<u>Référence:</u>

- W. Ebeling
  Lattices and Codes
  Chap I, § 1.4.

- Bourbaki
  Groupes et Algèbres de Lie
  Chap <u>VI</u>

Réseaux de Racines

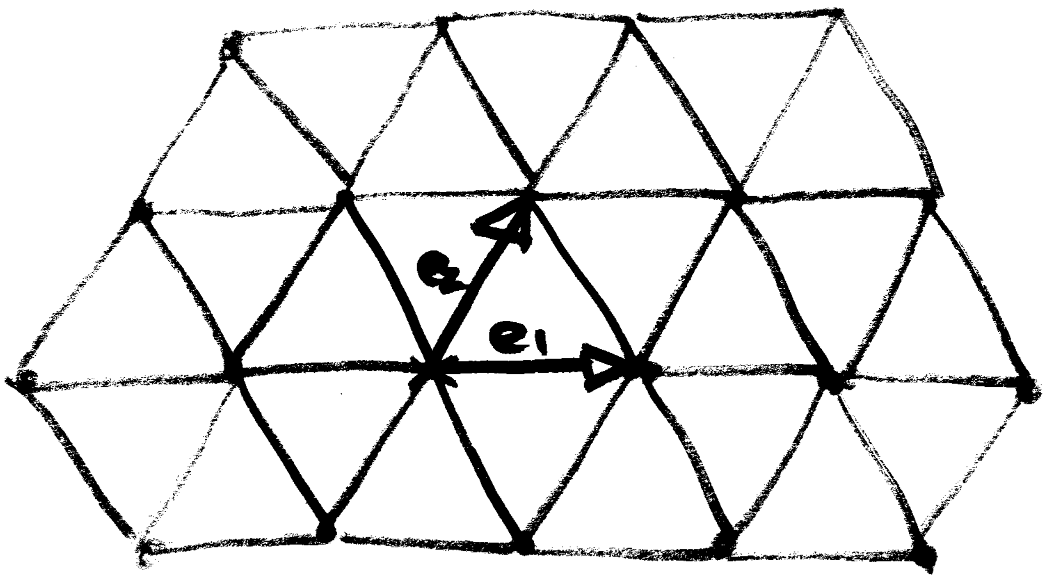
$\Gamma \subset \mathbb{R}^n$ un réseau pair.
(i.e. $\forall x \in \Gamma,\ x.x \in 2\mathbb{Z}$)

$R = \{\text{vecteurs minimaux}\}$
$\quad = \{x \in \Gamma,\ x.x = 2\}$

$x \in R$ est appelé une <u>racine</u>.

<u>Déf</u>: Si R engendre Γ, alors Γ est un <u>réseau de racines</u>.

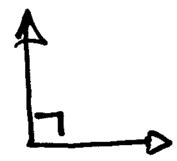
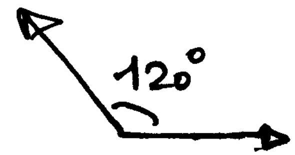
<u>Exemple</u> : Réseau Hexagonal



$\|e_1\| = \|e_2\| = \sqrt{2}$

Thm 1 : Si Γ est un réseau de racines, il possède une base $(e_1, \dots, e_n)$ telle que

$\forall i,\quad e_i \cdot e_i = 2 \quad$ (i.e. $e_i \in R$)

$\forall i,j,\ i \neq j \quad e_i \cdot e_j \in \{0, -1\}$ ( ou )

Exple :

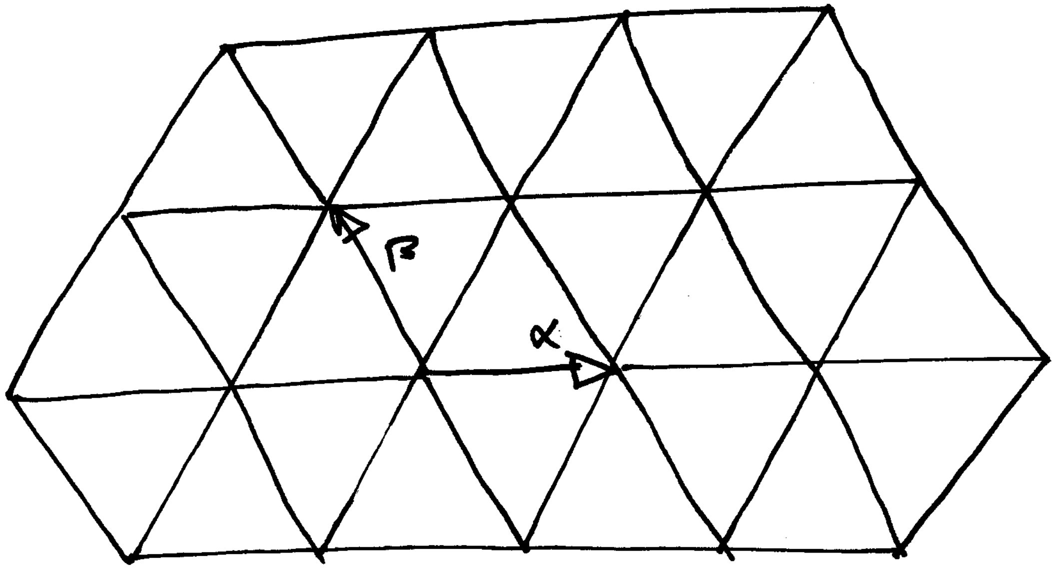
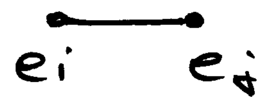


