13 Algèbre géométrique

(voir [Dieudonné], [Garrett])

- $GL(n)$ (étude géométrique).
- Formes bilinéaires et hermitiennes, groupes classiques.
- Théorème de Witt et l'extension d'isométries

On va étudier en détail les notions de l'algèbre géométrique.

Concernant la notation matricielle pour une matrice rectangulaire $A = (a_{ij})$ soit ${}^tA$ la transposée de A. Si les entrées de A se trouvent dans un anneau D muni d'involution σ, soit A^σ donnée par $(A^\sigma)_{ij} = a_{ij}^\sigma$.

13.1 Étude géométrique du groupe $GL(n)$ et de ses sous-groupes

Le groupe $GL(n)$ est le groupe classique le plus facilement étudié, mais il indique déjà les phénomènes les plus intéressants pour l'utilisation dans beaucoup d'autres situations. Le groupe général linéaire $GL(n,k)$ est le groupe de toutes les matrices inversibles de la taille $n \times n$ avec les entrés dans un corps commutatif k. Le groupe spécial linéaire $SL(n,k)$ est le groupe de toutes les matrices (inversibles) de la taille $n \times n$ avec les entrées dans un corps commutatif k, et de déterminant 1.

Pour une approche moins dépendante de coordonnées, on fixe un k-espace vectoriel V de dimension n et soit $GL_k(V)$ le groupe de tous les automorphismes k-lineaires de V. Tout choix d'une base de V sur k-basis donne un isomorphisme $GL_k(V) \to GL(n,k)$ en utilisant la matrice de l'application linéaire par rapport aux bases choisies. Soit $e_1, \cdots, e_n$ la base standard pour k^n

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \cdots \\ 0 \end{pmatrix}, \cdots, e_n = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 1 \end{pmatrix}.$$

Par ce choix de bases ordonnées on obtient un isomorphisme $GL_k(k^n) \to GL(n,k)$.

Un *drapeau* $\mathcal{F}$ dans V est une chaîne

$$\mathcal{F} = (V_{d_1} \subset V_{d_2} \subset \cdots \subset V_{d_m})$$

de sous-espaces, où V_{d_i} est de dimension d_i, et

$$d_1 < \cdots < d_m.$$

On dit que le type de ce drapeau est $(d_1, \cdots, d_m)$. Dans k^n le drapeau standard de type $(d_1, \cdots, d_m)$ est le drapeau de type $(d_1, \cdots, d_m)$ avec

$$V_{d_i} = ke_1 + \cdots + ke_{d_{i-1}} + ke_{d_i}.$$

On définit le *sous-groupe parabolique* $P_{\mathcal{F}}$ associé au drapeau $\mathcal{F}$ par :

$$P = \{g \in GL_k(V) : \forall i, gV_{d_i} = V_{d_i}\}$$

Si $V = k^n$ et $\mathcal{F}$ le *drapeau standard* de type $(d_1, \cdots, d_m)$, le sous-groupe parabolique $P_{\mathcal{F}}$ est formé par tous les éléments admettant un développement en blocs :

$$\begin{pmatrix} d_1 \times d_1 & & & * \\ & (d_2 - d_1) \times (d_2 - d_1) & & \\ & & \ddots & \\ 0 & & & (n - d_m) \times (n - d_m) \end{pmatrix}$$

où le $i^{\text{ème}}$ entrée diagonale est (comme indiqué) de type $(d_i - d_{i-1}) \times (d_i - d_{i-1})$, les entrées inférieures sont 0, les entrées supérieures sont arbitraires. Tout $g \in P = P_{\mathcal{F}}$ induit une application naturelle sur les quotients $V_{d_i}/V_{d_{i-1}}$, où on définit $V_{d_0} = 0$ et $V_{d_{m+1}} = V$). Alors le *radical unipotent* $R_u P$ est

$$R_u P = \{p \in P_{\mathcal{F}} : p = id \text{ sur tous } V_{d_i}/V_{d_{i-1}} \text{ et sur } V/V_{d_m}\}.$$

Le radical unipotent $R_u P$ est un sous groupe distingué de P. Dans le cas du sous-groupe parabolique standard P de type $(d_1, \cdots, d_m)$ sur k^n le radical unipotent est formé par les éléments de la forme

$$\begin{pmatrix} 1_{d_1} & * & \cdots & & \\ & 1_{d_2 - d_1} & * & \cdots & \\ & & \ddots & * & \cdots \\ & & & \ddots & * \\ 0 & & & & 1_{n-d_m} \end{pmatrix}$$

où 1_d désigne la matrice identité de type $d \times d$. Choisissons les sous-espaces V'_{n-d_i} de V de telle façon que V'_{n-d_i} est un sous-espace complémentaire de V_{d_i} dans V et tel que

$$V'_{n-d_m} \subset \cdots \subset V'_{n-d_1}$$

est un drapeau de type opposé au drapeau de V_{d_i}. On pose

$$P' = \{g \in GL_k(V) : \forall i, g V'_{n-d_i} = V'_{n-d_i}\}$$

$$M = P \cap P'$$

Alors M est dit une composante de Levi complementaire de P, et $P = P_{\mathcal{F}}$ est le produit semi-direct standard

$$P = M \ltimes R_u P$$

de M et $R_u P$, où M normalise $R_u P$. Pour le sous-groupe standard parabolique P dans $GL(n, k)$ de type $(d_1, \cdots, d_m)$ le choix standard du sous-espace complementaire est

$$V'_{n-d_i} = k e_{d_i+1} + \cdots + k e_n$$

Alors la composante de Levi standard est le groupe des matrices de la forme

$$\begin{pmatrix} d_1 \times d_1 & & & & \\ & d_2 - d_1 \times d_2 - d_1 & & & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & n - d_m \times n - d_m \end{pmatrix}$$

où le $i^{\text{ème}}$ élément diagonale est de type $(d_i - d_{i-1}) \times (d_i - d_{i-1})$, $i = 1, \ldots, m+1$, et tous les autres blocs sont nuls. Dans le cas du groupe $GL_k(V)$ la composante de Levi d'un sous-groupe minimal parabolique est dite un torus maximal (k-)déployé.

Le résultat suivant est un prototype du résultat analogue pour les classes plus larges de groupes.

PROPOSITION 13.1.1
a) Tous les sous-groupes paraboliques de type donné sont conjugués dans $GL_k(V)$
b) Toutes les composantes de Levi dans un sous-groupe parabolique P sont conjugués par éléments de P
c) Tous les tores maximaux k-déployés sont conjugués dans $GL_k(V)$

Pour montrer que tous les sous-groupes paraboliques de type donné sont conjugués, il suffit de voir que pour tout choix de deux drapeaux

$$V_{d_1} \subset V_{d_2} \subset \cdots \subset V_{d_m}$$
$$V'_{d_1} \subset V'_{d_2} \subset \cdots \subset V'_{d_m}$$

de même type il existe un $g \in GL_k(V)$ tel que $gV_{d_i} = V'_{d_i}$ pour tous i. On choisit deux bases $\{v_i\}$, $\{v'_i\}$ de V, de telle façon que

$$V_{d_i} = kv_1 + \cdots + kv_{d_i},$$
$$V'_{d_i} = kv'_1 + \cdots + kv'_{d_i}.$$

Alors on définit g par $gv_i = v'_i$. Ceci prouve que tous les sous-groupes paraboliques de type donné sont conjugués.

