Systèmes de racines

H. Randriam

27 novembre 1996

On se propose ici de présenter les bases de la théorie abstraite des systèmes de racines. Ces systèmes apparaissent en gros comme les valeurs propres de l'action adjointe sur une algèbre de Lie semi-simple complexe $\mathcal{G}$ d'une sous-algèbre de Cartan $\mathcal{H}$, l'élément important (mais que nous n'aborderons pas) étant que $\mathcal{G}$ est déterminée à isomorphisme près par son système de racines.

Cet exposé ne prétend à aucune originalité puisqu'il suit plus ou moins le traitement de J.-P.Serre, Algèbres de Lie semi-simples complexes (Benjamin).

1 Systèmes de racines et données radicielles

Définition 1 *Une partie R d'un espace vectoriel réel V est appelé système de racines si*

1. *R est fini, engendre V, et ne contient pas 0*
2. *pour tout $\alpha \in R$ il existe une symétrie hyperplane s_α laissant stable R, avec $s_\alpha(\alpha) = -\alpha$*
3. *pour tous $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ est un multiple entier de α.*

Les s_α sont uniquement déterminés. En effet la composée de deux telles symétries associées au même α est une transvection de vecteur α, et elle induit une permutation de R, donc est d'ordre fini puisque R engendre V. C'est donc l'identité. Ainsi on peut écrire de manière unique $s_\alpha = \mathrm{Id} - \breve{\alpha} \otimes \alpha$, avec $\breve{\alpha}(\alpha) = 2$ et $\breve{\alpha}(R) \subset \mathbb{Z}$. On appelle $\breve{\alpha}$ la racine inverse de α.

Soit $\alpha \in R$. Alors $s_\alpha(\alpha) = -\alpha \in R$. On dit que R est réduit si pour tout α on obtient ainsi toutes les racines proportionnelles à α.

Si R n'est pas réduit, il contient deux racines proportionnelles α et $t\alpha$, $0 < t < 1$. Alors $\breve{\alpha}(t\alpha) \in \mathbb{Z}$, donc $t = 1/2$.

Définition 2 *On appelle groupe de Weyl de R le sous-groupe W de $GL(V)$ engendré par les s_α.*

C'est un sous-groupe distingué du groupe $Aut(R)$ des automorphismes de V laissant stable R, lui-même sous-groupe du groupe (fini) des permutations de R.

On munit V d'une forme euclidienne invariante par W en faisant la moyenne des transformés par W d'une forme euclidienne arbitraire, de telle sorte que W devient un sous-groupe de $O(V)$. En identifiant V à son dual, on peut alors écrire $\check{\alpha} = 2/(\alpha,\alpha).\alpha$, et la troisième condition des systèmes de racines devient: $\forall \alpha, \beta \in R$, $2(\alpha,\beta)/(\alpha,\alpha) \in \mathbb{Z}$.

Si R est un système de racines de V, l'ensemble $\check{R}$ des racines inverses forme un système de racine de $\check{V}$. C'est le système inverse (ou dual) de V. Les symétries sont données par $s_{\check{\alpha}} = {}^t s_\alpha$, et on a $\check{\check{\alpha}} = \alpha$. Le groupe de Weyl de $\check{R}$ s'identifie à celui de R via l'application $w \mapsto {}^t w^{-1}$.

Remarque: On aurait aussi pu considérer un espace vectoriel V sur un corps K quelconque et une partie R de V remplissant les mêmes conditions. Pour $K = \mathbb{C}$, R est un système de racines du sous-espace réel de V qu'il engendre. Réciproquement tout système de racines complexes s'obtient comme complexifié d'un système de racines réel.

Voici une autre généralisation de la notion de système de racines:

Définition 3 *on appelle donnée radicielle un quadruplet* $(X, \Phi, \check{X}, \check{\Phi})$ *où* X *et* $\check{X}$ *sont des groupes abéliens libres de type fini en dualité sur* $\mathbb{Z}$, Φ *et* $\check{\Phi}$ *des parties finies de* X *et* $\check{X}$ *avec une bijection* $\alpha \mapsto \check{\alpha}$ *de* Φ *sur* $\check{\Phi}$, *telle que* $< \alpha, \check{\alpha} >= 2$. *Cela permet de définir des symétries* $s_\alpha = \mathrm{Id} - \check{\alpha} \otimes \alpha$ *sur* X *et* $s_{\check{\alpha}} = \mathrm{Id} - \alpha \otimes \check{\alpha}$ *sur* $\check{X}$, *et on impose* $s_\alpha(\Phi) = \Phi$, $s_{\check{\alpha}}(\check{\Phi}) = \check{\Phi}$

Il est alors clair que $(\check{X}, \check{\Phi}, X, \Phi)$ est aussi une donnée radicielle, dite duale de la précédente.

