

# SÉMINAIRE N. BOURBAKI

MICHEL DEMAZURE

## Structure du groupe orthogonal

*Séminaire N. Bourbaki*, 1960, exp. n° 169, p. 7-17

[http://www.numdam.org/item?id=SB\\_1958-1960\\_\\_5\\_\\_7\\_0](http://www.numdam.org/item?id=SB_1958-1960__5__7_0)

© Association des collaborateurs de Nicolas Bourbaki, 1960, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

STRUCTURE DU GROUPE ORTHOGONAL

par Michel DEMAZURE

(d'après T. TAMAGAWA [9])

1. Rappels et préliminaires.

a. Soit  $V$  vectoriel de dimension finie  $n$  sur  $k$  commutatif de caractéristique  $p$  quelconque. Une forme quadratique sur  $V$  est une application  $Q : V \rightarrow k$  telle que :

i.  $Q(ax) = a^2 Q(x)$  pour tous  $a \in k$ ,  $x \in V$ .

ii.  $(x, y) \rightarrow Q(x + y) - Q(x) - Q(y)$  est une forme bilinéaire sur  $V \times V$ .

Notant cette forme par  $(x, y) \rightarrow B(x, y)$ , on a les deux formules suivantes :

$$Q(x + y) = Q(x) + Q(y) + B(x, y) \quad (\text{formule du binôme})$$

et

$$B(x, x) = 2 Q(x) \quad (\text{en particulier } B(x, x) = 0, \text{ si } p = 2).$$

On dira que  $Q$  est dégénérée si  $B$  l'est. Si  $U$  est un sous-espace de  $V$ , on notera  $U'$  l'orthogonal de  $U$  :  $U' = \{x' \mid B(x, x') = 0 \text{ pour tout } x \in U\}$  ; et  $Q_U$  la restriction de  $Q$  à  $U$ . On dira que  $U$  est isotrope (resp. totale-ment singulier) si  $Q_U$  est dégénérée, i.e. si  $U \cap U' \neq 0$  (resp. si  $Q_U$  est identiquement nulle). On dira que  $x \in V$  est singulier si  $Q(x) = 0$ . Cf. [3]. Le sous-espace engendré par  $x_1, x_2, \dots, x_n$  sera noté  $\langle x_1, x_2, \dots, x_n \rangle$ .

b. Si  $Q$  (resp.  $Q'$ ) est une forme quadratique sur  $V$  (resp.  $V'$ ) vectoriel sur  $k$ , on appelle isométrie de  $V$  dans (resp. sur)  $V'$  une application  $k$ -linéaire injective (resp. bijective)  $\rho : V \rightarrow V'$  telle que  $Q'(\rho(x)) = Q(x)$  pour tout  $x$  de  $V$ .

On a alors le théorème de Witt ([1], théorème 3.9). Si  $V$  et  $V'$  sont non-isotropes et isométriques, toute isométrie d'un sous-espace de  $V$  dans  $V'$  se prolonge en une isométrie de  $V$  sur  $V'$ .

c. Si  $U$  est un sous-espace non-isotrope de  $V$  (en particulier si  $U = V$  et si  $Q$  est non dégénérée) on note  $O(U)$  le groupe orthogonal de  $Q_U$ , groupe des

isométries de  $U$  muni de  $Q_U$  sur lui-même. Le groupe des commutateurs de  $O(U)$  sera noté  $\Omega(U)$  et le groupe projectif associé  $P\Omega(U)$  selon l'habitude.

Le théorème de Witt a alors les deux corollaires suivants :

1° Pour qu'il existe  $\tau \in O(V)$  avec  $\tau(x) = y$ , il faut et il suffit que  $Q(x) = Q(y)$ .

2° Tous les sous-espaces totalement singuliers maximaux d'un sous-espace  $U$  non isotrope ont la même dimension (ceci résulte immédiatement du fait que pour des espaces totalement singuliers toute application linéaire biunivoque est une isométrie). Cette dimension est appelée indice de  $Q_U$  ou indice de  $U$  et notée  $\nu(U)$ . On notera  $\nu = \nu(V)$ .

On démontre ([1], théorème 2.11) que  $\nu(U) \leq (1/2) \dim U$  ; et on a évidemment

$$\nu(U) \geq 1 \iff \exists x \in U \text{ avec } Q(x) = 0.$$

Ceci dit, on a en vue le théorème ci-après.

