb{R}^* \subseteq \Gamma_0(\mathbb{R}^*)$ et $\mathbb{R} \subseteq \Gamma(\mathcal{R})$, donc que $(\Gamma(\mathcal{R}), \Gamma_0(\mathbb{R}^*), \mathbb{R}, \mathbb{R}^*)$ est une donnée radicielle.

Corollaire 6.6.6. — Le morphisme canonique $\Gamma_0(\mathbb{R}^*) \rightarrow M^*$ est le transposé du morphisme $x \mapsto \sum_i (\alpha_i^*, x) p_i$ qui définit un morphisme de données radicielles et on a un diagramme commutatif :

$$\begin{array}{ccc} & & \text{sc}(\mathcal{R}) \\ & \nearrow & \downarrow \wr \\ \mathcal{R} & & \\ & \searrow & \\ & & (\Gamma(\mathcal{R}), \Gamma_0(\mathbb{R}^*), \mathbb{R}, \mathbb{R}^*). \end{array}$$

On a donc une description explicite de $\text{sc}(\mathcal{R})$ en termes des poids de \mathcal{R} . De même, on trouve un diagramme commutatif :

$$\begin{array}{ccc} \text{ad}(\mathcal{R}) & & \\ \downarrow \wr & \searrow & \mathcal{R} \\ (\Gamma_0(\mathbb{R}), \Gamma(\mathcal{R}^*), \mathbb{R}, \mathbb{R}^*) & \nearrow & \end{array} .$$

Corollaire 6.6.7. — Pour que \mathcal{R} soit simplement connexe, il faut et il suffit que $M = \Gamma(\mathcal{R})$.

Remarque 6.6.8. — On a $\Gamma(\mathcal{R}) \cap M = \mathcal{V}(\mathbb{R}) \cap M$. Pour que \mathcal{R} soit semi-simple, il est donc nécessaire et suffisant que $M \subseteq \Gamma(\mathcal{R})$. 139

Des résultats de 6.5 il résulte aussi :

Corollaire 6.6.9. — Pour que \mathcal{R} soit produit d'une donnée simplement connexe par une donnée triviale, il faut et il suffit que $M \supseteq \Gamma(\mathcal{R})$.

(*) Attention : si la donnée n'est pas réduite, les α_i ne forment pas un système de racines simples.

Considérons maintenant l'isogénie canonique

$$f : \text{ad}(\mathcal{R}) \longrightarrow \text{sc}(\mathcal{R}),$$

et posons $Z(\mathcal{R}) = K(f)$. On a $Z(\mathcal{R}) \simeq Z(\text{sc } \mathcal{R}) \simeq Z(\text{ad } \mathcal{R})$.

Corollaire 6.6.10. — *On a un isomorphisme canonique $Z(\mathcal{R}) = \Gamma(\mathcal{R})/\Gamma_0(\mathbf{R})$. Plus précisément, on a une suite exacte de $W(\mathcal{R})$ -modules :*

$$0 \longrightarrow \Gamma_0(\mathbf{R}) \longrightarrow \Gamma(\mathcal{R}) \longrightarrow Z(\mathcal{R}) \longrightarrow 0.$$

Corollaire 6.6.11. — *On a un accouplement canonique*

$$Z(\mathcal{R}^*) \times Z(\mathcal{R}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

qui met ces groupes en dualité.

Remarque 6.6.12. — On a $Z(\mathcal{R} \times \mathcal{R}') \simeq Z(\mathcal{R}) \times Z(\mathcal{R}')$. Considérons en particulier des données simplement connexes \mathcal{R}_i , $i = 1, 2, \dots, n$ et une donnée triviale \mathcal{R}_0 . Posons $\mathcal{R} = \mathcal{R}_0 \times \mathcal{R}_1 \times \dots \times \mathcal{R}_n$. Soient $\mathcal{R} = (\mathbf{M}, \mathbf{M}^*, \mathbf{R}, \mathbf{R}^*)$, $\mathcal{R}_0 = (\mathbf{M}_0^*, \mathbf{M}_0^*, \emptyset, \emptyset)$. On a

$$\mathbf{M}/\Gamma_0(\mathbf{R}) \simeq \mathbf{M}_0 \times Z(\mathcal{R}_1) \times \dots \times Z(\mathcal{R}_n).$$

6.7. Automorphismes. — Un automorphisme de \mathcal{R} , c'est, d'après 6.1.4, un automorphisme de \mathbf{M} , soit u , tel que $u(\mathbf{R}) = \mathbf{R}$, ${}^t u(\mathbf{R}^*) = \mathbf{R}^*$. En particulier, tout élément w de $W(\mathcal{R})$ définit un automorphisme de \mathcal{R} .