Soit Q le sous-groupe de X engendré par Φ, et X_0 l'orthogonal dans X de $\check{\Phi}$. La donnée radicielle est dite semisimple si $X_0 = 0$, torale si Φ est vide.

On vérifie trivialement que si $\Phi \neq \emptyset$, c'est un système de racines de $Q \otimes \mathbb{R}$.

On a d'autre part la propriété suivante:

Lemme 1 $Q \cap X_0 = 0$ *et* $Q + X_0$ *est d'indice fini dans* X.

Demonstration: On définit $p : X \to \check{X}$ par $p(x) = \sum_{\alpha\in\Phi} < x, \check{\alpha} > \check{\alpha}$. Trivialement $X_0 \subset \ker p$, et comme $< x, p(x) >= \sum_{\alpha\in\Phi} < x, \check{\alpha} >^2$, il y a égalité. Ensuite en sommant sur β l'identité

$$< \alpha, \check{\beta} >^2 \check{\alpha} =< \alpha, \check{\beta} > \check{\beta} + < \alpha, s_{\check{\alpha}}(\check{\beta}) > s_{\check{\alpha}}(\check{\beta})$$

on trouve que $p(\alpha) = 1/2. < \alpha, p(\alpha) > \check{\alpha}$. Cela montre que p induit une surjection de $Q \otimes \mathbb{Q}$ sur son dual, qui par symétrie ont donc même dimension. On en déduit que $Q \cap \ker p = 0$, ce qui permet de conclure.

2 Bases

Soit R un système de racines de V.

On commence par étudier les positions relatives possibles de deux racines. Soient $\alpha, \beta \in R$. Posons $n(\beta,\alpha) = \check{\alpha}(\beta) = 2(\alpha,\beta)/(\alpha,\alpha) \in \mathbb{Z}$. Si ϕ est l'angle que font α et β, on a $n(\beta,\alpha) = 2(|\beta|/|\alpha|)\cos\phi$ d'où $n(\alpha,\beta)n(\beta,\alpha) = 4\cos^2\phi$. En se limitant au cas où les racines ne sont pas proportionnelles, il n'y a que 7 possibilités (à échange près):

1	$n(\alpha,\beta)=0$	$n(\beta,\alpha)=0$	$\phi=\pi/2$	
2	$n(\alpha,\beta)=1$	$n(\beta,\alpha)=1$	$\phi=\pi/3$	$\|\beta\|=\|\alpha\|$
3	$n(\alpha,\beta)=-1$	$n(\beta,\alpha)=-1$	$\phi=2\pi/3$	$\|\beta\|=\|\alpha\|$
4	$n(\alpha,\beta)=1$	$n(\beta,\alpha)=2$	$\phi=\pi/4$	$\|\beta\|=\sqrt{2}\|\alpha\|$
5	$n(\alpha,\beta)=-1$	$n(\beta,\alpha)=-2$	$\phi=3\pi/4$	$\|\beta\|=\sqrt{2}\|\alpha\|$
6	$n(\alpha,\beta)=1$	$n(\beta,\alpha)=3$	$\phi=\pi/6$	$\|\beta\|=\sqrt{3}\|\alpha\|$
7	$n(\alpha,\beta)=-1$	$n(\beta,\alpha)=-3$	$\phi=5\pi/6$	$\|\beta\|=\sqrt{3}\|\alpha\|$

Proposition 1 *Soient $\alpha, \beta \in R$ non proportionnelles, $n(\alpha,\beta) > 0$. Alors $\alpha - \beta \in R$.*

DEMONSTRATION: On peut supposer $n(\alpha,\beta) = 1$, auquel cas $\alpha - \beta = s_\beta(\alpha)$.