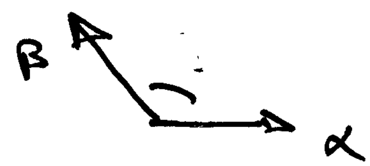
Diagramme de Dynkin Associé

* Chaque élément e_i de la base $\longleftrightarrow$ Un sommet $\underset{e_i}{\bullet}$

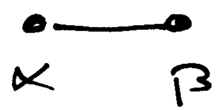
* e_i et e_j sont liés par une arête $\Longleftrightarrow$ $e_i \cdot e_j = -1$.



Exemple : Réseau Hexagonal



$\alpha \cdot \beta = -1$



Exple 2 : Réseau Réductible

$$\Gamma = \Gamma_1 \overset{\perp}{\oplus} \Gamma_2 \qquad \Gamma_1 \subset \mathbb{R}^{n_1},\ \Gamma_2 \subset \mathbb{R}^{n_2}$$

$$\Gamma \subset \mathbb{R}^{n_1+n_2}$$

$$\Delta \qquad \Delta_1 \cup \Delta_2$$

$$\Gamma = \underbrace{\mathbb{Z}e_1 \oplus \mathbb{Z}e_2}_{\text{Hexagonale}} \overset{\perp}{\oplus} \underbrace{\mathbb{Z}e_3 \oplus \mathbb{Z}e_4}_{\text{Hexagonale}}$$

$$e_1 \cdot e_2 = e_3 \cdot e_4 = -1$$

$$\begin{cases} e_1 \cdot e_3 = e_1 \cdot e_4 = 0 \\ e_2 \cdot e_3 = e_2 \cdot e_4 = 0 \end{cases}$$

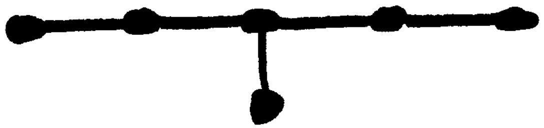
Δ

Deux composantes connexes.

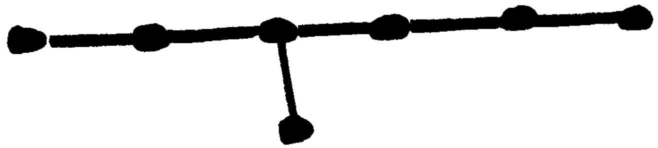
Théorème 2 : Les diagrammes connexes possibles sont :

A_n (n sommets).

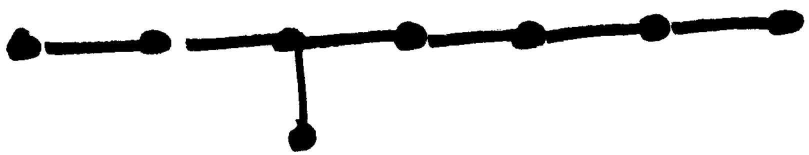
D_n (n sommets).



E_6



E_7



E_8

Et chaque diagramme correspond effectivement à un réseau.

Objectif du devoir :

Etudier le code de Hamming étendu $\widetilde{H}$

et le réseau associé $\Gamma_{\widetilde{H}}$

Réseau de Racines de type E_8

Question prêliminaire 1.

$$\mathrm{Gram}(v_1, \dots, v_n) = \begin{pmatrix} v_1 \cdot v_1 & \cdots & v_n \cdot v_1 \\ v_1 \cdot v_2 & & \vdots \\ \vdots & \ddots & \vdots \\ v_1 \cdot v_n & \cdots & v_n \cdot v_n \end{pmatrix}$$

$v_i \in \mathbb{R}^n$.

Si $(v_1, \dots, v_n)$ est liée, alors
$\det(\mathrm{Gram}(v_1, \dots, v_n)) = 0$

Remarque : Argument inductif ?
Si (e_1, e_2) libre, alors (e_1, e_2, e_1+e_2) liée
mais (e_1, e_2), (e_1, e_1+e_2), (e_2, e_1+e_2)
sont libres.

Si $(v_1, \dots, v_n)$ est liée, il existe $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$ tels que $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$.

<u>Alors</u>
$$\begin{cases} \lambda_1 v_1 \cdot v_1 + \dots + \lambda_n v_n \cdot v_1 = 0 \\ \vdots \\ \lambda_1 v_1 \cdot v_n + \dots + \lambda_n v_n \cdot v_n = 0 \end{cases}$$

cad $\lambda_1 C_1 + \dots + \lambda_n C_n = 0$

où $\mathrm{Gram}(v_1, \dots, v_n) = (C_1, \dots, C_n)$ colonnes.

D'où $\det(\mathrm{Gram}(v_1, \dots, v_n)) = 0$.