THÉORÈME. - Si  $Q$  est non-dégénérée, si  $n \geq 3$  et  $\nu \geq 1$ , alors  $P\Omega(V)$  est simple, sauf dans quelques cas exceptionnels que nous préciserons.

d. Effectuons encore quelques remarques avant d'aborder la démonstration :

1° Pour chaque direction de vecteurs non singuliers  $\langle u \rangle$ , on a une isométrie

$$\sigma_{\langle u \rangle} : z \rightarrow z - (B(u, z)/Q(u))u.$$

Pour  $p \neq 2$ ,  $\sigma_{\langle u \rangle}$  est la symétrie par rapport à  $\langle u \rangle'$ , nous lui conserverons ce nom de préférence à d'autres, plus savants, dans le cas où  $p = 2$ .

2° Si on prolonge tout élément de  $O(U)$  par l'identité sur  $U'$ , on obtient une injection de  $O(U)$  dans  $O(V)$  qui nous permettra d'identifier  $O(U)$  à un sous-groupe de  $O(V)$ .

3° Un lemme enfin nous servira constamment :

Soit  $x \in U$ ,  $x$  singulier,  $U$  non-isotrope de dimension  $\geq 2$ . Il existe  $y \in U$  singulier avec  $B(x, y) = 1$ .

En effet,  $Q_U$  étant non-dégénérée, il existe  $x' \in U$  avec  $B(x, x') \neq 0$ . Le vecteur

$$y = B(x, x')^{-1} x' - Q(x') B(x, x')^{-2} x$$

répond aux conditions exigées.

Dans toute la suite,  $V$  désignera un espace de dimension  $n \geq 3$  et  $Q$  une forme quadratique sur  $V$  non-dégénérée d'indice  $\geq 1$ . Ce que nous démontrerons sur  $V$  s'étendra automatiquement à tout sous-espace  $W$  de  $V$  de dimension  $\geq 3$ , non-isotrope et d'indice  $\geq 1$ .

$V$  contient en particulier un couple  $(x, y)$  du type envisagé dans le lemme, et  $U = \langle x, y \rangle'$  contient toujours un vecteur non singulier.

Nous allons construire un groupe  $\Omega_1(V)$  qui se révélera à l'usage être  $\Omega(V)$ .

## 2. Sous-groupes $H_{\langle x \rangle'}$ .

LEMME 1. - Soit  $x$  singulier et  $u \in \langle x \rangle'$ . Soit  $\rho_{x,u}$  l'application de  $\langle x \rangle'$  dans  $\langle x \rangle'$  définie par :

$$\rho_{x,u}(z) = z + B(z, u)x$$

- $\rho_{x,u}$  est une isométrie de  $\langle x \rangle'$  sur  $\langle x \rangle'$  qui laisse  $x$  invariant.
- $\rho_{x,u}$  s'étend de manière unique en un élément de  $O(V)$  qui, lorsque  $u$  est non-singulier est un élément de  $\Omega(V)$ .

En effet :

(a) est évident car  $Q(z + ax) = Q(z) + a^2 Q(x) + aB(z, x) = Q(z)$  et  $B(x, u) = 0$

(b) est plus long. Soit d'abord  $y$  singulier avec  $B(x, y) = 1$  et  $U = \langle x, y \rangle'$ .  
On a :

$$V = \langle x, y \rangle + U \quad \text{et} \quad \langle x \rangle' = \langle x \rangle + U$$

Remarquons ensuite que si  $u - u' \in \langle x \rangle$ ,  $\rho_{x,u} = \rho_{x,u'}$ , car  $B(z, u) = B(z, u')$  pour  $z \in \langle x \rangle'$ . On peut donc supposer  $u \in U$ . D'autre part (théorème de Witt)  $\rho_{x,u}$  s'étend en un élément  $\rho$  de  $O(V)$ . Pour voir que celui-ci est unique, il suffit de montrer que  $\rho(y)$  est bien déterminé. Or on a une décomposition :

$$\rho(y) = ax + by + v \quad \text{où} \quad a, b \in k, \quad v \in U.$$

Les conditions  $B(\rho(x), \rho(y)) = 1$ ,  $B(\rho(y), \rho(z)) = Q(\rho(y)) = 0$ ,  $\forall z \in U$  donnent :

$$b = 1, \quad B(z, u) + B(z, v) = 0, \quad \forall z \in U \text{ et } a + Q(u) = 0.$$