Définition 4 *On appelle base de R une partie $S \subset R$ qui forme une base de l'espace vectoriel V et telle que les coefficients dans cette base des éléments de R sont des entiers tous de même signe.*

On appelle chambre de Weyl une composante connexe du complémentaire dans V de l'union des hyperplans orthogonaux des racines. On se fixe une chambre de Weyl C et un $t \in C$. Soit $R_t^{\pm}$ l'ensemble des racines α vérifiant $\pm(t,\alpha) > 0$, de telle sorte que $R = R_t^+ \cup R_t^-$. Un $\alpha \in R_t^+$ est dit décomposable si on peut l'écrire $\alpha = \beta + \gamma$ avec $\beta, \gamma \in R_t^+$, indécomposable sinon. Soit S_t l'ensemble des éléments indécomposables de R_t^+. Ces ensembles ne dépendent bien sûr pas du choix de t dans C.

Théorème 1 *S_t est une base de R, et réciproquement si S est une base et $t \in V$ tel que $(t,S) > 0$, alors $S = S_t$.*

DEMONSTRATION: On remarque d'abord que tout élément $\alpha \in R_t^+$ est combinaison linéaire entière positive d'éléments de S_t (cela se montre par induction sur (t,α).). Ensuite, soient $\alpha, \beta \in S_t$. Comme ils sont tous deux irréductibles, $\alpha - \beta$ n'est pas une racine, et on a vu que ça impliquait $(\alpha,\beta) \leq 0$. Mais comme d'autre part on a $(t,\alpha) > 0$ pour tout $\alpha \in S_t$, un petit raisonnement montre que les éléments de S_t sont linéairement indépendants. On vient donc de voir que S_t est une base. Réciproquement soient S une base et t tel que $(t,S) > 0$, R^+

la partie de R formée des combinaisons linéaires entières positives d'éléments de S. Alors $R^+ \subset R_t^+$, $(-R^+) \subset R_t^-$, d'où $R^+ = R_t^+$, et alors S est formé d'indécomposables de R_t^+, d'où $S \subset S_t$, et enfin $S = S_t$.

On se fixe maintenant une base S et un t tel que $\forall \alpha \in S, (t, \alpha) = 1$ (de telle sorte que $S = S_t$).

Proposition 2 *Toute racine positive β s'écrit $\beta = \alpha_1 + \ldots + \alpha_k$ ($\alpha_i \in S$) de telle sorte que les sommes partielles $\alpha_1 + \ldots + \alpha_h, 1 \leq h \leq k$ soient des racines.*

DEMONSTRATION: Si $S \cup \{\beta\}$ n'est pas libre, on peut trouver un α tel que $(\alpha, \beta) > 0$, donc $\gamma = \beta - \alpha$ est une racine, et est même positive puisque α est indécomposable. On a alors $(t, \gamma) = (t, \beta) - 1$ et on peut conclure par une récurrence.

Proposition 3 *Supposons R réduit, et soit $\alpha \in S$. Alors s_α laisse stable $R^+ - \{\alpha\}$.*

DEMONSTRATION: Soit $\beta \in R^+ - \{\alpha\}$. β n'est pas proportionnel à α donc on peut trouver un $\gamma \in S$ ayant un coefficient > 0 dans la décomposition de β sur S. Alors $s_\alpha(\beta) = \beta - n(\beta, \alpha)\alpha$ a même coefficient en γ, et comme les coefficients sont tous de même signe, $s_\alpha(\beta) \in R^+$.

Corollaire 1 *Soit ρ la demi-somme des racines positives, et $\alpha \in S$. Alors $s_\alpha(\rho) = \rho - \alpha$.*

DEMONSTRATION: C'est évident.

Proposition 4 *Supposons R réduit, alors $\check{S}$ est une base de $\check{R}$.*

DEMONSTRATION: Dire que S est une base revient à remarquer qu'elle est formée des générateurs des demi-droites extrémales du cône convexe engendré par R^+. Or cette propriété n'est pas affectée par le passage au dual qui se fait au moyen de l'inversion $\check{\alpha} = 2\alpha/(\alpha, \alpha)$.

On supposera désormais que R est réduit.

Soit S une base de R, W_S le sous-groupe de W engendré par les s_α pour $\alpha \in S$.