Lemme 6.7.1. — *$W(\mathcal{R})$ est un sous-groupe invariant de $\text{Aut}(\mathcal{R})$. Plus précisément, si $u \in \text{Aut}(\mathcal{R})$ et $\alpha \in \mathbf{R}$, on a*

$$u s_\alpha u^{-1} = s_{u(\alpha)}.$$

La démonstration est la même que celle de 1.2.10.

Proposition 6.7.2. — *Soit S un système de racines simples. Posons*

$$E_S(\mathcal{R}) = \{u \in \text{Aut}(\mathcal{R}) \mid u(S) = S\}.$$

Alors $\text{Aut}(\mathcal{R})$ est le produit semi-direct de $W(\mathcal{R})$ par $E_S(\mathcal{R})$.

Cela résulte aussitôt de ce que $W(\mathcal{R})$ opère de façon simplement transitive sur les systèmes de racines simples et de ce que si S est un système de racines simples de \mathbf{R} , alors $u(S)$ est un système de racines simples pour tout automorphisme u de \mathcal{R} .

Nous verrons plus tard une description plus simple de $E_S(\mathcal{R})$ dans le cas des données radicielles réduites et irréductibles.

Définition 6.7.3. — On note $\text{Aut}^s(\mathcal{R})$ ⁽²²⁾ l'ensemble des $u \in \text{Aut}(\mathcal{R})$, tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{u} & \mathcal{R} \\ & \searrow & \swarrow \\ & \text{rad}(\mathcal{R}) & . \end{array}$$

On note $E_S^s(\mathcal{R}) = E_S(\mathcal{R}) \cap \text{Aut}^s(\mathcal{R})$.

141

Remarque 6.7.4. — Si $u \in \text{Aut}(\mathcal{R})$, on a donc $u \in \text{Aut}^s(\mathcal{R})$ si et seulement si $(u - \text{id})(M) \subseteq \mathcal{V}(R)$. En particulier $W(\mathcal{R}) \subseteq \text{Aut}^s(\mathcal{R})$. Il en résulte aussitôt :

Proposition 6.7.5. — *Le groupe $\text{Aut}^s(\mathcal{R})$ est le produit semi-direct de $W(\mathcal{R})$ par $E_S^s(\mathcal{R})$, pour tout système de racines simples S .*

À tout automorphisme de \mathcal{R} est associé par functorialité un automorphisme de $\text{ad}(\mathcal{R})$. On a donc un morphisme canonique

$$\text{Aut}(\mathcal{R}) \longrightarrow \text{Aut}(\text{ad}(\mathcal{R})).$$

Lemme 6.7.6. — *Le morphisme $\text{Aut}^s(\mathcal{R}) \rightarrow \text{Aut}(\text{ad}(\mathcal{R}))$ est injectif.*

Soit en effet u un automorphisme de M tel que $(u - \text{id})(M) \subseteq \mathcal{V}(R)$ et que ${}^t u(\alpha^*) = \alpha^*$ pour $\alpha^* \in R^*$. Pour tout $x \in M$, on a

$$(\alpha^*, u(x) - x) = ({}^t u(\alpha^*) - \alpha^*, x) = 0,$$

donc $u(x) - x = 0$, par 1.2.5.

Lemme 6.7.7. — *Le groupe $\text{Aut}^s(\mathcal{R})$ est fini.*

En effet, il nous suffit de prouver que $\text{Aut}(\mathcal{R})$ est fini si \mathcal{R} est adjoint. Comme M est engendré alors par R , tout automorphisme de \mathcal{R} est déterminé par la permutation de R qu'il définit.

Remarque 6.7.8. — On voit aussitôt que $\text{Aut}(\mathcal{R})$ (resp. $E_S(\mathcal{R})$) est fini si et seulement si $\text{rgred}(\mathcal{R}) - \text{rgss}(\mathcal{R}) \leq 1$.

142

6.8. p -morphisms de données radicielles réduites. — Dans ce numéro, p est un nombre entier > 0 fixé une fois pour toutes.

Définition 6.8.1. — Soient $\mathcal{R} = (M, M^*, R, R^*)$ et $\mathcal{R}' = (M', M'^*, R', R'^*)$ deux données radicielles réduites. On dit qu'un morphisme de groupes

$$f : M' \longrightarrow M$$

est un p -morphisme de \mathcal{R}' dans \mathcal{R} , si les conditions suivantes sont vérifiées : il existe une bijection

$$u : R \xrightarrow{\sim} R'$$

⁽²²⁾N.D.E. : Préciser l'origine de la notation $\text{Aut}^s(\mathcal{R}) \dots$

et une application $q : R \rightarrow \{p^n, n \in \mathbb{N}\}$ telles que :

- (i) on a $f(u(\alpha)) = q(\alpha)\alpha$ pour tout $\alpha \in R$.
- (ii) on a ${}^t f(\alpha^*) = q(\alpha)u(\alpha)^*$ pour tout $\alpha \in R$.