Pour démontrer que toutes les composantes de Levi dans un sous-groupe parabolique P sont conjugués par des éléments de P soit

$$V_{d_1} \subset \cdots \subset V_{d_m}$$

le drapeau pour lequel P est le stabilisateur, et soient $V^1_{n-d_i}, V^2_{n-d_i}$, (avec $1 \leq i \leq m$) deux choix de familles de sous-espaces complémentaires qui définissent les composantes de Levi correspondantes. Il suffit de trouver $p \in P$ de telle façon que $pV^1_{n-d_i} = V^2_{n-d_i}$ (pour tous les indices i).

Pour $\ell = 1, 2$, on définit $W^\ell_1, \ldots, W^\ell_{m+1}$ comme, respectivement,

$$V_{d_1}, V_{d_2} \cap V^\ell_{n-d_1}, V_{d_3} \cap V^\ell_{n-d_2}, \cdots, V_{d_m} \cap V^\ell_{n-d_{m-1}}, V^\ell_{n-d_m}.$$

Pour $\ell = 1, 2$ nous avons $V = \oplus W^\ell_i$. Par l'hypothèse, $\dim_k W^\ell_1 = \dim_k W^\ell_2$ pour tous j. Alors, il existe une infinité d'éléments $g \in GL_k(V)$ tels que $gW^1_j = W^2_j$ pour tous j. Pour chaque tel g, certainment $g \in P$, et puisque V^ℓ_j est une somme de W^ℓ_j, on a assurément $pV^1_{n-d_i} = V^2_{n-d_i}$ pour un $p \in P$ et pour ~~pour~~ tout i.

Soient T_1, T_2 deux tores maximaux k-déployés, on choisit des sous-groupes paraboliques minimaux P_i contenant T_i. Par la première partie de la proposition, il existe

$h \in GL_k(V)$ tel que $hP_1h^{-1} = P_2$. Alors hT_1h^{-1} est une autre composante de Levi (un torus maximal déployé) à l'intérieur de P_2, donc par la seconde assertion de la proposition il existe $p \in P_2$ tel que $p(hP_1h^{-1})p^{-1} = T_2$. Ceci donne la troisième assertion de la proposition. ∎

Maintenant on va généraliser le précédant directement en remplaçant le corps commutatif k par un corps gauche (un anneau de division) D. On reprend la version sans coordonnées de la discussion précédente ; les illustrations matricielles resterons les mêmes.

On définit un espace vectoriel V de dimension finie sur un corps gauche (anneau de division) D (c'est-à-dire, V est un module de génération finie sur D). La notion de dimension a un sens, étant définie comme le rang d'un module libre. Les résultats élémentaires sur l'indépendance linéaire et sur les bases sont les mêmes que sur les corps commutatifs.

La perte de la commutativité de D devient importante lorsque l'on considère les endomorphismes D-linéaires. Si D n'est pas commutatif, alors l'anneau $\mathrm{End}_D(V)$ de tous les endomorphismes D-linéaires de V ne contient pas D d'une façon naturelle. Alors, un choix de D-bases pour un espace vectoriel D de dimension $n$donne un isomorphisme

$$\mathrm{End}_D(V) \to \{n \times n \text{ matrices à coefficients dans } D^{opp}\}$$

où D^{opp} est l'anneau opposé à D. Ceci dit, D^{opp} est le même groupe additif D, mais avec la multiplication $*$, donnée par

$$x * y = yx$$

où yx est la multiplication dans D. (Parfois on peut éviter cette complication (innocente) en décrivant V comme étant un D-module "droit", mais de toute façon la définition d'un module "droit" est réellement celle d'un module sur l'anneau opposé D^{opp}.) Le groupe général linéaire $GL(n, D)$ sur D est le groupe de toutes les matrices inversibles de $n \times n$ à coefficients dans D. Une version sans coordonnées du groupe général linéaire est $GL_D(V)$, le groupe de tous les automorphismes D-linéaires de V. Un choix de D-bases pour V donne un isomorphisme

$$GL_D(V) \to GL(n, D^{opp})$$

Les définitions concernant les drapeaux et les sous-groupes paraboliques sont identiques à celles du cas où D est commutatif. Un drapeau $\mathcal{F}$ dans V est une chaîne

$$\mathcal{F} = (V_{d_1} \subset V_{d_2} \subset \cdots \subset V_{d_m})$$

de sous-espace , où V_i est de dimension i et

$$d_1 < \cdots < d_m.$$

Le type d'un drapeau est la suite $(d_1, \cdots, d_m)$.

Un sous-groupe parabolique $P = P_{\mathcal{F}}$ in $GL_D(V)$ est le stabilisateur d'un drapeau

$$\mathcal{F} = (V_{d_1} \subset V_{d_2} \subset \cdots \subset V_{d_m})$$

C'est-à-dire,

$$P_{\mathcal{F}} = \{g \in GL_D(V) : \forall i, gV_{d_i} = V_{d_i}\}$$

Tout $g \in P = P_{\mathcal{F}}$ induit une application naturelle sur les quotients $V_{d_i}/V_{d_{i-1}}$ (où on définit $V_{d_0} = 0$ et $V_{d_{m+1}} = V$). Le radical unipotent $R_u P$ est

$$R_u P = \{p \in P_{\mathcal{F}} : p = id \text{ sur } V_{d_i}/V_{d_{i-1}}\}$$

Le *radical unipotent* $R_u P$ est un sous-groupe distingué de P. En choisissant les sous-espaces V'_{n-d_i} de V de telle façon que V'_{n-d_i} est un sous-espace complémentaire de V_{d_i} dans V. Alors

$$V'_{n-d_i} \subset \cdots \subset V'_{n-d_1}$$

est un drapeau de type opposé de celui de V_{d_i}.

On pose

$$P' = \{g \in GL_D(V) : \forall i, gV'_{n-d_i} = V'_{n-d_i}\}$$

$$M = P \cap P'$$

Alors M est appelée une *composante de Levi* ou *un complémentaire de Levi* dans P, et $P = P_{\mathcal{F}}$ est le produit semi-direct

$$P = M \ltimes R_u P$$

de M et de $R_u P$, où M normalise $R_u P$.

PROPOSITION 13.1.2 *a) Tous les sous-groupes paraboliques de type donné sont conjugués dans* $GL_D(V)$

b) Toutes les composantes de Levi dans un sous-groupe parabolique P *sont conjugués par éléments de* P

Cours N 10 Lundi 30 mars 2015

13.2 Formes bilinéaires et formes hermitiennes, groupes classiques.

Dans cette section, on considère les groupes classiques définis comme des isométries ou des similitudes de « formes » sur les espaces vectoriels. On définit premièrement les groupes orthogonaux et les groupes symplectiques. Cette famille de descriptions peut être simplifiée, au prix d'une obscuration des membres les plus simples.