Théorème 2

1. *$\forall t \in V \exists w \in W \forall \alpha \in S, (w(t), \alpha) \geq 0$*
2. *pour toute base S', il existe $w \in W$ tel que $w(S') = S$*
3. *$\forall \beta \in R \exists w \in W, w(\beta) \in S$*
4. *$W = W_S$*

DEMONSTRATION: On commence par montrer 1., 2. et 3. pour W_S, ce qui est a priori plus fort. Pour 1., soit ρ la demi-somme de R^+ et $w \in W$ tel que $(w(t), \rho)$ soit maximum. Alors, pour tout $\alpha \in S$ on a

$$(w(t), \alpha) = (w(t), \rho - s_\alpha(\rho)) = (w(t), \rho) - (s_\alpha w(t), \rho)) \geq 0.$$

Pour 2. soit t' tel que $\forall \alpha' \in S', (t', \alpha') = 1$, puis $w \in W_S$ tel que $\forall \alpha \in S, (w(t'), \alpha) \geq 0$, donc > 0. On a alors $S = S_{w(t')}$ donc $S = w(S')$. Pour 3., soit $\beta \in R$. On commence par prendre un t_0 tel que $(t_0, \beta) = 0$ et $(t_0, \gamma) \neq 0$ si $\gamma \neq \pm\beta$. Ensuite soit t proche de t_0 et $\epsilon > 0$, $(t, \pm\beta) = \pm\epsilon$, $|(t, \gamma)| > \epsilon$ sinon. On a alors trivialement $\beta \in S_t$, et il suffit de prendre $w \in W_S, w(S_t) \subset S$. Montrons enfin 4.. W est engendré par les $s_\beta, \beta \in R$. Soit $w \in W_S$ tel que $w(\beta) \in S$. Alors $s_\beta = w^{-1}.s_{w(\beta)}.w \in W_S$.

REMARQUE: En fait on pourrait montrer que le w dont 2. affirme l'existence est unique.

3 Classification

Définition 5 *On appelle matrice de Cartan de R relativement à la base S la matrice de terme $(n(\alpha, \beta)|\alpha, \beta \in S)$.*

Proposition 5 *Un système de racines réduit est déterminé à isomorphisme près par sa matrice de Cartan.*

DEMONSTRATION: Cela découle immédiatement du fait que $R = W(S)$.

Soit E le groupe des permutations de S qui laissent la matrice de Cartan invariante, et qui s'identifie ainsi au groupe des automorphismes de R qui laissent stable S. Compte tenu du résultat mentionné dans la précédente remarque, on trouve que $\mathrm{Aut}(R)$ est produit semi-direct de E et W.

En particulier $E = \mathrm{Aut}(R)/W$.

Définition 6 *On appelle graphe de Coxeter de R relativement à la base S le graphe dont les sommets sont les éléments de S, deux sommets distincts α et β etant joints par $n(\alpha, \beta)n(\beta, \alpha)$ arêtes.*

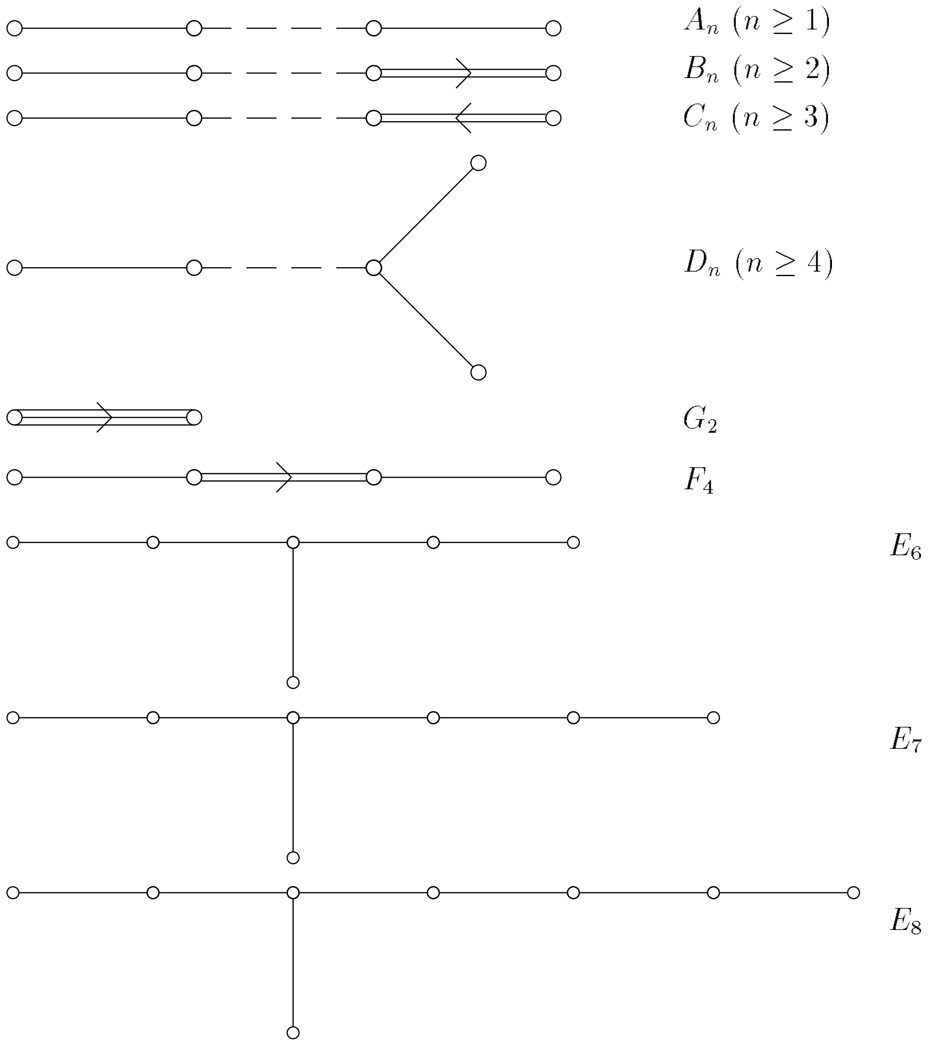
Proposition 6 *On suppose $V = V_1 \oplus V_2$ et $R \subset V_1 \cup V_2$. Alors $V_1 \perp V_2$ et $R_i = R \cap V_i$ est un système de racines de V_i.*