D'où enfin :

$$f(y) = -Q(u)x + y - u, \text{ et } f \text{ est unique comme annoncé.}$$

Notons  $f_{x,u}$  cette extension unique et supposons  $u$  non-singulier. Evaluons le produit :  $\sigma_{\langle u+Q(u)x \rangle} \sigma_{\langle u \rangle} (z)$  pour  $z \in \langle x \rangle^1$ . Il vient successivement :

$$\begin{aligned} \sigma_{\langle u+Q(u)x \rangle} (z - B(u, z)u/Q(u)) &= z - B(u, z)u/Q(u) - B(u+Q(u)x, z - B(u, z)u/Q(u)) \frac{u+Q(u)x}{Q(u)} \\ &= z - B(u, z)u/Q(u) + B(u, z) \frac{u+Q(u)x}{Q(u)} = z + B(u, z)x = f_{x,u}(z). \end{aligned}$$

D'après l'unicité de  $f_{x,u}$  on a :

$$\sigma_{\langle u+Q(u)x \rangle} \sigma_{\langle u \rangle} = f_{x,u}.$$

Il suffit maintenant de remarquer que  $Q(u + Q(u)x) = Q(u)$ , donc qu'il existe  $\tau \in O(V)$  avec  $\tau(u) = u + Q(u)x$ , donc  $f_{x,u} = \tau \sigma_{\langle u \rangle} \tau^{-1} \sigma_{\langle u \rangle} \in \Omega(V)$  ce qui achève la démonstration du lemme.

Notons maintenant les propriétés suivantes de  $f_{x,u}$  :

- i.  $f_{x,u} f_{x,v} = f_{x,u+v}$  pour  $u, v \in \langle x \rangle^1$
- ii.  $f_{x,cu} = f_{cx,u}$  pour  $u \in \langle x \rangle^1$  et  $c \in k^*$
- iii.  $\tau f_{x,u} \tau^{-1} = f_{\tau(x), \tau(x)}$  pour  $\tau \in O(V)$ .
- iv.  $f_{x,u} = 1 \Leftrightarrow u \in \langle x \rangle$

Il résulte de i. et iv. que  $u \rightarrow f_{x,u}$  est une injection du groupe additif de  $U$  dans  $O(V)$ . Son image ne dépend que de  $\langle x \rangle$  par ii. Notons-la  $H_{\langle x \rangle}$ .

D'après i., ii. et iii., les  $H_{\langle x \rangle}$  sont des sous-groupes abéliens conjugués de  $O(V)$ . Le plus petit sous-groupe distingué de  $O(V)$  contenant  $H_{\langle x \rangle}$  contient tous les  $H_{\langle x \rangle}$  et est engendré par eux ; on le note  $\Omega_1(V)$ . D'après une remarque déjà faite, si  $W$  est un "bon" sous-espace de  $V$ , on peut définir  $\Omega_1(W)$ , possibilité que l'on utilisera effectivement (lemme 4).

PROPOSITION 1. - Sauf dans le cas  $k = F_2$ ,  $n = 4$ ,  $\nu = 2$ ,  $\Omega_1(V)$  est un sous-groupe de  $\Omega(V)$ .

Compte tenu de la définition du groupe  $\Omega_1(V)$  et du fait que  $\Omega(V)$  est distingué, il suffit de montrer que  $H_{\langle x \rangle} \subset \Omega(V)$ , c'est-à-dire, par le lemme 1 b., que  $U$  est engendré par des éléments non-singuliers. Supposons donc qu'il existe  $v \in U$ , qui ne soit pas combinaison linéaire d'éléments non-singuliers de  $U$ . On aura en particulier :

$$Q(v) = 0 \text{ (soit } \nu(U) \geq 1) \text{ et } u \in U, Q(u) = 1 \Rightarrow Q(av + u) = 0, \forall a \in k^*$$

Comme  $Q(av + u) = 1 + aB(v, u)$  ceci entraîne d'abord que  $k^*$  est réduit à l'élément  $-B(v, u)^{-1}$  donc que  $k = F_2$  et que  $B(v, u) = 1$ . Ceci s'écrit encore :

$$B(v, u) = 0 \Rightarrow Q(u) = 0, \text{ d'où } 2 \leq \nu(U) = 2(\dim U - 1) \leq \dim U$$

d'où enfin

$$\dim U = 2 \text{ et } \nu(U) = 1 .$$

C.Q.F.D.