13.2.1 Formes bilinéaires, formes symétriques

Soit k un corps de caractéristique différente de 2 et soit V un k-espace vectoriel de dimension finie. Une forme (k-)*bilinéaire* sur V est une fonction à valeurs dans k sur $V \times V$ donc pour tous $x, y \in k$ et $v, v_1, v_2 \in V$

$$\begin{aligned}\langle v_1 + v_2, v\rangle &= \langle v_1, v\rangle + \langle v_2, v\rangle\\ \langle v, v_1 + v_2\rangle &= \langle v, v_1\rangle + \langle v, v_2\rangle\\ \langle xv, yv_1\rangle &= xy\langle v, v_1\rangle.\end{aligned}$$

Si on a toujours

$$\langle v_1, v_2\rangle = \langle v_2, v_1\rangle,$$

alors la forme bilinéaire est dite symétrique. La fonction

$$Q[v] = \langle v, v\rangle$$

est dite la forme quadratique associée, à partir de laquelle $\langle\cdot,\cdot\rangle$ peut être récupérée par

$$4\langle v_1, v_2\rangle = Q[v_1 + v_2] - Q[v_1 - v_2]$$

Le groupe orthogonal associé est le groupe d'isométries de Q (ou de $\langle\cdot,\cdot\rangle$), étant défini comme

$$O(Q) = O(\langle\cdot,\cdot\rangle) = \{g \in GL_k(V) : \forall v_1, v_2 \in V,\ \langle gv_1, gv_2\rangle = \langle v_1, v_2\rangle\}$$

Le groupe de similitudes associé est défini comme

$$\begin{aligned}GO(Q) = GO(\langle\cdot,\cdot\rangle) =&\{g \in GL_k(V) :\ \exists \nu(g) \in k^\times \text{ tel que}\\ &\forall v_1, v_2 \in V, \langle gv_1, gv_2\rangle = \nu(g)\langle v_1, v_2\rangle\}.\end{aligned}$$

Si on a pour tout
$\langle v_1, v_2\rangle = -\langle v_2, v_1\rangle$ pour tout $v_1, v_2 \in V$, alors la forme bilinéaire
$f : V \times V \to k$, $f(v_1, v_2) = \langle v_1, v_2\rangle$ est dite alternée ou symplectique.

Le groupe symplectique associé à f est le groupe d'isométrie de la forme $f = \langle,\rangle$ défini comme

$$Sp(f) = \{g \in GL_k(V) : \forall v_1, v_2 \in V,\ \langle gv_1, gv_2\rangle = \langle v_1, v_2\rangle\}$$

Le groupe de similitudes associé est défini comme

$$\begin{aligned}GSp(f) = \{&g \in GL_k(V) : \exists \nu(g) \in k^\times\\ &\text{tel que } \forall v_1, v_2 \in V,\ \langle gv_1, gv_2\rangle = \nu(g)\langle v_1, v_2\rangle\}\end{aligned}$$

13.2.2 Formes sesquilinéaires, formes hermitiens

Soit K un corps, une extension quadratique de k, son sous-corps trivial par l'action d'un automorphisme k-linéaire σ.

DÉFINITION 13.2.1
a) Une forme k-bilinéaire $f : V \times V \to K$, $f(v_1, v_2) = \langle v_1, v_2 \rangle$ sur un K-espace vectoriel de dimension finie V est dite sesquilinéaire *(avec une référence implicite à σ) si*

$$\langle xv_1, yv_2 \rangle = xy^\sigma \langle v_1, v_2 \rangle$$

(pour tous $x, y \in K$ et pour tous $v_1, v_2 \in V$).
b) Une forme sesquilinéaire $f = \langle , \rangle$ sur un K-espace vectoriel de dimension finie V est dite hermitienne, *si pour tous $v_1, v_2 \in V$ on a*

$$\langle v_2, v_1 \rangle = \langle v_1, v_2 \rangle^\sigma$$

Le groupe unitaire associé est le groupe d'isométries de $\langle , \rangle$, étant défini comme

$$U(f) = \{g \in GL_K(V) : \langle gv_1, gv_2 \rangle = \langle v_1, v_2 \rangle, \ \forall v_1, v_2 \in V\}$$

Le groupe de similitudes associé est défini comme

$$GU(f) = \{g \in GL_K(V) : \exists \nu(g) \in k^\times \text{ tel que } \forall v_1, v_2 \in V, \ \langle gv_1, gv_2 \rangle = \nu(g)\langle v_1, v_2 \rangle\}.$$

On peut traîter les groupes précédents simultanement, en incluant aussi des groupes plus généraux de la façon suivante : soit D est une algèbre de division avec une (anti-)involution σ. Notons que, $D \to D$ est telle que les propriétés

$$(\alpha)^{\sigma\sigma} = \alpha \text{ et } (\alpha + \beta)^\sigma = \alpha^\sigma + \beta^\sigma \text{ et } (\alpha\beta)^\sigma = \beta^\sigma \alpha^\sigma$$

pour tous $\alpha, \beta \in D$. Soit Z le centre de D. On suppose que D soit de dimension finie sur Z, et que

$$k = \{x \in Z \mid x^\sigma = x\}.$$

Soit V un D-espace vectoriel de dimension finie, et fixons $\varepsilon = \pm 1$. Soit

$$f = \langle \cdot, \cdot \rangle, f : V \times V \to D$$

une forme k-bilinéaire à valeurs dans D sur V de telle façon que

$$\langle v_2, v_1 \rangle = \varepsilon \langle v_1, v_2 \rangle^\sigma$$
$$\langle \alpha v_1, \beta v_2 \rangle = \alpha^\sigma \langle v_1, v_2 \rangle \beta$$

pour tous $\alpha, \beta \in D$ et $v_1, v_2 \in V$.

Une telle forme est dite ε-hermitienne sur V. On appelle un tel espace V (muni de $\langle , \rangle$) un (D, σ, ε)-espace.

13.2.3 Groupes d'isométries généraux

Soit V_i deux (D,σ,ε)-espaces muni de formes $f_i = \langle , \rangle_i$ pour $(i = 1, 2)$. Une application D-linéaire $\varphi : V_1 \to V_2$ est une isométrie si, pour tous $u, v \in V_1$,

$$\langle \varphi u, \varphi v\rangle_2 = \langle u, v\rangle_1$$

L'applicaton φ est une similitude s'il existe $\nu \in k^\times$ tel que, pour tous $u, v \in V_1$,

$$\langle \varphi u, \varphi v\rangle_2 = \nu\langle u, v\rangle_1$$

Écrivons $\varphi : V_1 \cong V_2$ si φ est une isométrie.

DÉFINITION 13.2.2
a) Le groupe d'isométries *associé à* $f = \langle , \rangle$ *sur* $V = V_1 = V_2$ *est défini comme*

$$U(f) = \{g \in GL_D(V) : \forall v_1, v_2 \in V, \langle gv_1, gv_2\rangle = \langle v_1, v_2\rangle, \ \}.$$

b) Le groupe de similitudes *associé est défini comme*

$$GU(f) = \{g \in GL_D(V) : \exists \nu(g) \in k^\times \text{ tel que } \forall v_1, v_2 \in V, \ \langle gv_1, gv_2\rangle = \nu(g)\langle v_1, v_2\rangle\}.$$

13.2.4 Orthogonalisation, vecteurs isotropes*

Un D-sous-espace U dans un (D,σ,ε)-espace V possède un complémentaire orthogonal

$$U^\perp = \{u' \in V \ \ \langle u', u\rangle = 0, \forall u \in U\}$$

Noter que $U \cap U^\perp = 0$ n'est pas assuré en général. Le noyau de tout l'espace V est noté par $V^\perp$. La forme est dite non dégénérée si $V^\perp = 0$. Souvent on va supposer (sans référence à la forme) que simplement l'espace V est non dégénéré.

Si V_1, V_2 sont deux (D,σ,ε)-espaces avec les formes, respectivement, $\langle , \rangle_1, \langle , \rangle_2$, alors la somme directe $V_1 \oplus V_2$ de D-espaces vectoriels est un (D,σ,ε)-espace muni de la forme

$$\langle v_1 + v_2, v_1' + v_2'\rangle = \langle v_1, v_1'\rangle_1 \langle v_2, v_2'\rangle_2$$

On l'apppelle la somme orthogonale. En général, deux sous-espaces V_1, V_2 d'un (D,σ,ε)-espace sont orthogonaux si

$$V_1 \subset V_2^\perp,$$

ou, de façon équivalente, si $V_2 \subset V_1^\perp$.