Code de Hamming étendu

$$\tilde{H} = \{ (x_1, \dots, x_7, x_1 + \dots + x_7),\ (x_1, \dots, x_7) \in H \}$$

$$= \{ (x_1, x_2, x_3, x_4, x_1 + x_2 + x_3, x_1 + x_2 + x_4, x_1 + x_3 + x_4, x_2 + x_3 + x_4) \}$$

$\tilde{H} \subset \mathbb{F}_2^{\,8}$, de dimension 4.

Code de Hamming étendu

$$\tilde{H} = \{ (x_1, \dots, x_7, x_1 + \dots + x_7), (x_1, \dots, x_7) \in H \}$$

$$= \{ (x_1, x_2, x_3, x_4, x_1 + x_2 + x_3, x_1 + x_2 + x_4, x_1 + x_3 + x_4, x_2 + x_3 + x_4) \}$$

$\tilde{H} \subset \mathbb{F}_2^{8}$, de dimension 4.

Mots : 00000000 11111111

$\tilde{c}_1 = 00010111$	10001110	14 mots de poids 4
$\tilde{c}_2 = 00101011$	00111100	
$\tilde{c}_3 = 01001101$	01011010	
$\tilde{c}_4 = 11000011$	01100110	
$\tilde{c}_5 = 10011001$	10110010	
$\tilde{c}_6 = 10100101$	11010100	
$\tilde{c}_7 = 01110001$	11101000	

Code de Hamming étendu $\tilde{H}$

Rappel : C code binaire linéaire, $C \subset \mathbb{F}_2^n$

$$C^\perp = \left\{ y \in \mathbb{F}_2^n,\ x \underset{\mathbb{F}_2}{\cdot} y = 0 \ \forall x \in C \right\}$$

où
$$x \underset{\mathbb{F}_2}{\cdot} y = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_2 .$$
$$= \frac{1}{2} \left(w(x+y) - w(x) - w(y) \right) \in \mathbb{F}_2$$

Code de Hamming étendu $\tilde{H}$

Rappel : C code binaire linéaire, $C \subset \mathbb{F}_2^n$

$$C^\perp = \left\{ y \in \mathbb{F}_2^n,\ x \underset{\mathbb{F}_2}{\cdot} y = 0 \ \forall x \in C \right\}$$

où $x \underset{\mathbb{F}_2}{\cdot} y = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_2$.

$$= \frac{1}{2}\left(w(x+y) - w(x) - w(y) \right) \in \mathbb{F}_2$$

Prop 4.29 : $\tilde{H}$ est doublement pair.
Donc $\tilde{H} \subset \tilde{H}^\perp$

Or $\dim \tilde{H} = 4$

$\dim \tilde{H}^\perp = \text{longueur}(\tilde{H}) - \dim \tilde{H}$

$= 8 - 4 = 4.$

Donc $\tilde{H} = \tilde{H}^\perp$

Réseau Associé à un Code

$$\rho : \mathbb{Z}^n \longrightarrow \mathbb{F}_2^n$$
$$(x_1, \dots, x_n) \longmapsto (\overline{x_1}, \dots, \overline{x_n}).$$

<u>Déf</u>: Le réseau $\Gamma_C \subset \mathbb{R}^n$ associé au code $C \subset \mathbb{F}_2^n$ est

$$\Gamma_C = \frac{1}{\sqrt{2}} \rho^{-1}(C)$$

<u>cad</u> : $x = (x_1, \dots, x_n) \in \mathbb{R}^n$

$x \in \Gamma_C$ si $\begin{cases} \sqrt{2}.x \in \mathbb{Z}^n \\ \rho(\sqrt{2}.x) \in C \end{cases}$

<u>Question</u> II . 1 . <u>b)</u>

$f_i = \frac{1}{\sqrt{2}} \tilde{c}_i$ $\qquad$ $\tilde{c}_i \in \tilde{H} \subset \mathbb{F}_2^n$

vu comme élément de $\{0,1\}^n \subset \mathbb{Z}^n \subset \mathbb{R}^n$.

$\rho(\sqrt{2}\, f_i) = \tilde{c}_i \in \tilde{H}$. Donc $f_i \in \Gamma_{\tilde{H}}$.

<u>Question</u> II . 1 . <u>b)</u>

$$f_i = \frac{1}{\sqrt{2}} \tilde{c}_i \qquad \tilde{c}_i \in \tilde{H} \subset \mathbb{F}_2^n$$

vu comme élément de $\{0,1\}^n \subset \mathbb{Z}^n \subset \mathbb{R}^n$.

$\rho(\sqrt{2}\, f_i) = \tilde{c}_i \in \tilde{H}$. Donc $f_i \in \Gamma_{\tilde{H}}$.

<u>Question</u> II . 2 . <u>a)</u>

$$e_8 = \frac{1}{\sqrt{2}} (-1, 0, -1, -1, 0, 0, 1, 0)$$

$\rho(\sqrt{2}\, e_8) = (1, 0, 1, 1, 0, 0, 1, 0) \in \tilde{H}$.

Donc $e_8 \in \Gamma_{\tilde{H}}$.

<u>Remarque</u> :

$\tilde{H}$ est de dimension 4, $\tilde{H} \subset \mathbb{F}_2^n$.