### 3. Etude du groupe $P \Omega_1(V)$ .

Soit  $\bar{V}$  l'espace projectif  $P(V)$ . Soit  $C$  la quadrique de  $\bar{V}$  définie par l'équation  $Q(x) = 0$ . Pour chaque sous-espace  $U$  de  $V$ , on notera  $\bar{U} = P(U)$  et  $C_U = C \cap \bar{U}$ . Si  $G$  est un groupe de transformations linéaires de  $V$ , on notera  $PG$  le groupe de transformations projectives associé. Si  $\nu \in O(V)$ , alors  $\tilde{\nu}(C) = C$  (notation évidente). Nous allons étudier le comportement de  $P \Omega_1(V)$  comme groupe de transformations de  $C$ , c'est-à-dire montrer qu'il est transitif et primitif (sauf pour  $n = 4$ ,  $\nu = 2$ ).

LEMME 2. - Soient  $p = \langle x \rangle \in C$  et  $T_p = \langle x \rangle'$  l'hyperplan tangent à  $C$  en  $p$ . Soient  $y$  et  $U$  définis comme précédemment et  $K(p) = T_p \cap C$ .

- $K(p)$  est le cône de sommet  $p$  et de directrice  $C_U$
  - $\bar{H}_p = P H_{\langle x \rangle}$  est simplement transitif sur  $C - K(p)$ .
- (a) On a l'équivalence :

$$z \in \langle x \rangle', Q(z) = 0 \Leftrightarrow z = ax + u, u \in U, Q(u) = 0 .$$

(b) On a de même :

$$\langle z \rangle \in C - K(p) \Leftrightarrow Q(z) = 0, \quad B(z, x) \neq 0.$$

Il y a alors correspondance biunivoque entre les points  $\langle z \rangle \in C - K(p)$  et les points  $z$  tels que  $Q(z) = 0, B(x, z) = 1$ . Or si on écrit  $z = ax + by - u$ , ces conditions s'écrivent :  $a = -Q(u), b = 1$ , d'où enfin, en se reportant au lemme 1,  $z = \rho_{x,u}(y)$ . On a donc correspondance biunivoque entre  $U$  et  $C - K(p)$  par  $u \rightarrow \rho_{x,u}(y)$  et les propriétés i. et iv. des  $\rho_{x,u}$  permettent de conclure.

REMARQUE. - Si  $\nu = 1$ ,  $K(p)$  est réduit à  $p$ .

PROPOSITION 2. -  $P\Omega_1(V)$  est un groupe transitif de transformations de  $C$ .

Compte tenu du lemme 2, il suffit de vérifier le lemme 3 :

LEMME 3. - Soient  $q$  et  $r$  deux points de  $C$ , il existe  $p \in C$  avec  $q \notin K(p), r \notin K(p)$ .

Choisissons  $y$  et  $z$  singuliers avec  $\langle y \rangle = q, \langle z \rangle = r$ . Distinguons deux cas :

1° Si  $B(y, z) \neq 0$ , on peut supposer  $B(y, z) = 1$ ; prenant  $u \in \langle y, z \rangle'$ ,  $Q(u) \neq 0$  puis  $x = \rho_{y,u}(z) = -Q(u)y + z - u$ , on vérifie que  $p = \langle x \rangle$  répond au problème posé.

2° Si  $B(y, z) = 0$  alors  $\langle y, z \rangle$  est totalement singulier et on peut trouver  $x$  tel que :  $Q(x) \neq 0, B(x, y) \neq 0, B(y, z) \neq 0$  (prendre  $x$  tel que  $Q(x) = 0, B(x, y) = 1$  dans le plan engendré par  $y$  et un supplémentaire de  $\langle z \rangle'$ ). Alors  $p = \langle x \rangle$  convient.