Corollaire 6.8.2. — *Un 1-morphisme n'est autre qu'un morphisme.*

Corollaire 6.8.3. — *Le transposé d'un p -morphisme est un p -morphisme.*

Lemme 6.8.4. — *Si $w \in W(\mathcal{R})$, $\alpha \in R$, on a $q(w(\alpha)) = q(\alpha)$. L'application $s_\alpha \mapsto s_{u(\alpha)}$ se prolonge en un isomorphisme $\bar{u} : W(\mathcal{R}) \rightarrow W(\mathcal{R}')$ tel que*

$$u(w(\alpha)) = \bar{u}(w)(u(\alpha)).$$

Il suffit de prouver que pour $\alpha, \beta \in R$, on a $u(s_\alpha(\beta)) = s_{u(\alpha)}u(\beta)$ et $q(s_\alpha(\beta)) = q(\beta)$. Or on a successivement :

$$\begin{aligned} f(s_{u(\alpha)}u(\beta)) &= f(u(\beta)) - (u(\alpha)^*, u(\beta))f(u(\alpha)) \\ &= q(\beta)\beta - q(\beta)q(\alpha)^{-1}(\alpha^*, \beta)q(\alpha)\alpha \\ &= q(\beta)(\beta - (\alpha^*, \beta)\alpha) = q(\beta)s_\alpha(\beta). \end{aligned}$$

- 143 Si $\gamma = u^{-1}(s_{u(\alpha)}u(\beta))$, on a donc $q(\gamma)\gamma = f(u(\gamma)) = q(\beta)s_\alpha(\beta)$. Les deux racines γ et $s_\alpha(\beta)$ sont donc proportionnelles (sur \mathbb{Q}), donc égales ou opposées, mais $q(\gamma)$ et $q(\beta)$ sont positifs. On a donc $q(\gamma) = q(\beta)$ et $\gamma = s_\alpha(\beta)$.

Définition 6.8.5. — Les $q(\alpha)$ sont dits les *exposants radiciels* de f .

Exemple 6.8.6. — Soient \mathcal{R} une donnée radicielle réduite et $q = p^n$ ($n \in \mathbb{N}$). Alors la multiplication par $q : M \rightarrow M$, $x \mapsto qx$ est un p -morphisme dont tous les exposants radiciels sont égaux à q (et $u = \text{id}$); on le note

$$q : \mathcal{R} \longrightarrow \mathcal{R}.$$

Proposition 6.8.7. — *Dans les notations de 6.8.1, u réalise un isomorphisme de l'ensemble des systèmes de racines simples (resp. de racines positives) de R sur l'ensemble correspondant pour R' .*

Cela résulte aussitôt de 3.1.5 (resp. 3.2.1).

7. Structure

144

7.1. Décomposition d'une donnée radicielle. —

Proposition 7.1.1. — *Soient \mathcal{R} une donnée radicielle, S un système de racines simples.*

(i) *Soient R' et R'' deux ensembles de racines clos et symétriques formant une partition de R . Si on note $S' = S \cap R'$, $S'' = S \cap R''$, alors $R' = R_{S'}$, $R'' = R_{S''}$, et toute racine de S' est orthogonale à toute racine de S'' .*

(ii) *Soient S' et S'' deux sous-ensembles de S faisant une partition de S et orthogonaux. Alors $R' = R_{S'}$ et $R'' = R_{S''}$ forment une partition de R .*

Prouvons d'abord (i).

Lemme 7.1.2. — *Sous les conditions de (i), si α , β et $\alpha + \beta$ sont racines, elles appartiennent toutes les trois à R' ou toutes les trois à R'' .*

Supposons par exemple $\alpha + \beta \in R'$. Alors on ne peut avoir $\alpha, \beta \in R''$, car R'' est clos; supposons donc $\alpha \in R'$. Alors $-\alpha \in R'$ et $\beta = (\beta + \alpha) - \alpha \in R'$.

Montrons maintenant que $R' = R_{S'}$ par récurrence sur l'ordre d'une racine $\alpha \in R' \cap \mathcal{P}(S)$. Si $\text{ord}_S(\alpha) = 1$, alors $\alpha \in R' \cap S = S'$. Si $\text{ord}_S(\alpha) > 1$, il existe $\beta \in S$ tel que $\alpha - \beta \in R$. Par le lemme, on a $\beta \in S'$, $\alpha - \beta \in R'$, donc $\alpha - \beta \in R_{S'}$ par récurrence et enfin $\alpha = (\alpha - \beta) + \beta \in R_{S'}$.