$\Gamma_{\tilde{H}}$ est un réseau de $\mathbb{R}^8$

$$
\begin{aligned}
e(\sqrt{2}\, e_8) &= 10110010 = \tilde{c}_1 + \tilde{c}_6 \\
&= 00010111 \\
&+ 10100101 \\
&= e(\sqrt{2}\, g_1) + e(\sqrt{2}\, g_6) \text{ dans } \mathbb{F}_2^n.
\end{aligned}
$$

<u>Mais</u> e_8, g_1 et g_5 sont linéairement indépendants dans $\mathbb{R}^8$.

On pose $e_1 = f_1$; $e_2 = f_2 - f_1$; .. ; $e_7 = f_7 - f_6$.

Prop [$(e_1, \dots, e_8)$ est une base de $\Gamma_{\tilde{H}}$.

- $e_1, .., e_8 \in \Gamma_{\tilde{H}}$.

- $$\mathrm{Gram}(e_1, .., e_8) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & \boxed{-1} \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & \boxed{0} \\ 0 & 0 & 0 & 0 & \boxed{-1} & 0 & \boxed{0} & 2 \end{pmatrix} = G$$

$$\begin{cases} e_8 \cdot e_7 = 0 \\ e_8 \cdot e_5 = -1 \end{cases}$$

- $\det G = 1$.

Donc $(e_1, .., e_8)$ est libre.

Soit $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_8 \subset \Gamma_{\tilde{H}}$

$$[\Gamma_{\tilde{H}} : \Gamma] = \text{cardinal}\left(\Gamma / \Gamma_{\tilde{H}}\right)$$

$$= \frac{\det(\Gamma)}{\det(\Gamma_{\tilde{H}})} = \frac{1}{1}$$

(car $\tilde{H}$ auto-duale, donc $\Gamma_{\tilde{H}}$ unimodulaire et $\det(\Gamma_{\tilde{H}}) = 1$).

<u>D'où</u> $\Gamma_{\tilde{H}} = \Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_8$

$(e_1, \dots, e_8)$ Base de $\Gamma_{\tilde{H}}$

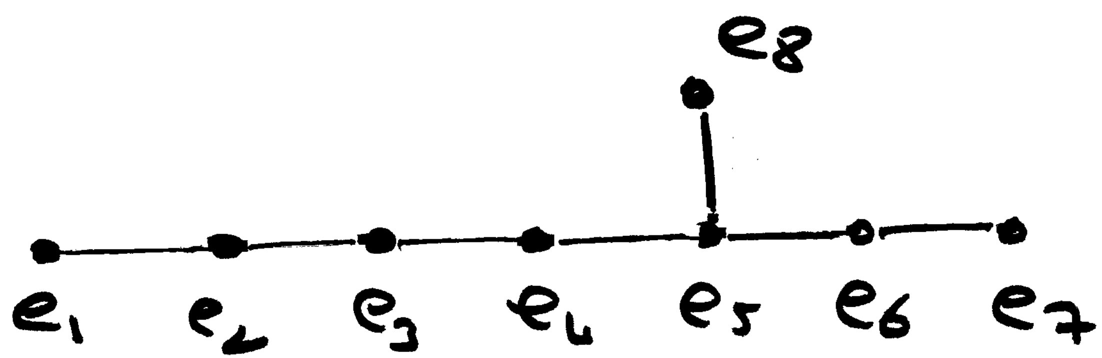
$$G = \begin{array}{cc} \left(\begin{array}{cccccccc} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{array}\right) & \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{array} \\ \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} & \end{array}$$

$\forall i \in \{1, \dots, 8\}$

$e_i \cdot e_i = 2$.

Donc $\Gamma_{\tilde{H}}$ est un réseau de racines.

<u>Diagramme de Dynkin</u> :



$\Gamma_{\tilde{H}}$ réseau de type E_8.

Γ réseau de racines

$R = \{x \in \Gamma,\ x \cdot x = 2\} = \{\text{Racines de } \Gamma\}$.

Thm 1 : Γ possède une base formée de racines $e_1, \dots, e_n$ telles que $e_i \cdot e_j \in \{0, -1\}$.

Γ réseau de racines

$R = \{x \in \Gamma,\ x \cdot x = 2\} = \{\text{Racines de } \Gamma\}$.

Thm 1 : Γ possède une base formée de racines $e_1, \dots, e_n$ telles que $e_i \cdot e_j \in \{0, -1\}$.

* Γ possède une base formée de racines car R engendre Γ.

* Soient $x, y \in R$

$(x \cdot y)^2 \leq (x \cdot x)(y \cdot y) = 4$.

Donc $(x \cdot y) \in \{0, 1, -1, 2, -2\}$.

* Cas d'égalité de Cauchy-Schwartz :

$x \cdot y = \pm 2 \iff x, y$ colinéaires

$\iff x = \pm y$

* $(x-y)\cdot(x-y) = x \cdot x + y \cdot y - 2\, x \cdot y$

$= 4 - 2\, x \cdot y .$

$x \cdot y = 1 \iff (x-y)\cdot(x-y) = 2$

$\iff (x-y) \in R .$

<u>Def</u> : $S \subset R$ est un Système Fondamental de Racines si

(i) S est une base de Γ

(ii) $\forall \beta \in R$, $\beta = \sum_{\alpha \in S} k_\alpha \alpha$ avec des coeff. k_α tous de même signe.