Si $\langle v, v\rangle = 0$ pour $v \in V$, alors v est un vecteur isotrope. Si$\langle v, v'\rangle = 0$ pour tout $v, v' \in U$ pour un sous-espace U de V alors U est un sous-espace (totalement) isotrope. S'il n'existe pas de vecteur isotrope non nul dans U, alors on dit que U est anisotrope.

PROPOSITION 13.2.3 *Soit V un (D,σ,ε)-espace non-dégénéré avec un sous-espace U. Alors U est non-dégénéré si et seulement si $V = U \oplus U^\perp$, et si et seulement si $U^\perp$ est non-dégénéré*

Preuve. On utilise l'application $\Lambda : V \to \mathrm{Hom}_D(U, D)$ donnée par $v \to \lambda_v$ où

$$\lambda_v(u) = \langle u, v \rangle.$$

Il découle de la non-dégénéréscance de V que Λ est surjective. Le noyau est donc $U^\perp$ Alors, par l'algèbre linéaire on a

$$\dim_D U^\perp + \dim_{D^{opp}} \Lambda(U) = \dim_D V$$

Donc, comme la dimension de $\Lambda(V)$ est la même que la dimension de U, par décompte de dimensions, on a $U \cap U^\perp = 0$ si et seulement si $U + U^\perp$ est une somme directe (et donc une somme orthogonale). Puisque $U \subset U^{\perp\perp}$, le fait que U est dégénéré implique que $U \cap U^\perp$ est non nul. Alors $U^\perp \cap U^{\perp\perp}$ est non nul puisqu'il contient $U \cap U^\perp$ donc $U^\perp$ est dégénéré. De l'autre coté, U est non-dégénéré implique que $U + U^\perp$ est une somme directe, donc $\dim U = \dim V - \dim U^\perp$.

Puisque $\dim U^{\perp\perp} = \dim V - \dim U^\perp$ on déduit de la non-dégénéréscance de V, que $U^{\perp\perp} = U$, donc $U^{\perp\perp} + U^\perp$ est une somme directe, et $U^\perp$ est non-dégénéré. ∎

Une D-base $e_1, \ldots, e_n$ pour un (D, σ, ε)-espace V est dite orthogonale si $\langle e_i, e_j \rangle$ pour $i \neq j$.

PROPOSITION 13.2.4 *Soit V un (D, σ, ε)-espace. Supposons que le cas où $\varepsilon = -1$, $D = k$, et σ et trivial est exclu. Si le produit $\langle , \rangle$ n'est pas identiquement nul, alors il existe $v \in V$ avec $\langle v, v \rangle \neq 0$. Si V est non-dégénéré, alors il possède une base orthogonale.*

Preuve. Supposons que $\langle v, v \rangle = 0$ pour tous $v \in V$. Alors

$$0 = \langle x + y, x + y \rangle = \langle x, x \rangle + \langle x, y \rangle + \varepsilon \langle x, y \rangle^\sigma + \langle y, y \rangle = \langle x, y \rangle + \varepsilon \langle x, y \rangle^\sigma$$

Si $\varepsilon = 1$ et le produit $\langle , \rangle$ n'est pas identiquement nul, il existe x, y tels que $\langle x, y \rangle = 1$.

Alors on a

$$0 = \langle x, y \rangle + \varepsilon \langle x, y \rangle^\sigma = 1 + 1,$$

Contradiction. Supposons que $\varepsilon = -1$ et σ n'est pas triviale sur D. Alors il existe $\alpha \in D$ tel que $\alpha^\sigma \neq \alpha$, et avec $\omega = \alpha - \alpha^\sigma$, $\omega^\sigma = -\omega$. Si $\langle , \rangle$ n'est pas identiquement nul alors il existe x, y tels que $\langle x, y \rangle = 1$. Alors on a

$$0 = \langle \omega x, y \rangle + \varepsilon \langle \omega x, y \rangle^\sigma = \omega^\sigma \langle x, y \rangle - \langle x, y \rangle^\sigma \omega =$$
$$-\omega + \varepsilon\omega = -2\omega,$$

Contradiction.

Pour construire une base orthogonale, on utilise la récurrence par dimension. Si la dimension d'un espace non-dégénéré V est 1, alors tout vecteur non nul forme une base orthogonale. En général, par la discussion précédente, on peut trouver $v \in V$ de telle façon que $\langle v, v \rangle \neq 0$. Alors $Dv^\perp$ est non–dégénéré et V est une somme directe orthogonale de Dv et de $Dv^\perp$, par la proposition précédente. ∎

Supposons que V est de dimension deux, avec une base ordonnée x, y de telle façon que

$$\langle x, x \rangle = \langle y, y \rangle = 0 \text{ et } \langle x, y \rangle = 1$$

Alors V est un plan hyperbolique et x, y est un paire hyperbolique dans V. Un (D, σ, ε)-espace est hyperbolique, s'il est une somme orthogonale de plans hyperboliques.

PROPOSITION 13.2.5 *Soit V et W deux espaces hyperboliques de même dimension (avec les même données (D, σ, ε). Alors il existe une isométrie $f : V \to W$. Ceci dit, la dimension est un seul invariant d'un espace hyperbolique.*

Preuve : Comparer les paires hyperboliques. ∎

PROPOSITION 13.2.6 *On considère un espace V non-dégénéré avec $\varepsilon = -1, D = k$, et soit σ trivial. Alors V est* hyperbolique, *ceci dit, V est une somme orthogonale de plans hyperboliques.*

Preuve. Puisque σ est triviale, $\alpha\beta = \beta\alpha$ pour tous $\alpha, \beta \in D$, alors D est un corps. Puisque

$$\langle x, x\rangle = -\langle x, x\rangle$$

et la caractéristique est différente de 2, tout vecteur est isotrope. Fixons $x \in V$ non-nul, et considérons $y \in V$ tels que $\langle x, y\rangle \neq 0$. Alors, quitte à remplacer y par un élément de D on peut supposer $\langle x, y\rangle = 1$, c'est-à-dire, un paire hyperbolique. Alors $Dx + Dy$ et $(Dx + Dy)^{\perp}$ sont non-dégénérés, et on fait la récurrence sur la dimension. ∎

PROPOSITION 13.2.7 *Soit V est un espace non-dégénéré, et soit $-V$ le même espace muni de la forme opposée sur V. Alors la somme orthogonale*

$$W = V \oplus -V$$

est hyperbolique.

Preuve. Dans le cas d'espaces alternés non-dégénérés (avec $D = k, \varepsilon = 1, \sigma$ triviale), l'espace V lui-même est déjà hyperbolique, donc $-V$ l'est. De l'autre coté, pour un espace non-alterné non-dégénéré V, on peut choisir une base orthogonale $\{e_i\}$ (pour les deux V et $-V$. Alors on affirme que dans $V \oplus -V$ les sous-espaces

$$H_i = De_i \oplus De_i$$

sont des plans hyperboliques, pour tous les indices i. (Ceci donnerait la preuve de la proposition). Puisque la caractéristique est différente de 2, on peut considérer les vecteurs

$$x_i = \frac{1}{2}e_i \oplus e_i, y_i = \langle e_i, e_i\rangle^{-1}e_i \oplus -e_i$$

qui sont linéairement independents (puisque $1 \neq -1$). Ils constitutent deux isotropes par construction. Puis, les constantes sont telles que pour la forme $\langle , \rangle$ sur $V \oplus -V$ on a $\langle x_i, y_i\rangle = 1$. ∎

PROPOSITION 13.2.8 *Soit V un espace non-dégénéré, et soit W un sous-espace. Soit W_0 le noyau de W. Alors il existe un sous-espace non-dégénéré W_1 of W tel que $W_0 + W_1 = W$ est une somme directe. De plus,pour toute base $x_1, \cdots, x_n$ de W_0, et pour tout tel W_1 il existe une partie $\{y_i\} \subset W_1^{\perp}$, telle que les sous-espaces $Dx_i + Dy_i$ sont des plans hyperboliques mutuellement orthogonaux. En particulier,*

$$W + \sum_i Dy_i = W \bigoplus \oplus_i Dy_i$$

est non-dégénéré et $W_0 + \sum_i Dy_i$ est un espace hyperbolique.