Montrons enfin que S' et S'' sont orthogonaux. Si $\alpha \in S'$ et $\beta \in S''$, alors $(\beta^*, \alpha) \leq 0$. Si $(\beta^*, \alpha) \neq 0$, alors $\beta + \alpha$ est racine contrairement au lemme.

Démontrons (ii). Si S' ou S'' est vide, c'est immédiat. Sinon et si $R_{S'}$ et $R_{S''}$ ne forment pas une partition de R , il existe une racine α de la forme **145**

$$\alpha = \sum m'_i \alpha'_i + \sum m''_j \alpha''_j, \quad m'_i \in \mathbb{Z}_+, \quad m''_j \in \mathbb{Z}_+,$$

où on note α'_i (resp. α''_j) des éléments de S' (resp. S''). Appliquant 3.1.2, on en déduit une relation de la forme (quitte à inverser S' et S'') :

$$\delta = \gamma + \beta, \quad \gamma \in R_{S'}, \quad s \in S'', \quad \delta \in R.$$

Mais comme $(\beta^*, \gamma) = 0$, $\gamma - \beta$ est aussi racine par 2.2.5, ce qui est impossible.

Proposition 7.1.3. — *Soit \mathcal{R} une donnée radicielle. Les conditions suivantes sont équivalentes :*

(i) *Il n'existe pas de partition non triviale de R en deux sous-ensembles clos et symétriques.*

(ii) *Pour un (resp. tout) système de racines simples S de R , il n'existe pas de partition de S en deux sous-ensembles non vides orthogonaux.*

(iii) *La représentation naturelle de $W(\mathcal{R})$ dans $\mathcal{V}(R)$ est irréductible.*

(iv) *Pour tout couple (α, β) de racines, il existe une suite de racines $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n$, avec $\alpha = \alpha_0$, $\alpha_n = \beta$, les racines α_i et α_{i+1} ($i = 0, \dots, n-1$) étant non orthogonales.*

On a (i) \Leftrightarrow (ii) par 7.1.1. On a évidemment (iv) \Rightarrow (ii). Réciproquement, si (ii) est vérifiée pour S , la condition (iv) est vérifiée si $\alpha, \beta \in S$. Or pour tout racine, il existe une racine simple qui ne lui soit pas orthogonale (3.1.1 par exemple). D'autre part (iii) \Rightarrow (i). En effet sous les conditions de 7.1.1, $\mathcal{V}(R')$ est stable par $W(\mathcal{R})$. Il reste à prouver (i) \Rightarrow (iii). **146**

Soit donc H un sous-espace vectoriel de $\mathcal{V}(R)$, stable par $W(\mathcal{R})$. Pour tout $\alpha \in R$, l'équation $s_\alpha(H) = H$ donne aussitôt $\alpha \in H$, ou $\alpha^* \in H^\perp$ (orthogonal de H dans $\mathcal{V}(R^*)$, qui est en dualité avec $\mathcal{V}(R)$). Si on pose $R' = \{\alpha \in R \mid \alpha \in H\}$ et $R'' = \{\alpha \in R \mid \alpha^* \in H^\perp\}$, on a réalisé une partition de R en deux sous-ensembles clos et symétriques.

Définition 7.1.4. — *Une donnée radicielle (resp. un système de racines) vérifiant les conditions équivalentes de 7.1.3 et de rang semi-simple $\neq 0$ est dite irréductible.*

Corollaire 7.1.5. — Pour toute donnée radicielle \mathcal{R} , il existe une partition unique (à l'ordre près) de R en sous-ensembles clos, symétriques et irréductibles.

Corollaire 7.1.6. — Toute donnée radicielle adjointe (resp. simplement connexe) est produit de données radicielles adjointes (resp. simplement connexes) irréductibles.

Il suffit de le voir dans le cas adjoint. L'assertion résulte alors de ce que sous les conditions de 7.1.1, on a

$$\Gamma_0(R) = \Gamma_0(R') \times \Gamma_0(R'').$$

Corollaire 7.1.7. — Pour toute donnée radicielle (resp. et réduite) \mathcal{R} , il existe une isogénie $\mathcal{R} \rightarrow \mathcal{R}'$, où \mathcal{R}' est produit d'une donnée radicielle triviale et de données simplement connexes irréductibles (resp. et réduites).

147

7.2. Propriétés des données radicielles irréductibles. —

Définition 7.2.1. — Soit \mathcal{R} une donnée radicielle irréductible. On pose pour tout $\alpha \in R$,

$$\text{long}(\alpha) = \ell(\alpha)/\ell(\alpha_0);$$

où $\alpha_0 \in R$ est telle que $\ell(\alpha_0)$ soit minimum; on dit que $\text{long}(\alpha)$ est la longueur de α .