DEMONSTRATION: Si $\alpha \in R_1$ et $\beta \in R_2$, $\alpha - \beta \notin V_1 \cup V_2 \supset R$ donc $(\alpha, \beta) \leq 0$ et de même $(\alpha, -\beta) \leq 0$.

On dit alors que R est somme des sous-systèmes R_i. On a alors la notion naturelle de système de racines irréductible, et on vérifie facilement qu'un système de racines est irréductible si et seulement sison graphe de Coxeter est connexe.

Le graphe de Coxeter ne permet pas de retrouver la matrice de Cartan. Pour ce faire on introduit le schéma de Dynkin, obtenu en rajoutant sur les arêtes multiples du graphe de Coxeter un signe $>$ indiquant quelle est la racine la plus longue.

Théorème 3 *Tout schéma de Dynkin connexe non vide est isomorphe à l'un des suivants:*



La démonstration se fait en plusieurs étapes.

A un schéma de Dynkin d'ensemble de sommets S on associe une forme bilinéaire symétrique sur R^S de base canonique $(e_\alpha)_{\alpha \in S}$ en imposant: $(e_\alpha, e_\alpha) = 1$ et $(e_\alpha, e_\beta) = \cos(\pi/2), \cos(2\pi/3), \cos(3\pi/4)$ ou $\cos(5\pi/6)$, selon que α et β sont joints par 0, 1, 2 ou 3 arêtes. Une condition nécessaire est alors que cette forme est définie positive. Si c'est le cas on dira que le schéma de Dynkin est admissible.

On vérifie immédiatement que tout sous-schéma d'un schéma de Dynkin admissible obtenu en enlevant des sommets et toutes les arêtes partant de ces sommets est encore admissible.

Soit $e = \sum_{\alpha \in S} e_\alpha$. Alors $0 > e^2 = \sum_{\alpha \in S} e_\alpha^2 + 2\sum_{\{\alpha \neq \beta\}}(e_\alpha, e_\beta)$. Mais si $(e_\alpha, e_\beta) \neq 0$, c'est ≤ -1. Le nombre de paires $\{e_\alpha, e_\beta\}$ reliées par au moins une arête est donc au plus $\#S - 1$. Le schéma étant connexe, on en déduit que c'est un arbre. En particulier il est acyclique.

Soit $\alpha \in S$ et $(\beta_i)_{i=1\ldots k}$ les sommets reliés à α. Alors par acyclicité, les e_{β_i} sont deux à deux orthogonaux, et le sous-espace vectoriel qu'ils engendrent ne contient pas e_α. Ainsi le carré de la distance de e_α à ce sous-espace vaut $1 - \sum_{i=1}^k (e_\alpha, e_{\beta_i})^2 > 0$, donc $4\sum_{i=1}^k \cos^2(\phi_{\alpha\beta_i}) \leq 3$. Autrement dit il part de tout sommet au plus 3 arêtes, comptées avec multiplicité.