COROLLAIRE 13.2.9 *Soit V un espace non-dégénéré. Alors il existe un sous-espace hyperbolique H de V et un sous-espace anisotrope A de V tel que V est la somme directe orthogonale $V = H \oplus A$.*

13.2.5 Classification d'espaces orthogonaux et hermitiens.

On rapelle d'abord une classification d'espaces orthogonaux et hermitiens à isométrie près ((voir [Lang], Ch.XIV, §7 , §11).

On donnera une classification plus fine d'espaces quadratiques et une généralisation de la loi d'inértie et de la notion de la signature (voir §1 du Chapitre IV de [Se70] et §3 de Partie II de [KosMan]).

13.2.6 Formes symétriques sur les corps ordonnés

THÉORÈME 13.2.10 (LOI D'INERTIE DE SYLVESTER*) *Soit k un corps ordonné, et E un k-espace vectoriel muni d'une forme symetrique non-gégénérée. Alors il existe un entier $r \geq 0$ tel que pour toute base orthogonale $\{v_1, \cdots, v_n\}$ de E, il y a exactement r éléments $\langle v_i, v_i \rangle$ strictement positifs, et exactement $n - r$ éléments $\langle v_i, v_i \rangle$ strictement négatifs.*

Preuve. On pose $a_i = \langle v_i, v_i \rangle$ et $b_i = \langle w_i, w_i \rangle$ pour toute autre base orthogonale. On raisonne par l'absurde. Si $b_i = \langle w_i, w_i \rangle$ sont strictement positifs pour exactement s éléments avec $i = 1, 2, \cdots, s$, il suffit de montrer que

$$v_1, \cdots, v_r, w_{s+1}, \cdots, w_n$$

sont linéairement indépendents, alors $r + n - s \leq n$, donc $r \leq s$ et $r = s$ par symétrie. Si

$$u = x_1 v_1 + \cdots + x_r v_r = -y_{s+1} w_{s+1} - \cdots - y_n w_n,$$

$$\langle u, u \rangle = x_1^2 \langle v_1, v_1 \rangle + \cdots + x_r^2 \langle v_r, v_r \rangle = y_{s+1}^2 \langle w_{s+1}, w_{s+1} \rangle + \cdots + y_n^2 \langle w_n, w_n \rangle,$$

d'où la contradiction : on a $\langle u, u \rangle > 0$ et $\langle u, u \rangle < 0$ au même temps. ∎

DÉFINITION 13.2.11

a) La signature *de g est le couple $(r_+, r_-) = (r, rk(g) - r)$ qui défini le nombre $\sigma(g) = r_+ - r_-$. Pour toute forme hyperbolique h, $\sigma(h) = 0$ et $\sigma(g \oplus h) = \sigma(g)$.*

b) Une forme positive définie *est de signature $(r_+, r_-) = (n, 0)$.*

COROLLAIRE 13.2.12 (CRITÈRE DE SYLVESTER) *Soit k un corps ordonné, et E un k-espace vectoriel muni d'une forme symetrique non-gégénérée g. Alors g est positive définie si et seulement si tous les mineurs principaux Δ_i sont strictement positifs.* ∎

James Joseph Sylvester (3 septembre, 1814, Londre - 15 mars, 1897 Oxford)

13.2.7 Cas des formes hermitiennes

Soit k_0 un corps ordonné, et soit $K = k_0(\alpha)$, où $\alpha^2 < 0$, et on pose $\alpha^\sigma = -\alpha$. On considère un K-espace vectoriel hermitien E muni d'une forme hermitienne $(x, y) \mapsto \langle x, y\rangle$, donc $\langle y, x\rangle = \langle x, y\rangle^\sigma$. On observe que $\langle x, x\rangle \in k_0$ pour tout $x \in E$.

THÉORÈME 13.2.13 (LOI D'INERTIE HERMITIENNE) *Soit E un K-espace vectoriel muni d'une forme hermitienne g. Il existe une base orthogonale de E.*

Si g est non-gégénérée, il existe un entier $r \geq 0$ tel que pour toute base orthogonale $\{v_1, \cdots, v_n\}$ de E, il y a exactement r éléments $\langle v_i, v_i\rangle$ strictement positifs, et exactement $n - r$ éléments $\langle v_i, v_i\rangle$ strictement négatifs.

Preuve. On pose $a_i = \langle v_i, v_i\rangle$ et $b_i = \langle w_i, w_i\rangle$ pour toute autre base orthogonale. On raisonne par l'absurde. ∎

La signature de g est le couple $(r_+, r_-) = (r, rk(g) - r)$ et on pose $\sigma(g) = r_+ - r_-$. Pour toute forme hyperbolique h, $\sigma(h) = 0$ et $\sigma(g \oplus h) = \sigma(g)$.

Identité de polarisation :

$$\langle u + \alpha v, u + \alpha v\rangle = \langle u, u\rangle - \alpha\langle u, v\rangle^\sigma + \alpha\langle u, v\rangle + \alpha\alpha^\sigma\langle v, v\rangle$$
$$\langle u - \alpha v, u - \alpha v\rangle = \langle u, u\rangle + \alpha\langle u, v\rangle^\sigma - \alpha\langle u, v\rangle + \alpha\alpha^\sigma\langle v, v\rangle$$
$$\alpha\langle u + v, u + v\rangle = \alpha\langle u, u\rangle + \alpha\langle u, v\rangle^\sigma + \alpha\langle u, v\rangle + \alpha\langle v, v\rangle$$
$$\alpha\langle u - v, u - v\rangle = \alpha\langle u, u\rangle - \alpha\langle u, v\rangle^\sigma - \alpha\langle u, v\rangle + \alpha\langle v, v\rangle, \text{ d'où}$$
$$\langle u, v\rangle = \frac{1}{4\alpha}[\langle u + \alpha v, u + \alpha v\rangle - \langle u - \alpha v, u - \alpha v\rangle + \alpha\langle u + v, u + v\rangle - \alpha\langle u - v, u - v\rangle]$$

13.2.8 Formes matricielle d'isométries*

Groupes $O(r_+, r_-)$ et $U(r_+, r_-)$.

13.2.9 Groupes symplectiques en coordonnées*

RAPPEL : Soit V un K-espace vectoriel de dimension finie sur un corps K de caractéristique différente de deux (par exemple, de caractéristique 0). Une forme K-bilinéaire

$$f : V \times V \to K$$

est dite *alternée* si pour tout $u \in V$, on a $f(u, u) = 0$.

(a) Montrer que pour tout corps K de caractéristique différernte de 2 cette condition est équivalente à l'identité : pour tout $u, v \in V$

$$f(u, v) = -f(v, u).$$

(b) On appelle une forme bilinéaire f *symplectique* si elle est antisymétrique et non-dégénérée, c'est-à-dire

$$\forall u \in V\backslash\{0\}, \exists u' \in V, f(u, u') \neq 0.$$

Montrer que l'application $\varphi : V \to V^*$, $\varphi(u)(v) = f(u, v)$ est un isomorphisme de K-espaces vectoriels.