Lemme 7.2.2. — Soit \mathcal{R} une donnée radicielle irréductible. Le groupe de Weyl opère transitivement dans l'ensemble des racines de même longueur.

En effet, soient $\alpha, \beta \in R$. Comme la représentation de W dans $\mathcal{V}(R)$ est irréductible, α ne peut être orthogonale à tous les $w(\beta)$, $w \in W$. Il existe donc $w \in W$, avec $w(\beta)$ non orthogonale à α . Or $\ell(w(\beta)) = \ell(\beta)$ et on conclut par 2.3.2

Lemme 7.2.3. — Si \mathcal{R} est irréductible et réduite, alors $\text{long}(R)$ est $\{1\}$, $\{1, 2\}$, ou $\{1, 3\}$.

En vertu de la remarque utilisée ci-dessus, pour tout $\alpha, \beta \in R$, il existe toujours un $w \in W$ tel que $w(\beta)$ ne soit pas orthogonale à α . On a donc $\ell(\alpha)/\ell(\beta) = 1, 2, 3, 1/2$ ou $1/3$ (par 2.3.1). On a donc $\text{long}(\alpha) = 1, 2$, ou 3 , mais si $\text{long}(\alpha) = 2$, $\text{long}(\beta) = 3$, alors $\ell(\alpha)/\ell(\beta) = 2/3$, ce qui est impossible.

Remarque 7.2.4. — En raisonnant de manière semblable, on prouve le résultat suivant : si R est irréductible et non réduit avec $\text{rgss}(\mathcal{R}) > 1$, on a $\text{long}(R) = \{1, 2, 4\}$. Si on pose $\text{long}^{-1}(i) = R_i$, alors $\text{ind}(R) = R_1 \cup R_2$, $R_4 = 2R_1$ et deux racines non proportionnelles de R_1 sont orthogonales. Réciproquement si R est un système irréductible et réduit tel que $\text{long}(R) = \{1, 2\}$, posons $\text{long}^{-1}(i) = R_i$ et supposons que deux racines non proportionnelles de R_1 soient orthogonales; alors $R \cup 2R_1$ est irréductible, non réduit et $\text{ind}(R \cup 2R_1) = R$.

148

Lemme 7.2.5. — Si \mathcal{R} est une donnée radicielle irréductible, \mathcal{R}^* l'est aussi et le produit $\text{long}(\alpha) \text{long}(\alpha^*)$ est constant, lorsque α parcourt R .

Cela résulte aussitôt de 7.1.3 (iv) et 2.2.6.

Définition 7.2.6. — Soit \mathcal{R} une donnée radicielle quelconque. On appelle longueur de $\alpha \in R$ et on note $\text{long}(\alpha)$ la longueur de α dans sa composante irréductible.

Lemme 7.2.7. — Il existe un unique homomorphisme de groupes $u : \Gamma_0(\mathbb{R}) \rightarrow \Gamma_0(\mathbb{R}^*)$ tel que $u(\alpha) = \text{long}(\alpha)\alpha^*$ pour $\alpha \in \mathbb{R}$.

En vertu de 3.5.5, il suffit de vérifier que si $\alpha, \beta, \alpha + \beta \in \mathbb{R}$, on a

$$\text{long}(\alpha)\alpha^* + \text{long}(\beta)\beta^* = \text{long}(\alpha + \beta)(\alpha + \beta).$$

Mais α, β et $\alpha + \beta$ sont dans la même composante irréductible de \mathbb{R} par 7.1.2 et on est ramené à 1.2.2.

Remarque 7.2.8. — Pour $\alpha, \beta \in \mathbb{R}$, on a $(u(\alpha), \beta) = (u(\beta), \alpha)$. En effet, cela revient à

$$\text{long}(\alpha)(\alpha^*, \beta) = \text{long}(\beta)(\beta^*, \alpha)$$

qui est évidemment vérifiée si α et β sont orthogonales. Si α et β ne sont pas orthogonales, alors elles sont dans la même composante irréductible de \mathbb{R} , et on est ramené à 1.2.1, formule (9).

Remarque 7.2.9. — La forme bilinéaire symétrique $(u(x), y)$ est positive non dégénérée sur $\Gamma_0(\mathbb{R})$.