Nous allons maintenant étudier la primitivité de  $P\Omega_1(V)$  sur  $C$ . Pour cela, soit pour  $p \in C$ ,  $L_p$  le stabilisateur de  $p$  :  $L_p = \{ \tau, \bar{\tau} \in P\Omega_1(V), \tau(p) = p \}$ .

D'après BOURBAKI ([2], paragraphe 7, proposition 5), démontrer que  $P\Omega_1(V)$  est primitif (i.e.  $L_p$  maximal) revient à prouver l'assertion suivante :

(P)  $\left\{ \begin{array}{l} \text{Toute partie } M \text{ de } C, \text{ telle que} \\ \text{i. } M \text{ contient au moins deux points } p \text{ et } q \text{ distincts} \\ \text{ii. } \forall \bar{\tau} \in P\Omega_1(V), \bar{\tau}M \cap M \neq \emptyset \text{ entraîne } \bar{\tau}M = M, \\ \text{est } C \text{ toute entière.} \end{array} \right.$

Pour  $\nu = 1$ , par la proposition 2 et le lemme 2,  $P\Omega_1(V)$  est deux fois transitif (car  $\bar{H}_p$  stabilise  $p$  et  $K(p)$  est réduit à  $p$ ). (P) est donc vérifiée.

Si nous exceptons le cas  $n = 4$ ,  $\nu = 2$ , il nous reste à vérifier (P) pour  $n \geq 5$ ,  $\nu \geq 2$ . Etablissons d'abord deux lemmes.

LEMME 4. - Pour  $n \geq 5$ ,  $\nu \geq 2$ ,  $L_p$  est transitif sur  $K(p) - p$ .

Soient  $\langle x \rangle = p$ ,  $y$  avec  $B(x, y) = 1$ ,  $Q(y) = 0$  et  $U = \langle x, y \rangle'$ . On a par hypothèse  $\dim U \geq 3$ ,  $\nu(U) \geq 1$  de sorte que  $P\Omega_1(U)$  est transitif sur  $C_U$  (proposition 2).

On a évidemment  $\bar{H}_p \subset L_p$  et  $P\Omega_1(U) \subset L_p$ . Soient  $q$  et  $r$  dans  $K(p) - p$  et cherchons un  $f \in L_p$  tel que  $f(q) = r$ . D'après le lemme 2 a., on peut trouver  $\tilde{v} \in P\Omega_1(U)$  tel que  $\tilde{v}(q)$  soit aligné avec  $p$  et  $r$ . Il suffit de résoudre le cas où  $p$ ,  $q$  et  $r$  sont alignés, c'est-à-dire où on a, si on pose  $q = \langle t \rangle$ ,  $r = \langle z \rangle$ ,  $z = ax + bt$ ,  $b \neq 0$ . Soit  $u \in U$ , tel que  $B(t, u) = a/b$ ; on a  $f_{x,u}(t) = br$ , d'où  $\bar{f}_{x,u}(q) = r$ .

LEMME 5. - Pour  $\nu \geq 2$ , si  $p, q \in C$ ,  $p \neq q$ , on peut trouver  $r \in C$ ,  $r \neq p$  avec  $r \in K(p)$ ,  $r \notin K(q)$ .

Soient  $p = \langle x \rangle$ ,  $q = \langle y \rangle$ . Si  $\langle y, z \rangle$  est totalement singulier, il existe  $z$  singulier avec  $B(x, z) = 0$ ,  $B(y, z) = 1$ . Si  $\langle y, z \rangle$  est non-isotrope, il existe  $z'$  singulier dans  $\langle x, y \rangle'$ ; posons  $z = x + z'$ . Dans les deux cas  $r = \langle z \rangle$  est le point cherché.

Supposons donc  $n \geq 5$ ,  $\nu \geq 2$  et démontrons l'assertion (P).

Si la ligne  $pq$  est contenue dans  $C$ , alors  $p, q \in K(p)$ ,  $K(q)$ , et le lemme 4 entraîne que  $K(p)$  et  $K(q)$  sont contenus dans  $M$  par ii. Par le lemme 5, il existe  $q' \neq p$ ,  $q' \in K(q) \subset M$ ,  $q' \notin K(p)$ , donc on peut supposer s'être donné  $p$  et  $q$  dans  $M$  tels que la ligne  $pq$  ne soit pas sur  $C$ . Supposons-le dorénavant. Le lemme 2 montre alors que  $M \supset C - K(p)$ ,  $C - K(q)$ . Par le lemme 5, il y a un  $r \in K(p)$ ,  $r \neq p$ ,  $r \notin K(q)$ , donc  $r \in M$ , mais alors la ligne  $pr$  étant dans  $C$ , on a  $K(p) \subset M$  comme on l'a vu, d'où en définitive  $M \supset C - K(p)$ ,  $K(p)$ , c'est-à-dire  $M = C$ .