S est alors une base comme dans le théorème.

<u>Def</u> : $S \subset R$ est un système fondamentale de Racines si

(i) S est une base de Γ

(ii) $\forall \beta \in R$, $\beta = \sum_{\alpha \in S} k_\alpha \alpha$ avec des coeff. k_α tous de même signe.

S est alors une base comme dans le théorème.

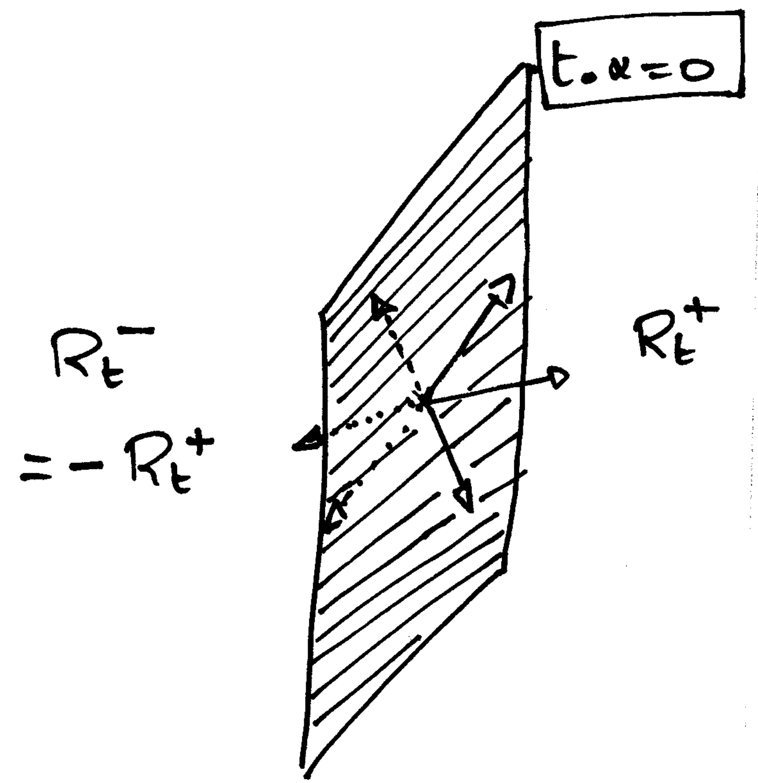
Soient $\alpha, \beta \in S$.

- α et β sont non colinéaires. Donc $\alpha \cdot \beta \neq \pm 2$
- Si $\alpha \cdot \beta = 1$, $\alpha - \beta$ est une racine, dont les coeff ne sont pas de même signe. Donc $\alpha \cdot \beta \neq 1$.

Donc $\alpha \cdot \beta \in \{0, -1\}$.

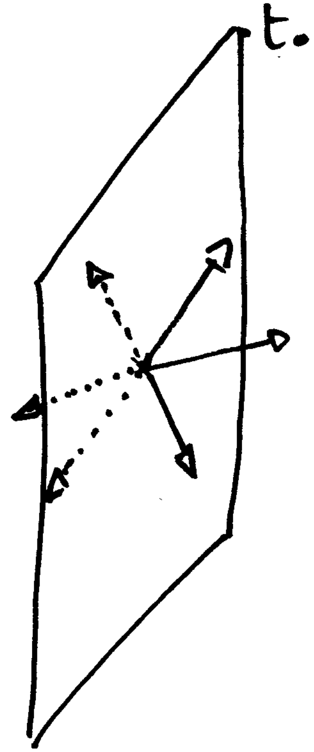
<u>Donc</u> on veut montrer qu'il existe un système de racines fondamentales $S \subset R$.

On peut en construire un de la façon suivante :



<u>Donc</u> on veut montrer qu'il existe un système de racines fondamentales $S \subset R$.

On peut en construire un de la façon suivante :