En effet, soient \mathbb{R}_i les composantes irréductibles de \mathbb{R} . On a

$$\Gamma_0(\mathbb{R}) = \prod_i \Gamma_0(\mathbb{R}_i),$$

et la forme bilinéaire $(u(x), y)$ est le produit des formes

$$2^{-1}\ell(\alpha_i)^{-1}(p(x), y)$$

sur les $\Gamma_0(\mathbb{R}_i)$, où $\ell(\alpha_i)$ est le minimum de $\ell(\alpha)$ pour $\alpha \in \mathbb{R}_i$. Or ces différentes formes bilinéaires symétriques sont positives non dégénérées (1.2.6). 149

7.3. Matrice de Cartan. — Soit \mathcal{R} une donnée radicielle. Si S est un système de racines simples, on appelle *matrice de Cartan* de \mathcal{R} relativement à S la matrice carrée sur l'ensemble d'indices S définie par

$$a_{\alpha\beta} = (\alpha^*, \beta), \quad \text{pour } \alpha, \beta \in S.$$

Remarquons d'abord que si S' est un autre système de racines simples et w un élément de $W(\mathcal{R})$ tel que $w(S) = S'$, on a

$$(w(\alpha)^*, w(\beta)) = (\alpha^*, \beta),$$

donc que la matrice de Cartan de \mathcal{R} relativement à S' s'obtient à partir de celle relative à S par l'isomorphisme $S \rightarrow S'$ sur l'ensemble d'indices défini par w . Il en résulte qu'à un isomorphisme près sur l'ensemble d'indices, la matrice de Cartan ne dépend que de \mathcal{R} .

Proposition 7.3.1. — La matrice de Cartan possède les propriétés suivantes :

- (i) $a_{\alpha\alpha} = 2$, $a_{\alpha\beta} \leq 0$ pour $\alpha \neq \beta$.
- (ii) $a_{\alpha\beta} = 0$ entraîne $a_{\beta\alpha} = 0$.

(iii) Il existe des entiers strictement positifs m_α ($= \text{long}(\alpha)$) tels que la matrice

$$(m_\alpha a_{\alpha\beta})$$

soit symétrique, positive et non dégénérée.

150 (iv) Les mineurs diagonaux de la matrice $(a_{\alpha\beta})_{\alpha,\beta \in S}$, i.e. les déterminants

$$\det(a_{\alpha\beta})_{\alpha,\beta \in S'} \quad \text{pour } S' \subset S,$$

sont strictement positifs.

(v) On a $s_\alpha(\beta) = \beta - a_{\alpha\beta} \alpha$ et $s_\alpha(\beta^*) = \beta^* - a_{\beta\alpha} \alpha^*$.

En effet, (v) est une définition, (i) résulte de 3.2.11, (ii) de 2.2.2, (iii) de 7.2.9, (iv) se déduit aussitôt de (iii) par la relation

$$\det(m_\alpha a_{\alpha\beta})_{\alpha,\beta \in S'} = \prod_{\alpha \in S'} m_\alpha \cdot \det(a_{\alpha\beta})_{\alpha,\beta \in S'}.$$

Proposition 7.3.2. — Soient \mathcal{R} et \mathcal{R}' deux données radicielles simplement connexes (resp. adjointes) et réduites, S (resp. S') un système de racines simples de \mathcal{R} (resp. \mathcal{R}'), et $u : S \rightarrow S'$ un isomorphisme tel que si on note $(a_{\alpha\beta})$ et $(a'_{\alpha'\beta'})$ les matrices de Cartan de \mathcal{R} et \mathcal{R}' relativement à S et S' , on ait :

$$a'_{u(\alpha),u(\beta)} = a_{\alpha,\beta}.$$

Alors, il existe un unique isomorphisme de \mathcal{R} sur \mathcal{R}' qui induise u sur S .

Il suffit évidemment de faire la démonstration dans le cas adjoint. Alors $M = \Gamma_0(\mathcal{R})$ et $M' = \Gamma_0(\mathcal{R}')$ sont les groupes abéliens libres engendrés par S et S' . Il existe donc un unique isomorphisme de groupes de M sur M' qui induise u sur S . Notons-le aussi u . Montrons que $u(\mathcal{R}) \subseteq \mathcal{R}'$. Toute racine α de \mathcal{R} s'écrit $s_{\alpha_1} \cdots s_{\alpha_n}(\alpha_{n+1})$ avec $\alpha_i \in S$. On a évidemment

$$u(\alpha) = s_{u(\alpha_1)} \cdots s_{u(\alpha_n)}(u(\alpha_{n+1})),$$

en vertu de l'hypothèse sur u et des relations (v) de 7.3.1.

151 Il reste à prouver que ${}^t u(\mathcal{R}'^*) \subseteq \mathcal{R}^*$, ce qui résulte de ce que les éléments de M^* (resp. M'^*) sont déterminés par la dualité avec \mathcal{R} ou S (resp. \mathcal{R}' ou S'), par 1.2.5.

Corollaire 7.3.3. — Une donnée radicielle réduite simplement connexe ou adjointe est déterminée à isomorphisme près par sa matrice de Cartan.