Nous avons ainsi terminé la démonstration de la

PROPOSITION 3. - Sauf pour  $n = 4$ ,  $\nu = 2$ ,  $P\Omega_1(V)$  est un groupe primitif de transformations de  $C$ .



4. Le groupe  $\Omega(V)$  .

Revenant au groupe  $\Omega_1(V)$  nous allons maintenant démontrer (toujours à quelques exceptions près) que  $\Omega(V) = \Omega_1(V)$  et qu'il est son propre groupe dérivé.

Rappelons quelques résultats classiques ([3], théorème 3.9, [1], chapitre 4, théorème 3.23).

A l'exception du cas  $k = F_2$ ,  $n = 4$ ,  $\nu = 2$ ,  $O(V)$  est engendré par les  $\sigma_{\langle u \rangle}$ . Si on note  $O^+(V)$  le groupe des  $\tau \in O(V)$  qui sont le produit d'un nombre pair de symétries, alors  $\Omega(V)$  est aussi le groupe des commutateurs de  $O^+(V)$ . Enfin  $\tau \in O(V) \Rightarrow \tau^2 \in \Omega(V)$ .

LEMME 6. - Soient  $x$  et  $y$  singuliers avec  $B(x, y) = 1$ . On a (sauf pour  $k = F_2$ ,  $n = 4$ ,  $\nu = 2$ )

$$O(V) = O(\langle x, y \rangle) \Omega_1(V)$$

Il suffit de voir que si  $u$  est un vecteur non singulier,  $\sigma_{\langle u \rangle} \in O(\langle x, y \rangle) \Omega_1(V)$ . Soit  $v \in \langle x, y \rangle$  tel que  $Q(u) = Q(v)$ ; il existe alors  $\tau \in O(V)$  avec  $\tau(v) = u$ . Notons  $x' = \tau(x)$ ,  $y' = \tau(y)$ . On va d'abord voir qu'il existe  $\tau' \in \Omega_1(V)$  avec  $\tau'(x) = x'$ ,  $\tau'(y) = y'$ . D'après la proposition 2, il existe  $\rho \in \Omega_1(V)$  avec  $\langle x' \rangle = \rho(\langle x \rangle)$ ; si  $\langle z \rangle = \rho^{-1}(\langle y' \rangle)$ , on a  $\langle z \rangle \in C - K(p)$ ; par le lemme 2, il existe  $\sigma \in \Omega_1(V)$  avec  $\sigma(\langle x \rangle) = \langle x \rangle$ ,  $\sigma(\langle y \rangle) = \langle z \rangle$ . Il suffit de poser  $\tau' = \rho \sigma \in \Omega_1(V)$ .

Comme  $u \in \langle x', y' \rangle = \tau'(\langle x, y \rangle)$ ,  $u'' = \tau'^{-1}(u) \in \langle x, y \rangle$ . On a alors

$$\sigma_{\langle u \rangle} = \tau' \sigma_{\langle u'' \rangle} \tau'^{-1} = \sigma_{\langle u'' \rangle} [(\sigma_{\langle u'' \rangle} \tau' \sigma_{\langle u'' \rangle}) \tau'^{-1}] \in O(\langle x, y \rangle) \Omega_1(V)$$

PROPOSITION 5. - Sauf dans le cas exclu. dans le lemme 6,  $\Omega_1(V) = \Omega(V)$  .

On a (proposition 1)  $\Omega_1(V) \subset \Omega(V) \subset O^+(V)$ , d'où (lemme 6) :

$$O^+(V) = O^+(\langle x, y \rangle) \Omega_1(V)$$

et

$$O^+(V) / \Omega_1(V) = O^+(\langle x, y \rangle) / O^+(\langle x, y \rangle) \cap \Omega_1(V) .$$

Par un calcul direct (trivial)  $O^+(\langle x, y \rangle)$  est abélien (comme d'ailleurs tout  $O^+(P)$  pour  $P$  de dimension 2); ce qui entraîne  $\Omega(V) \subset \Omega_1(V)$  .