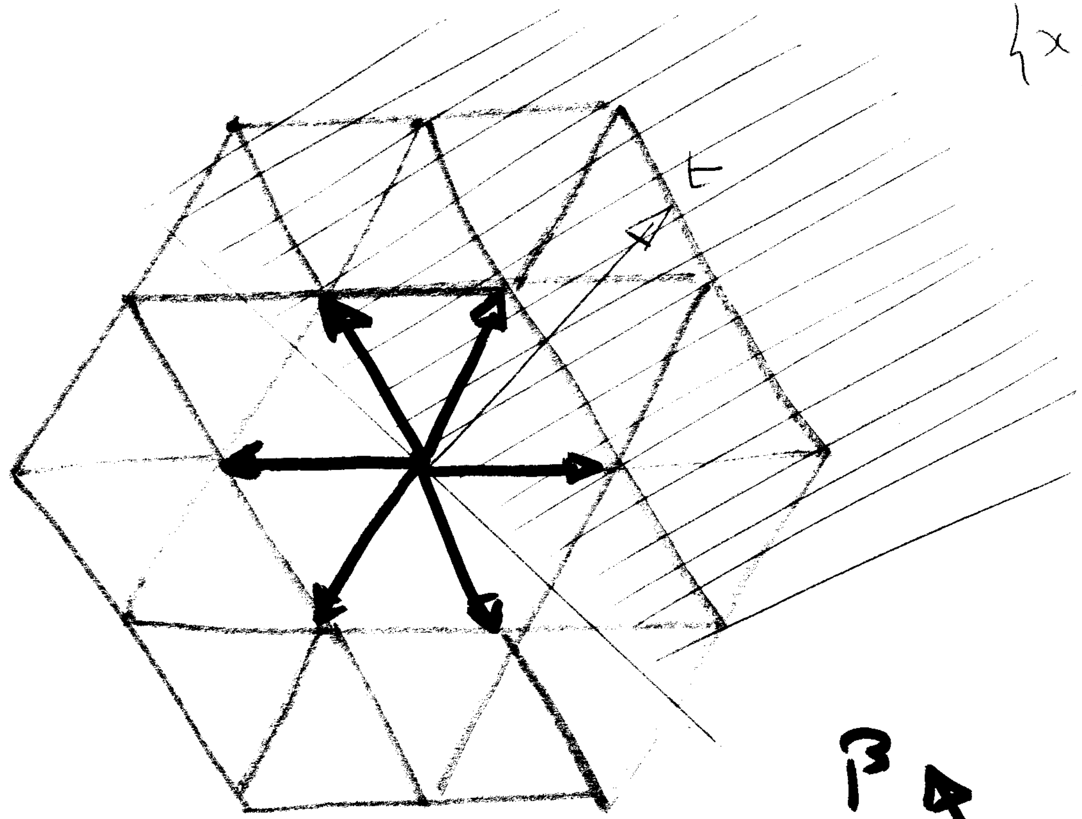


- $R = R_t^+ \cup (-R_t^+)$
  où $R_t^+ = \{\alpha \in R,\ t \cdot \alpha > 0\}$.
- $\alpha \in R_t^+$ est <u>décomposable</u> si il existe $\beta, \gamma \in R_t^+$, $\alpha = \beta + \gamma$
- $S_t = \{\alpha \in R_t^+,\ \alpha \text{ indécomposable}\}$

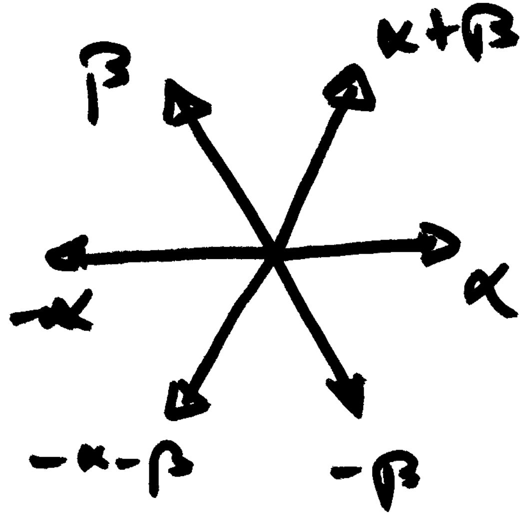
<u>Prop</u> : S_t est un système de Racines Fondamentales

Réseau Hexagonal

$\{x,\ x.t > 0\}$.



$$\left[\begin{array}{l} S_t = \{\alpha, \beta\} \\ R_t^+ = \{\alpha, \beta, \alpha+\beta\}. \end{array}\right.$$



Prop : S_t est un système de racines fondamentale

LR 1 : $R_t^+ \subset CL_+(S_t)$

$$\underset{\{ \sum_{\beta \in S_t} \lambda_\beta \beta \;,\; \lambda_\beta \geq 0 \}}{\overset{\shortparallel}{}}.$$

Supposons par l'absurde $R_t^+ \not\subset CL_+(S_t)$ et choisissons $\alpha \in R_t^+$, $\alpha \notin CL_+(S_t)$, tel que $t \cdot \alpha$ minimal.

* $\alpha \notin S_t$. Donc α est décomposable, $\alpha = \beta + \gamma$
* $t \cdot \alpha = \underbrace{t \cdot \beta}_{>0} + \underbrace{t \cdot \gamma}_{>0}$. Comme $t \cdot \alpha$ est minimal et $t \cdot \beta < t \cdot \alpha$, $t \cdot \gamma < t \cdot \alpha$, β et γ appartiennent à $CL_+(S_t)$.
* Mais alors $\alpha = \beta + \gamma \in CL_+(S_t)$.

contradiction.

<u>Corollaire</u> : * S_t vérifie la condition (ii)
* S_t est générateur.

On montre de même que S_t est une famille libre. Ceci prouve le Thm 1.

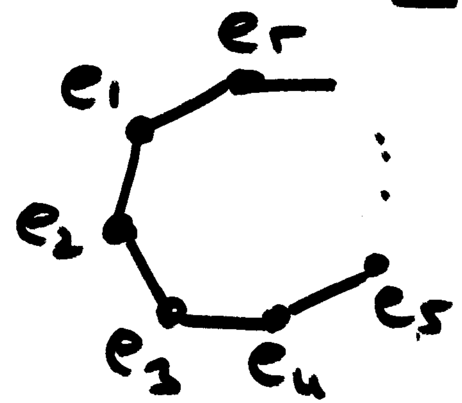
<u>Dorénavant</u> : | Γ est un réseau de racines
| S un syst. de racines fondamentales.