Corollaire 7.3.4. — Soient \mathcal{R} une donnée radicielle réduite et simplement connexe (resp. adjointe), et S un système de racines simples. Le groupe $E_S(\mathcal{R})$ s'identifie au groupe des automorphismes de l'ensemble S qui laissent invariante la matrice de Cartan.

Remarque 7.3.5. — La question de l'existence d'une donnée radicielle correspondant à une matrice de Cartan donnée vérifiant (i) (ii) et (iv) (par exemple) ne se résoud pas facilement directement, sans utiliser la classification.

7.4. Diagrammes de Dynkin. —

Définition 7.4.1. — On appelle structure de *diagramme de Dynkin* (le mot « schéma » a été banni pour des raisons évidentes) sur un ensemble fini S la donnée d'un ensemble de couples d'éléments distincts de S , dits couples liés, et d'une application de S dans l'ensemble $\{1, 2, 3\}$. La notion d'isomorphisme de telles structures est évidente.

Définition 7.4.2. — Soient \mathcal{R} une donnée radicielle et S un système de racines simples. On appelle diagramme de Dynkin de \mathcal{R} relativement à S , l'ensemble S , deux racines simples étant liées si et seulement si elles ne sont pas orthogonales, à chaque racine étant associée sa longueur. 152

Proposition 7.4.3. — *Diagramme de Dynkin et matrice de Cartan se déterminent bi-univoquement.*

En effet l'équivalence

$$\alpha \text{ et } \beta \text{ ne sont pas liés} \iff a_{\alpha\beta} = 0,$$

et la relation

$$\text{long}(\alpha) a_{\alpha\beta} = \text{long}(\beta) a_{\beta\alpha},$$

(avec $\inf \text{long}(\alpha) = 1$ dans chaque composante connexe du diagramme) déterminent les $a_{\alpha\beta}$ en fonction des liaisons et des longueurs, et réciproquement (le détail de la vérification est laissé au lecteur).

Corollaire 7.4.4. — *Une donnée radicielle réduite simplement connexe ou adjointe est déterminée par son diagramme de Dynkin.*

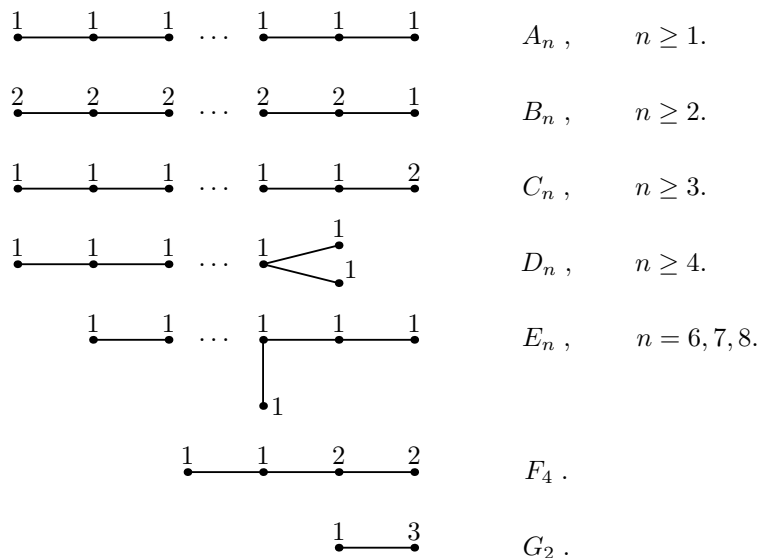
Corollaire 7.4.5. — *Soient \mathcal{R} une donnée radicielle réduite simplement connexe ou adjointe et S un système de racines simples. Le groupe $E_S(\mathcal{R})$ s'identifie au groupe des automorphismes du diagramme de Dynkin de \mathcal{R} relativement à S , c'est-à-dire au groupe des permutations de S conservant les longueurs et les liaisons.*

Remarque 7.4.6. — On classe avec la méthode habituelle (*) les divers diagrammes de Dynkin connexes, et on montre que chacun correspond effectivement à une donnée radicielle *réduite simplement connexe irréductible*. On trouve les types bien connus 153 ci-dessous.

Par 7.4.5, on trouve aussitôt le groupe $E_S(\mathcal{R})$ correspondant :

$$\begin{aligned} E_S(\mathcal{R}) &= \{e\} \text{ pour } A_1, B_n, C_n, E_7, E_8, F_4, G_2. \\ E_S(\mathcal{R}) &= \mathbb{Z}/2\mathbb{Z} \text{ pour } A_n \ (n \geq 2), D_n \ (n \geq 5), E_6. \\ E_S(\mathcal{R}) &= \mathfrak{S}_3 \text{ pour } D_4. \end{aligned}$$

(*) *Confer* Bourbaki, Groupes et algèbres de Lie, chap. VI. ou Séminaire Sophus Lie.