Soient α et β reliés. Alors si le schéma est admissible, le schéma obtenu en identifiant α et β est encore admissible. En effet, soit $(x_\gamma)_{\gamma \in S/\alpha=\beta=p}$ une famille de réels non tous nuls arbitraire. Alors $(\sum_{\gamma \in S/\alpha=\beta=p} x_\gamma . e_\gamma)^2 = (x_p e_\alpha + x_p e_\beta + \sum_{\gamma \in S-\{\alpha,\beta\}} x_\gamma . e_\gamma)^2 - (1 + 2(e_\alpha, e_\beta))x_p^2 > 0$

Cela implique que tout schéma de Dynkin admissible a au plus: un point de ramification ou alors une arête multiple

Soient $1, 2, \ldots, k$ une chaîne simple de sommets. Alors $e = \sum_{l=1}^k l e_l$ est de carré $\sum_{l=1}^k l^2 - 2\sum_{l=1}^{k-1} l(l+1)/2 = k(k+1)/2$.

Supposons maintenant que notre graphe ait un point de ramification e. Soient $(x_1, \ldots, x_p)$, $(y_1, \ldots, y_q)$ et $(z_1, \ldots, z_r)$, les vecteurs correspondants aux chaînes partant de ce point de ramification, $x = \sum_l l x_l$, etc. Alors $x^2 = p(p+1)/2, y^2 = q(q+1)/2, z^2 = r(r+1)/2$. D'autre part x, y, z sont 2 à 2 orthogonaux, et $(e, x) = -p/2, (e, y) = -q/2, (e, z) = -r/2$. Le carré de la distance de e au sous-espace engendré par (x, y, z) vaut $1 - (e, x/|x|)^2 - (e, y/|y|)^2 - (e, z/|z|)^2 > 0$ d'où

$$\frac{1}{p+1} + \frac{1}{q+1} + \frac{1}{r+1} > 1.$$

Les seuls schémas admissibles possibles sont donc bien E_6, E_7, E_8 et les D_n.

Un raisonnement analogue permet de régler le sort des schémas ayant une arête multiple. Ainsi un schéma de Dynkin admissible nécessairement un de ceux enoncés par le théorème.

Remarque: Si un schéma de Dynkin est admissible, on peut trouver un système de racines lui correspondant en multipliant par des constantes convenables

les e_α associés.

Poursuivons la démonstration du théorème. Il s'agit maintenant de prouver la réciproque, à savoir que tous ces schémas de Dynkin sont bien admissibles, et pour cela on va construire des systèmes de racines leur correspondant. Les vérifications sont laissées au lecteur.

- A_n: V l'hyperplan de $\mathbb{R}^{n+1}$ orthogonal à $e_1 + \ldots + e_n$, R l'ensemble des $e_i - e_j$, $i \neq j$, et S les $e_i - e_{i+1}$, $1 \leq i \leq n$,
- B_n: V=$\mathbb{R}^n$, R formé des $\pm e_i$ et des $\pm e_i \pm e_j$, $i \neq j$, et $S = (e_1 - e_2, \ldots, e_{n-1} - e_n, e_n)$.
- C_n: l'inverse de B_n formé des $\pm 2e_i$ et des $\pm e_i \pm e_j$.
- D_n: $V = \mathbb{R}^n$, R formé des $\pm e_i \pm e_j$, $i \neq j$, et $S = (e_1 - e_2, \ldots, e_{n-1} - e_n, e_{n-1} + e_n)$.
- G_2: isomorphe à l'anneau des entiers du corps des racines cubiques de 1, dont la norme vaut 1 ou 3.
- F_4: $V = \mathbb{R}^4$, R formé des $\pm e_i$, des $\pm e_i \pm e_j$, $i \neq j$, et des $(\pm e_1 \pm e_2 \pm e_3 \pm e_4)/2$, avec $S = (e_2 - e_3, e_3 - e_4, e_4, (e_1 - e_2 - e_3 - e_4)/2)$
- E_8: $V = \mathbb{R}^8$, R formé des $\pm e_i \pm e_j$, $i \neq j$ et des $\sum_i (-1)^{m(i)} e_i$ tels que $\sum_i m(i)$ soit pair, et de base $S = ((e_1 + e_2 - \sum_{i=2}^{7} e_i)/2, e_1 + e_2, e_2 - e_1, \ldots, e_7 - e_6)$.
- E_6 et E_7: l'intersection de E_8 avec le sous-espace engendré par les 6 ou 7 premiers vecteurs de S.