Diagramme de Dynkin associé Δ :

* Chaque $e_i \in S$ $\longleftrightarrow$ un sommet $\underset{e_i}{\bullet}$
* e_i et e_j sont liés $\iff e_i \cdot e_j = -1$.

$$\underset{e_i}{\bullet}\!\!-\!\!-\!\!-\!\!\underset{e_j}{\bullet}$$

<u>Lemme</u> : Δ ne contient pas de cycle.



cycle de longueur r.

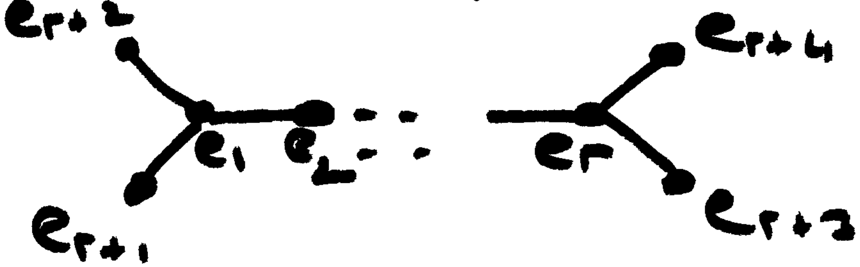
Si Δ contient un tel cycle,

$$(e_1 + \cdots + e_r)^2 = \sum_{i=1}^{r} e_i \cdot e_i + 2 \sum_{1 \leq i < j \leq r} e_i \cdot e_j$$

$$= 2r - 2r = 0$$

Donc $e_1 + \cdots + e_r = 0$. Impossible !
($(e_1, \ldots, e_n)$ base de $\mathbb{R}^n$).

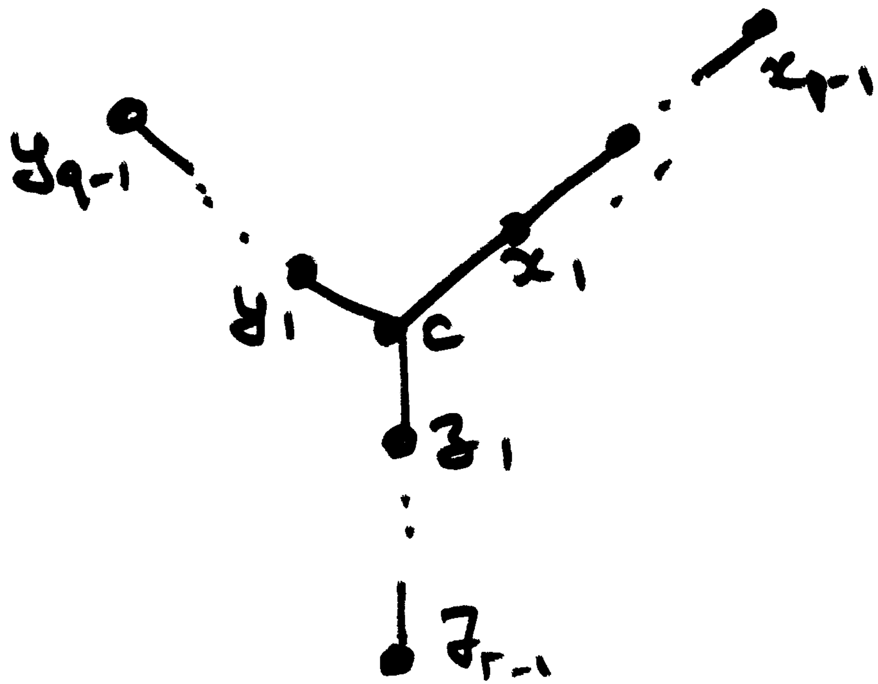
Lemme : Δ ne contient pas de sous-graphe de la forme



Preuve : Comme ci-dessus :

$$\| 2e_1 + \cdots + 2e_r + e_{r+1} + \cdots + e_{r+4} \|^2 = 0.$$

Donc Δ est de la forme :



$p \leq q \leq r$

Soit $\omega = c + \frac{1}{p}\left[(p-1)x_1 + (p-2)x_2 + \cdots + x_{p-1}\right]$

$$+ \frac{1}{q}\left[(q-1)y_1 + (q-2)y_2 + \cdots + y_{q-1}\right]$$

$$+ \frac{1}{r}\left[(r-1)z_1 + (r-2)z_2 + \cdots + z_{r-1}\right]$$

$$\omega^2 = \omega \cdot \omega = -1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 0.$$

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

Soit $\omega = c + \frac{1}{p}\left[(p-1)x_1 + (p-2)x_2 + \cdots + x_{p-1}\right]$
$+ \frac{1}{q}\left[(q-1)y_1 + (q-2)y_2 + \cdots + y_{q-1}\right]$
$+ \frac{1}{r}\left[(r-1)z_1 + (r-2)z_2 + \cdots + z_{r-1}\right]$

$$\omega^2 = \omega \cdot \omega = -1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 0.$$

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

* $p = 1$ $q \le r$ arbitraires.