7.5. Compléments sur les p -morphisms. — Soit $f : \mathcal{R} \rightarrow \mathcal{R}'$ un p -morphisme (cf. 6.8). Il est clair sur les définitions que la bijection $u : R \xrightarrow{\sim} R'$ associée à f fait se correspondre systèmes de racines simples, systèmes de racines positives, composantes irréductibles (etc.) de R et de R' . Supposons donc pour simplifier R et R' *irréductibles*.

Lemme 7.5.1. — *Si R et R' sont irréductibles, il existe $k \in \mathbb{Q}$ tel que pour tout $\alpha \in R$*

$$k \operatorname{long}(u(\alpha)) = q(\alpha)^2 \operatorname{long}(\alpha).$$

En effet, on a

$$\begin{aligned} \operatorname{long}(\alpha)(\alpha^*, \beta) &= \operatorname{long}(\beta)(\beta^*, \alpha), \\ \operatorname{long}(u(\alpha))(u(\alpha)^*, u(\beta)) &= \operatorname{long}(u(\beta))(u(\beta)^*, u(\alpha)). \end{aligned}$$

154 On en déduit aussitôt que pour α et β non orthogonales, on a

$$\operatorname{long}(u(\alpha))^{-1} q(\alpha)^2 \operatorname{long}(\alpha) = \operatorname{long}(u(\beta))^{-1} q(\beta)^2 \operatorname{long}(\beta).$$

On conclut alors par 7.1.3.

Remarque 7.5.2. — Il résulte de 7.2.2. et 6.8.4. que $q(\alpha)$ ne dépend que de $\operatorname{long}(\alpha)$. On voit alors facilement que si $q(\alpha)$ n'est pas constant, alors $q(\alpha) \operatorname{long}(\alpha)$ est constant, ce qui montre qu'alors $p = 2$ ou 3 . Un coup d'oeil sur les diagrammes du numéro précédent montre qu'il y a quatre cas possibles (on désigne par la même lettre un diagramme de Dynkin et la donnée radicielle simplement connexe réduite correspondante) :

$$\begin{aligned} p = 2, \quad B_n &\xrightarrow{f_1} C_n, & C_n &\xrightarrow{f_2} B_n & (\text{avec } C_2 = B_2). \\ p = 2, \quad F_4 &\xrightarrow{g} F_4. \\ p = 3, \quad G_2 &\xrightarrow{h} G_2. \end{aligned}$$

Le lecteur remarquera que $f_1 \circ f_2$, $f_2 \circ f_1$, $g \circ g$ et $h \circ h$ sont des p -morphisms de la forme décrite en 6.8.6.

7.5.3. — On voit aussitôt sur la description précédente que si \mathcal{R} et \mathcal{R}' sont deux données radicielles réduites de rang semi-simple ≤ 2 et si on a un p -morphisme de \mathcal{R}' dans \mathcal{R} , alors \mathcal{R} et \mathcal{R}' sont de même type. Plus précisément, on a le tableau suivant.

Notations : Soit $f : \mathcal{R}' \rightarrow \mathcal{R}$ un p -morphisme. On désigne par q (resp. q_1) une puissance positive quelconque de p . On utilise pour les systèmes de rang 2 les notations du numéro 4 (on désigne par α, β les racines simples, avec $\ell(\alpha) \leq \ell(\beta)$). 155

Type	p	valeurs de f	valeurs de ${}^t f$
Trivial	quelconque	-	-
A_1	quelconque	$f(\alpha') = q\alpha$	${}^t f(\alpha^*) = q\alpha'^*$
$A_1 \times A_1$	quelconque	$f(\alpha') = q\alpha$ $f(\beta') = q_1\beta$	${}^t f(\alpha^*) = q\alpha'^*$ ${}^t f(\beta^*) = q_1\beta'^*$
A_2, B_2, G_2	quelconque	$f(\alpha') = q\alpha$ $f(\beta') = q\beta$	${}^t f(\alpha^*) = q\alpha'^*$ ${}^t f(\beta^*) = q\beta'^*$
B_2	$p = 2$	$f(\alpha') = q\beta$ $f(\beta') = 2q\alpha$	${}^t f(\alpha^*) = 2q\beta'^*$ ${}^t f(\beta^*) = q\alpha'^*$
G_2	$p = 3$	$f(\alpha') = q\beta$ $f(\beta') = 3q\alpha$	${}^t f(\alpha^*) = 3q\beta'^*$ ${}^t f(\beta^*) = q\alpha'^*$

Bibliographie

- [BLie68] N. Bourbaki, *Groupes et algèbres de Lie*, Ch. 4–6, Hermann, 1968.
 [Se66] J.-P. Serre, *Algèbres de Lie semi-simples complexes*, Benjamin, 1966.