PROPOSITION 6. - Le groupe  $\Omega'(V)$  dérivé de  $\Omega(V)$  coïncide avec celui-ci à l'exception des cas :

- i.  $n = 3$  ,  $k = F_3$
- ii.  $n = 4$  ,  $\nu = 2$  ,  $k = F_2$  ou  $F_3$  .

Soient  $x$  ,  $y$  et  $u$  avec  $Q(x) = Q(y) = 0$  ,  $B(x, y) = 1$  ,  $Q(u) \neq 0$  ,  $u \in \langle x, y \rangle'$  . Il suffit de montrer que  $\rho_{x,u} \in \Omega'(V)$  . En effet ceci entraînera successivement  $H_{\langle x \rangle} \subset \Omega'(V)$  d'où  $\Omega_1(V) \subset \Omega'(V)$  et la proposition précédente conclura.

Supposons d'abord que  $k$  ait plus de 3 éléments, il y aura en particulier  $c \in k$  avec  $c^2 \neq 0, 1$  . Soit  $\tau$  l'élément de  $O(\langle x, y \rangle)$  défini par  $\tau(x) = cx$  ,  $\tau(y) = c^{-1}y$  . On aura  $\tau^2 \in \Omega(V)$  et

$$\tau^2 \rho_{x,u} \tau^{-2} \rho_{x,u}^{-1} = \rho_{c^2x,u} \rho_{x,-u} = \rho_{x,(c^2-1)u} .$$

Comme  $c^2 - 1 \neq 0$  ,  $\rho_{x,u} \in \Omega'(V)$  .

Si maintenant  $k = F_2$  ou  $F_3$  on peut supposer  $n = 4$  ,  $\nu = 1$  ou  $n \geq 5$  ,  $\nu \geq 2$  (en effet le seul cas non exclu par le texte est  $k = F_2$  ,  $n = 3$  ,  $\nu = 1$  qui est impossible car alors  $B(u, u) = 0$  entraîne que  $B$  est dégénérée, cas implicitement exclu ). Il existe alors un plan  $P$  non-isotrope et d'indice 0 avec  $u \in P \subset \langle x, y \rangle'$  .

Si  $k = F_2$  , il existe dans  $P$  un vecteur  $v$  avec  $B(u, v) = Q(v) = 1$  et si on définit un élément  $\tau$  de  $O(P)$  par  $\tau(u) = v$  ,  $\tau(v) = u + v$  , on a  $\tau^3 = 1$  d'où  $\tau = (\tau^{-1})^2 \in \Omega(V)$  et  $\tau \rho_{x,v} \tau^{-1} \rho_{x,v}^{-1} = \rho_{x,u+v} \rho_{x,-v} = \rho_{x,u}$

Si  $k = F_3$  , il existe dans  $P$  un vecteur  $v$  avec  $B(u, v) = 0$  ,  $Q(u) = Q(v)$  . Soit alors  $\tau \in O(P)$  défini par  $\tau(u) = -v$  ,  $\tau(v) = u$  ; on a  $\tau^2 \in \Omega(V)$  et

$$\tau^2 \rho_{x,u} \tau^{-2} \rho_{x,u}^{-1} = \rho_{x,-u} \rho_{x,-u} = \rho_{x,u} .$$

##### 5. Démonstration du théorème fondamental.

Avant celle-ci, un ultime lemme :

LEMME 7. -  $PO(V)$  est un groupe fidèle de transformations de  $C$  .

Soit en effet un élément  $\tau \in O(V)$  tel que pour tout  $x$  singulier, on ait  $\tau(x) = \lambda_x x$  ( $\lambda_x \in k$ ). Soient  $x$  et  $y$  singuliers,  $B(x, y) = 1$ . Pour tout  $u \in \langle x, y \rangle$ , le vecteur  $v = \rho_{x,u}(y) = y - Q(u)x - u$  est singulier. On a donc pour certains scalaires  $a, b, c$  :

$$\tau(x) = ax, \quad \tau(y) = by, \quad \tau(v) = cv$$

soit :

$$(1) \quad by - Q(u)ax - \tau(u) = cy - cQ(u)x - cu.$$

Si  $Q(u) = 0$ , on a, par hypothèse,  $\tau(u) = du$  pour un  $d \in k$ .