(c) On considère le sous-espace $W \subset V$ engendré par u et u', et soit

$$V' = \{v \in V \mid \forall w \in W, f(v,w) = 0\}.$$

Montrer qu'il y a une décomposition $V = W \oplus V'$.

(d) En déduire que la dimension de V sur K est paire.

(f) En déduire qu'il existe une base $\{e_i\}$ de V telle que la matrice $A_f = (a_{i,j})$ de la forme f dans cette base est

$$J_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \\ -1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & \cdots & -1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

(f) Pour toute forme hermitienne positive H sur un espace vectoriel complexe V on pose

$$f(z,w) = \text{Im } H(z,w).$$

Montrer que la forme f est symplectique (sur $\mathbb{R}$).

Déscription matricielle du groupe symplectique $G_n = \text{Sp}(V)$, à l'aide des matrices blocs :

(a) On considère l'ensemble

$$\text{Sp}(V) = \{g \in GL(V) \mid \forall u, v \in V, f(g(u), g(v)) = f(u,v)\}.$$

Montrer que $\text{Sp}(V)$ est un groupe dit symplectique (un sous-groupe de $\text{GL}(V)$).

(b) En utilisant une base de I d), montrer qu'il existe un isomorphisme

$$\text{Sp}(V) \xrightarrow{\sim} \text{Sp}_n(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_{2n}(K) \;\middle|\; a,b,c,d \in \text{Mat}_n(K), {}^t ac = {}^t ca, {}^t ad - {}^t cb = I_n \right\}$$

Soit $A = (a_{ij}) \in GL_{2n}(K)$ une matrice *antisymétrique inversible*, c'est-à-dire, $a_{ii} = 0$, ${}^t A = -A$, et $\det(A) \neq 0$. Pour toute base $\{e_i \mid i = 1, \cdots, 2n\}$, on a alors une forme symplectique f dont la matrice coincide avec A. Montrer qu'il existe une matrice inversible $C \in GL_{2n}(K)$, telle que ${}^t CAC = J_n \in GL_{2n}(K)$. En déduire que $\det A = (\det C)^{-2}$ est un carré dans le groupe miltiplicatif K^*.

(c) *Le pffafian.* Tout d'abord, soient t_{ij} $(1 \leq i < j \leq 2n)$ $n(2n-1)$ variables indépendantes, et soit $K = \mathbb{Q}(t) = \mathbb{Q}(t_{ij})$ le corps des fractions des variables t_{ij} $(1 \leq i < j \leq n)$. On considère la matrice $T = (t_{ij})$, où on pose $t_{ii} = 0$ pour $i = 1, 2, \cdots, 2n$, et $t_{ji} = -t_{ij}$ pour $1 \leq i < j \leq n$. Alors la matrice T est *antisymétrique inversible* sur K, donc d'après I(b), il existe une matrice inversible $C \in GL_{2n}(K)$, telle que ${}^t CTC = J_n \in GL_{2n}(K)$, et le polynôme $\det T = (\det C)^{-2}$ coincide donc avec le carré d'une *fraction rationnelle* dans K.

Montrer qu'il existe un polynôme $\mathrm{Pf}(T) \in \mathbb{Z}[t] = \mathbb{Z}[t_{ij}]$ dit le *pffafian générique* de T, tel que $\det(T) = \mathrm{Pf}(T)^2$.

(d) Montrer que si $n = 1$, $\mathrm{Pf}(T) = t_{12}$, et si $n = 2$,

$$\mathrm{Pf}(T) = t_{12}t_{34} - t_{13}t_{24} + t_{14}t_{23}.$$

(voir [Dieudonné], [Lang], [KosMan]).

(e) Pour tout anneau commutatif R et pour toute matrice antisymétrique $A \in GL_{2n}(R)$ on considère l'homomorphisme

$$\varphi \ : \mathbb{Z}[t] \to R,\ t_{ij} \mapsto a_{ij},$$

et on pose $\mathrm{Pf}(A) = \varphi(\mathrm{Pf}(T))$. Montrer qu'on a $\det(A) = \mathrm{Pf}(A)^2$.

(f) Montrer que pour toute matrice $C \in \mathrm{Mat}_{2n}(R)$ on a

$$\mathrm{Pf}({}^tCAC) = \det(C)\mathrm{Pf}(A).$$

Solution. On déduit tout d'abord une formule générique : soient u_{ij} $(1 \leq i, j \leq 2n)$ $4n^2$ variables algébriquement indépendantes sur $\mathbb{Q}$, et telles que t_{ij} et u_{ij} sont $4n^2+n(2n-1)$ variables algébriquement indépendantes sur $\mathbb{Q}$. On pose $U = (u_{ij}) \in \mathrm{Mat}_{2n}(K')$, où $K' = \mathbb{Q}(t_{ij}, u_{ij})$ est le corps des fractions des variables t_{ij} $(1 \leq i < j \leq 2n)$ et u_{ij} $(1 \leq i, j \leq 2n)$.

On déduit de I(e) que

$$\mathrm{Pf}({}^tUTU)^2 = \det(U)^2\mathrm{Pf}(T)^2 \Rightarrow \mathrm{Pf}({}^tUTU) = \pm\det(U)\mathrm{Pf}(T)$$

Ensuite, on substitue $U = I_{2n}$ et $T = J_n$, ceci implique immédiatement que le signe ci-dessus est $+$.

Enfin, pour tout anneau commutatif R, pour toute matrice antisymétrique $A \in GL_{2n}(R)$ et pour toute matrice carrée $C \in \mathrm{Mat}_{2n}(R)$ on considère l'homomorphisme

$$\psi \ : \mathbb{Z}[t, u] \to R,\ t_{ij} \mapsto a_{ij}, u_{ij} \mapsto c_{ij},$$

et on déduit

$$\mathrm{Pf}({}^tCAC) = \det(C)\mathrm{Pf}(A).$$

(g) En déduire que pour toute matrice symplectique $G = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_n(K)$ on a $\det(G) = 1$.

13.3 Théorème de Witt et l'extension d'isométries

Ici, on donne un résultat traditionnel sur les extensions d' isométries dans les espaces non-dégénérés munis de la forme ci-dessus.

Ce résultat implique dans un cas spécial, que tous les sous-groupes paraboliques « de même type » dans les groupes d'isométries (et dans les groupes de similitudes) sont conjugués. On exclut le cas de la caractéristique 2, et on utilise les même notations que ci-dessus. Pour un (D, σ, ε)-espace V muni de forme $\langle , \rangle$, soit $-V$ note le (D, σ, ε)-espace qui est le même D-espace vectoriel mais muni de forme $-\langle , \rangle$. Soit V_0 désigne le noyau d'un (D, σ, ε)-espace V.

THÉORÈME 13.3.1 (WITT)

Soient U, W deux sous-espaces d'un espace non-dégénéré V. Toute isométrie $\phi : U \to W$ admet une extension à une isométrie $\Phi : V \to V$. (Ceci dit, la restriction de Φ sur U est ϕ).

Si U, V, W sont espaces tels que $U \oplus V \cong U \oplus W$, alors $V \cong W$.

Pour simplicité, on va traîter uniquement le cas symetrique (des formes quadratiques en caractéristique $\neq 2$).