$n = q + r$

* $p = 2$, $q = 2$, r arbitraire

* $p = 2$, $q = 3$ $\frac{1}{r} > 1 - \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$

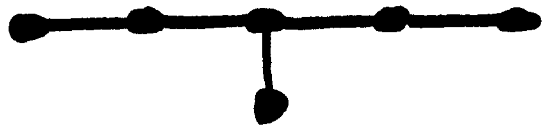
$r \in \{3, 4, 5\}$

E_6, E_7, E_8.

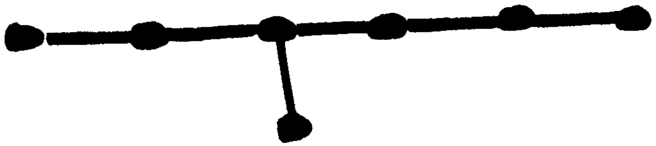
<u>Théorème 2</u> : Les diagrammes $\overbrace{\text{possibles}}^{\text{connexes}}$ sont :

A_n (n sommets)

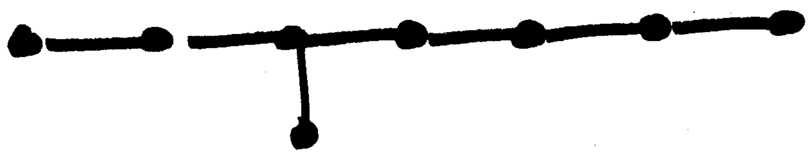
D_n (n sommets).



E_6



E_7

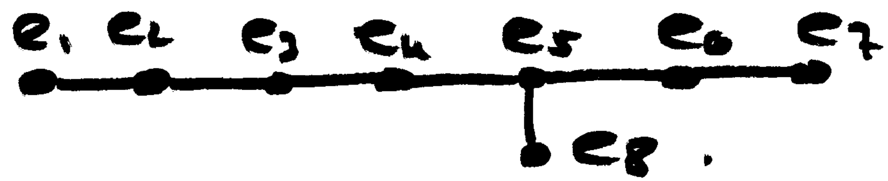


E_8

Et chaque diagramme correspond effectivement à un réseau.

<u>Exemple</u> : Construction d'un réseau de type E_7.

On part de $\Gamma_{\tilde{H}} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_8$



Posons $v = 2e_1 + 3e_2 + 4e_3 + 5e_4 + 6e_5 + 4e_6 + 2e_7 + 3e_8$.

$$v.e_1 = 2e_1.e_1 + 3e_2.e_1 = 4 - 3 = 1.$$

$$v.e_2 = 2e_1.e_2 + 3e_2.e_2 + 4e_3.e_2 = -2+6-4 = 0$$

$\vdots$

$$v.e_8 = 0.$$

Soit $x = x_1 e_1 + \cdots + x_8 e_8 \in \Gamma_{\tilde{H}}$

$$x \cdot v = x_1\, e_1 \cdot v + \cdots + x_8\, e_8 \cdot v = x_1 .$$

Donc $x \cdot v = 0 \iff x_1 = 0$.

<u>Ainsi</u>

$$\Gamma = \{ x \in \Gamma_{\tilde{H}} \, , \, x \cdot v = 0 \} \subset \underbrace{\{ x \in \mathbb{R}^8 , x \cdot v = 0 \}}_{\cong \mathbb{R}^7}$$

$$= \mathbb{Z} e_2 \oplus \cdots \oplus \mathbb{Z} e_7$$

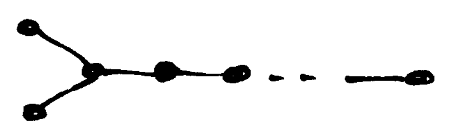
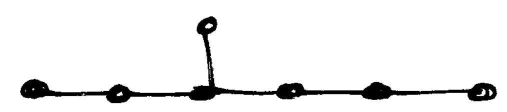
Réseau de type E_7.

<u>Prolongement</u> : Soit Γ un réseau de Racines Irréductible.

Il existe un code $C \subset \mathbb{F}_2^n$ tel que $\Gamma = \Gamma_C$

$\iff$ Γ est de type

A_1 D_n $n \geq 4$ pair E_7 ou E_8


Système de Racines:

$\Phi \subset \mathbb{R}^n$ tel que :

1. Φ engendre $\mathbb{R}^n$
2. $\forall \alpha \in \Phi$, α et $-\alpha$ sont les seuls multiples de α dans Φ
3. $\forall \alpha \in \Phi$, Φ est stable par la réflexion par rapport à l'hyperplan orthogonal à α.
4. Le projeté orthogonal de $\beta \in \Phi$ sur $\mathbb{R}\alpha$ appartient à $\mathbb{Z} \cdot \frac{\alpha}{2}$

Si Γ est un rêseau de racine, $R \subset \Gamma$ est un système de racine.

Il existe des systèmes de racines dont les vecteurs ne sont pas tous de longueur 2.

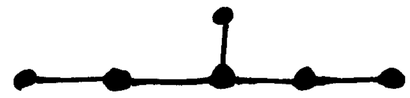
Les systèmes de racines irréductibles sont classifiés :

A_n 

B_n 

C_n 

D_n 

E_6 

E_7 

E_8 

F_4 

G_2