Si  $Q(u) \neq 0$ , d'après (1),  $\tau(u) \in \langle x, y, u \rangle$  non isotrope. Dans ce sous-espace  $\tau(u)$  et  $u$  sont tous deux perpendiculaires à  $\langle x, y \rangle$ . Alors on a aussi  $\tau(u) = du$ . Reportant dans (1) on obtient évidemment :  $a = b = c = d$ , d'où

$$\forall u, \quad \tau(u) = au, \quad \text{c'est-à-dire } \bar{c} = 1$$

**THÉOREME.** -  $P\Omega(V)$  est simple sauf pour :

- i.  $k = F_3, n = 3$
- ii.  $k$  quelconque,  $n = 4, \nu = 2$ .

Soit  $N$  un sous-groupe distingué de  $P\Omega(V)$  non réduit à  $\{1\}$ . Pour  $p \in C$ , le groupe  $L_p$  défini dans le lemme 4 est maximal (proposition 3) et l'intersection des ses conjugués est réduite à  $\{1\}$  (lemme 7). Ceci entraîne que le groupe  $NL_p$  est tout  $P\Omega(V)$ . En effet  $NL_p = L_p$  entraînerait  $N \subset L_p$  c'est-à-dire  $N = \{1\}$ .

$N$  est donc transitif sur  $C$ .  $N\bar{H}_p$  contenant alors tous les conjugués de  $\bar{H}_p$  car  $\rho \in N$  entraîne  $\bar{H}_{\rho(p)} = \rho\bar{H}_p\rho^{-1} = (\rho\bar{H}_p)(\rho^{-1}.1) \in N\bar{H}_p$ , on a :

$$N\bar{H}_p = P\Omega_1(V) = P\Omega(V) \quad (\text{proposition 5}).$$

Ceci implique :

$$P\Omega(V)/N = N\bar{H}_p/N = \bar{H}_p/\bar{H}_p \cap N$$

mais  $\bar{H}_p$  étant abélien, la proposition 6 entraîne  $N = P\Omega(V)$ .

$P\Omega(V)$  est donc simple

C. Q. F. D.

## BIBLIOGRAPHIE

- [1] ARTIN (Emil). - Geometric algebra. - New York, Interscience, 1957 (Interscience Tracts in pure and applied Mathematics, 3).
- [2] BOURBAKI (Nicolas). - Algèbre, Chapitre 1 : Structures algébriques. - Paris, Hermann, 1942 (Act. scient. et ind., 934; Éléments de Mathématique, 4).
- [3] CHEVALLEY (Claude). - The algebraic theory of spinors. - New York, Columbia University Press, 1954.
- [4] DICKSON (D. E.). - Linear groups. - Leipzig, B. G. Teubner, 1901.
- [5] DIEUDONNÉ (Jean). - Sur les groupes classiques. - Paris, Hermann, 1948 (Act. scient. et ind., 1040 ; Publ. Inst. Math. Univ. Strasbourg, 6).
- [6] EICHLER (Martin). - Quadratische Formen und orthogonale Gruppen. - Berlin, Springer, 1952 (Die Grundlehren der mathematischen Wissenschaften ..., 63).
- [7] IWASAWA (Kenkiti). - Über die Einfachheit der speziellen projektiven Gruppen, Proc. Imp. Acad. Tokyo, t. 17; 1941, p. 57-59.
- [8] SIEGEL (Carl Ludwig). - Über die Zetafunktionen indefiniter quadratischer Formen, II., Math. Z., t. 44, 1938, p. 398-426.
- [9] TAMAGAWA (Tsuneo). - On the structure of orthogonal groups, Amer. J. of Math., t. 80, 1958, p. 191-197.

La démonstration originelle du théorème est due à DICKSON ([4]) pour  $k$  fini, à DIEUDONNÉ ([5]) pour le cas général. Le principe de la démonstration de [9] donnée ici est dû à IWASAWA ([7]). Les  $\rho_{x,u}$  furent introduits par EICHLER ([6], chapitre 1, paragraphe 3) et une autre interprétation en est donnée par SIEGEL ([8] p. 408).

---