13.3.1 Théorème de Witt, [Se70]

Soient (V, Q) et (V', Q') deux modules quadratiques *non-dégénérés* ; soit U un sous-espace vectoriel de V, et soit $s : U \to V'$ un morphisme injectif de U dans V'. On cherche à prolonger s à un sous-espace plus grand que U, et si possible à V tout entier. On commence par le cas où U est dégénéré :

LEMME 13.3.2 *Si U est dégénéré, on peut prolonger s en un morphisme métrique injectif $s_1 : U_1 \to V'$, où U_1 contient U comme hyperplan.*

Soit x un élément non nul de $\mathrm{rad}(U)$. Comme x est isotrope, la proposition 12.11.9 montre qu'il existe un plan hyperbolique de V qui le contient ; on peut donc trouver $y \in V$ tel que $\langle x, y\rangle = 1$ et $\langle y, y\rangle = 0$. Puisque y n'est pas orthogonal à x, on a $y \notin U$, et le sous-espace $U_1 = U \oplus ky$ contient U comme hyperplan. On construit de même un élément $y' \in V'$ tel que $\langle s(x), y'\rangle = 1$ et $\langle y', y'\rangle = 0$. On pose $s_1(y) = y'$. ∎

THÉORÈME 13.3.3 *Si (V, Q) et (V', Q') sont deux modules quadratiques isomorphes et non-dégénérés, tout morphisme injectif*

$$s : U \to V'$$

d'un sous-espace vectoriel U de V peut être prolongé en un isomorphisme de V sur V'.

PREUVE. Puisque V et V' sont isomorphes,on peut supposer $V = V'$. D'autre part, en appliquant le lemme ci-dessus, on voit que l'on peut se borner au cas où U est non-dégénéré. On raisonne par récurrence sur $\dim U$.

Si $\dim U = 1$, U est engendré par un élément non isotrope. Si $y = s(x)$, on a $\langle y, y\rangle = \langle x, x\rangle$. On peut choisir $\varepsilon = \pm 1$ tel que $x + \varepsilon y$ ne soit pas isotrope ; sinon, en effet, on aurait

$$2\langle x, x\rangle + 2\langle x, y\rangle = 2\langle x, x\rangle - 2\langle x, y\rangle = 0,$$

ce qui entraînerait $\langle x, x\rangle = 0$. Choisissons un tel ε et soit H l'hyperplan orthogonal à $z = x + \varepsilon y$; on a $V = kz \hat{\oplus} H$. Soit σ la symétrie par rapport à H, i.e. un automorphisme de V qui est identique sur H et qui change z en $-z$. Comme $x - \varepsilon y$ appartient à H, on a

$$\sigma(x - \varepsilon y) = x - \varepsilon y, \quad \text{et } \sigma(x + \varepsilon y) = -x - \varepsilon y,$$

d'où $\sigma(x) = -\varepsilon y$. L'automorphisme $-\varepsilon\sigma$ prolonge donc s.

Si $\dim U > 1$, on décompose U sous la forme $U_1 \hat{\oplus} U_2$ avec $U_1, U_2 \neq 0$.

D'après l'hypothèse de récurrence la restriction s_1 de s à U_1 se prolonge en un automorphisme σ_1 de V ; quitte à remplaçer s par $\sigma_1^{-1} \circ s$, on peut donc supposer que s est identité sur U_1. Le morphisme s applique alors U_2 dans l'orthogonal V_1 de U_1 ; d'après l'hypothèse de récurrence, la restriction de s sur U_2 se propolge donc en un automorphisme σ_2 de V_1 ; l'automorphisme σ de V qui est identité sur U_1 , et σ_2 sur V_1 repond alors à la question. ∎

COROLLAIRE 13.3.4 ("LOI DE SIMPLIFICATION") *Deux sous-espaces isomorphes d'un module quadratique non-dégénéré ont des orthogonaux isomorphes*

On prolonge un isomorphisme entre les deux sous-espaces en un automorphisme du module, et on restreint ce dernier aux orthogonaux.

En particulier, si U, V, W sont espaces tels que $U \oplus V \cong U \oplus W$, alors $V \cong W$.

COROLLAIRE 13.3.5 (CLASSIFICATION D'ESPACES ORTHOGONAUX) *Tout module quadratique L admet une décomposition orthogonale*

$$L = L_0 \oplus L_h \oplus L_a$$

où L_0 est isotrope, L_h hyperbolique et L_a anisotrope. Pour toutes deux telles décompositions il existe une isométrie $f : L \to L$, respectant cette décompositions.

En effet, $L_0 = \mathrm{rad} L$, et $L = L_0 \hat{\oplus} L_1$. Si L_a n'est pas anisotrope, on considère dans L_1 un espace maximal isotrope U qui existe par le lemme de Zorn. Complétons ce sous-espace à un espace hyperbolique $L_h \subset L_1$ de dimension double, et soit $L_a = L_h^{\perp}$ dans L_1. Alors L_a n'a pas des vecteurs isotropes (par la maximalité de U).

Unicité : pour deux décompositions

$$L = L_0 \oplus L_h \oplus L_a = L_0 \oplus L'_h \oplus L'_a$$

il existe une isométrie $f : L_0 \oplus L_h \to L_0 \oplus L'_h$, et on la complète par le théorème de Witt. ∎

Ce corollaire est une généralisation de la loi d'inertie, reduisant la classification d'espaces orthogonaux à celle d'espaces anisotropes.

13.3.2 Groupe de Witt*

(voir [Lang], [KosMan], [Mi-Hu]). On considère l'ensemble $W(k)$ des classes d'espaces orthogonaux anisotropes sur un corps k (à isométrie près).

On considère l'opération d'addition sur $W(k)$: pour deux espaces orthogonaux anisotropes L_1 et L_2, de classes $[L_1], [L_2] \in W(k)$ on définit $[L_1] + [L_2]$ comme la partie anisotrope de $L_1 \hat{\oplus} L_2$ (bien définie par le corollaire 13.3.1).

THÉORÈME 13.3.6

a) L'ensemble $W(k)$ muni d'addition est un groupe abélien

b) Soit L_α l'espace de dimension 1 muni du produit scalaire $\langle x, y \rangle = \alpha xy$. Alors la classe $[L_\alpha]$ ne dépend que de la classe de $\alpha (k^*)^2$, est les $[L_\alpha]$ engendrent $W(k)$. ∎

13.3.3 Exemples : $W(\mathbb{F}_q)$, $W(\mathbb{R})$, $W(\mathbb{Q})$

(voir Ch.4 de [Mi-Hu]).

THÉORÈME 13.3.7 (SANS DÉMONSTRATION)

a) Le groupe $W(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z}, & \text{si } q \equiv 1 \bmod 4 \\ \text{non-cyclique d'ordre 4}, & \text{si } q \equiv 3 \bmod 4 \end{cases}$

b) Le groupe $W(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z}$ *par l'application de la signature* $\sigma(Q) = r_+ - r_-$ *;*

c) Il existe une suite exacte

$$0 \to \mathbb{Z} \to W(\mathbb{Q}) \ \to \bigoplus_p W(\mathbb{F}_p) \to 0.$$

Si $P^\sigma = P$, on a $\left(\frac{P}{Q}\right)^\sigma Q^\sigma = \frac{P}{Q}Q$, donc $P = 0$ ou $Q^\sigma = Q$, puisque $k(X_1, \ldots, X_n)$ est intègre.

Si P et Q ont un facteur commun, quitte à diviser par se facteur, on se ramène au cas où ils n'ont pas de facteur commun non trivial.

Si Q n'est pas symétrique, comme les transpositions engendrent $\mathfrak{S}_n$, il existe une transposition τ telle que $Q^\tau \neq Q$.

Si $\tau = (i, j)$, avec $1 \leqslant i < j \leqslant n$, considérons $P^\tau - P$ (ou $Q^\tau - Q$) comme un polynôme en X_j, à coefficients dans l'anneau $k[X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n]$. on a $(P^\tau - P)(X_j) \equiv (P^\tau - P)(X_i) \pmod{X_i - X_j}$, or $P^\tau(X_i) = P(X_i)$, donc $X_i - X_j$ divise $P^\tau - P$ (et $Q^\tau - Q$, pour la même raison).

Comme $\left(\frac{P}{Q}\right)^\tau = \frac{P}{Q}$, on a $P^\tau Q = PQ^\tau$, donc $(P^\tau - P)Q = (Q^\tau - Q)P$. En particulier, P divise $(P^\tau - P)Q$ dans l'anneau factoriel $k[X_1, \ldots, X_n]$. Comme P et Q n'ont aucun facteur commun, on trouve que P divise $(P^\tau - P)$.

Le degré en X_m de $\frac{P^\tau - P}{P}$ est inférieur ou égal à 0, pour tout m, donc $\lambda = \frac{P^\tau - P}{P} \in k$.

On a alors $P^\tau - P = \lambda P$ et $Q^\tau - Q = \lambda Q$. Comme $Q \neq Q^\tau$, on a aussi $\lambda \in k^*$.

Comme $X_i - X_j$ divise $(P^\tau - P)$ et $(Q^\tau - Q)$, c'est un facteur commun à P et Q, d'où une contradiction.

Donc Q est symétrique, et donc P l'est aussi d'après la deuxième question.

A.5 Contrôle continu du mardi 14 mars 2006

1. Soient p un nombre premier, et $\mathbb{F}_{p^{10}}$ un corps de p^{10} éléments.

(a) Trouver tous les sous corps $F \subset \mathbb{F}_{p^{10}}$.

(b) Montrer que le groupe $\mathrm{Aut}(\mathbb{F}_{p^{10}})$ de tous les automorphismes de $\mathbb{F}_{p^{10}}$ est cyclique, et trouver tous ses générateurs.

(c) Trouver le nombre de tous les polynômes unitaires irréductibles de degré 10 sur $\mathbb{F}_{p^{10}}$.

2. a) Trouver le terme constant du polynôme minimal P sur $\mathbb{Q}$ du nombre algébrique $\alpha = \sqrt{2} + \sqrt[3]{3}$.

b) Trouver toutes les racines complexes de P.

c) Déterminer le groupe de Galois du corps engendré par toutes les racines complexes de P.

3.* On considère une extension galoisienne L/K de groupe de Galois $\mathrm{Gal}(L/K)$, isomorphe au groupe symétrique S_5.

a) Déterminer toutes les sous-extensions galoisiennes E/K, où $K \subset E \subset L$.

b) Donner un exemple de deux sous-extensions E_1/K et E_2/K, ($E_1 \subset L$, $E_2 \subset L$) telles que E_1 et E_2 ne sont pas incluses l'une dans l'autre, le composé $E_1 \cdot E_2$ n'est pas égal à L, et l'intersection $E_1 \cap E_2$ n'est pas égale à K.

2006

4.* On considère le polynôme à coefficients rationnels

$$P(T) = T^3 - 3T - 1.$$

(a) Trouver le discriminant de P.

(b) Montrer que P est irréductible sur $\mathbb{Q}$ et qu'il possède trois racines réelles α_1, α_2, α_3, telles que $\alpha_3 < \alpha_2 < 0 < \alpha_1$.

(c) Montrer que si α est racine P, il en est de même de $2 - \alpha^2$. On pose $K = \mathbb{Q}(\alpha_1)$.

(d) Montrer que l'extension $K/\mathbb{Q}$ est galoisienne, et que tout élément de son groupe de Galois induit une permutation paire sur l'ensemble $\{\alpha_1, \alpha_2, \alpha_3\}$.

Références

Ouvrages de base :

[Bosch] Siegfried Bosch, *Algebra*, 3rd Ed., 1999

[Bourbaki] Bourbaki N. *Algèbre, Chap.8 . "Modules et anneaux semi-simples"*, Masson, Paris 1981.

[Dieudonné] Jean Alexandre Dieudonné, *La géométrie des groupes classiques*, Springer, 1963.

[Godement] Roger Godement, *Cours d'algèbre.*, Hermann, Paris, 1969

[Lang] Serge Lang , *Algebra.* Reading, Mass. : Addison–Wesley, 3rd Ed., 1993.

[Se70] Jean– Pierre Serre, *Cours d'arithmétique.* Paris, Press Univ. France, 1970.

[VdW71] B.L. van der Waerden, *Algebra I,II*, New York : Springer Verlag, 1971, 1967.

Lectures complémentaires :

[AMcD] I. G. MacDonald et M. F.Atiyah, *Introduction to Commutative Algebra.* Reading, MA : Addison-Wesley, 1969.

[Bigard] Alain Bigard, Géométrie, Cours et exercices corrigés pour le Capes et l'agrégation, Masson, 1998

[BS85] Z.I. Borevich, I.R.Shafarevich, *Number Theory.* Traduction anglaise. : New York/London : Academic Press, 1966.

[ChL] Antoine Chambert-Loir *Algèbre commutative*, `http ://www.polytechnique.fr/ chambert/ teach/algcom.pdf`

[Coq02] Robert Coquereaux, *Espaces fibrés et connexions. Une introduction aux géométries classiques et quantiques de la physique théorique.* Centre de Physique Théorique, Luminy - Marseille, `http ://www.cpt.univ-mrs.fr/~coque/book/sourceforhtml.html`

[Garrett] Paul Garrett's Page `http ://www.math.umn.edu/~garrett/m/buildings/`

2006

[Jac] N. Jacobson, *Basic Algebra I and II*, New York, NY : W.H. Freeman, 1974, 1989. Second Edition.

[Kob87] Neal Koblitz, *A course of number theory and cryptography*, Graduate texts in mathematics 114, New York : Springer Verlag, 1987.

[Kos82] A.I. Kostrikin, *Introduction to Algebra New York*, NY : Springer-Verlag, 1982

[KosMan] A.I. Kostrikin, Yu. I. Manin, *Linear algebra and geometry*, Nauka, Moscow 1986 ; English translation, Gordon and Breach, New York-London 1989

[Li-Ni] Rudolf Lidl et Harald Niederreiter, *Introduction to finite fields and their applications.* Addison–Wesley : Reading, 1983

[Ma-Pa] Yu.I. Manin et A.A.Panchishkin, *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p.

[Mi-Hu] J. Milnor et D.Hüsemoller, *Symmetric bilinear forms*, Springer-Verlag, 1973

[Sha87] I.R. Shafarevich, (1987) : Fundamental notions of algebra. Itogi Nauki, 11, 1987. English transl. : Encycl. Math. Sci 11. Berlin–Heidelberg–New York : Springer–Verlag, 1990.

[Weyl] Hermann Weyl, The Classical Groups : Their Invariants and Representations

[Tits] Jacques Tits, *Le Monstre (d'après R. Griess, B. Fischer et al.)* dans Séminaire Bourbaki, Vol. 1983/84. Astérisque no 121-122, (1985), 105–122.

[Wei74] A.Weil (1974) : Basic Number Theory. 3rd ed. Berlin–Heidelberg–New York : Springer–Verlag, 1974.

[W] Wikipédia, *Wikipédia, l'encyclopédie libre*
`http ://fr.wikipedia.org/wiki)`

[Stein] William Stein, *An Explicit Approach to Number Theory* (à paraître, voir page internet : `http ://modular.fas.harvard.edu/edu/Fall2001/124/lectures`).