RÉDACTION N° 181

COTE : NBR 084

TITRE : SANS TITRE GÉNÉRAL (ALGÈBRE)
FORMES QUADRATIQUES

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 71

NOMBRE DE FEUILLES : 71

COMMENTAIRES DU RÉDACTEUR.

J'étais en train de travailler à cette rédaction quand j'ai été interrompu par la nécessité de rédiger rapidement un petit livre sur les spineurs, qui sera publié par Columbia à l'occasion de son bicentenaire. Sur les conseils de Dieudonné, je communique néanmoins à mon illustre maître ce début de rédaction qui d'une part n'est qu'un début et d'autre part n'est probablement pas sous la forme définitive qu'il eût prise.

On trouvera probablement trop longue la présentation des puissances réduites dans les algèbres extérieures de caractéristique p (arrangement des trucs Lepage-Papy), et je serai d'accord ; cependant, il me semble qu'on peut se poser la question de savoir s'il ne faut pas mettre cela quelque part dans Bourbaki, cela est utile en diverses circonstances.

J'insiste sur la forme donnée au th. de Witt ; le précédent rédacteur est d'ailleurs d'accord avec moi et me dit qu'il ne l'a mis sous sa forme restreinte que par obéissance, à mon avis abusive, à quelque lubie de Congrès.

Le lecteur se souviendra que j'ai toujours adhéré strictement à la règle de noter à droite (resp.: à gauche) les multiplications scalaires du dual d'un module à gauche (resp.: à droite) même quand l'anneau de base est commutatif.

Je joins deux courts papiers, l'un sur les transferts d'anneau de base, l'autre sur les algèbres extérieures, à verses au dossier des révisions des Chap. II et III ; n'ayant pas de double, j'aimerais que ces papiers fussent tirés.

FORMES QUADRATIQUES.

Nous ferons dans ce chapitre les conventions suivantes. Le mot "anneau" (resp.: "algèbre") signifiera "anneau (resp.: algèbre) possédant un élément unité" . Les éléments unité des divers anneaux que nous considérerons seront uniformément notés 1 . Par une représentation d'un anneau (resp.: d'une algèbre) A dans un anneau (resp.: une algèbre) B , nous entendrons une représentation de A dans B qui applique l'élément unité de A sur celui de B . Par un sous-anneau (resp.: sous-algèbre) de A , nous entendrons un sous-anneau (resp.: une sous-algèbre) de A qui contient l'élément unité. Par un ensemble de générateurs S d'un anneau (resp.: d'une algèbre) A , nous entendrons une partie S de A telle que S $\{1\}$ soit un ensemble de générateurs au sens usuel. Par un module sur A nous entendrons un module unitaire sur A .

---

§ 1. FORMES RÉFLEXIVES.

Soit A un anneau.

Nous avons défini la notion de forme bilinéaire sur le produit $M \times N$ d'un module à gauche M sur A et d'un module à droite N sur A . Nous allons maintenant considérer le cas où M et N ont les mêmes éléments et la même addition.

Définition 1. Par un duamodule sur A , nous entendrons un ensemble M qui est muni à la fois d'une structure de module à gauche et d'une structure de module à droite sur A , ces deux modules ayant le même groupe additif.

Si M est un duomodule, les modules à ga uche et à droite sous-jacents à M seront désignés par M_g et M_d .

On notera que nous n'imposons pas la condition que l'on ait $(ax)b = a(xb)$ si $a \in A$, $x \in M$, $b \in B$. C'est pourquoi nous parlons de "duomodules" et non de "bimodules".

Exemples. 1. Soit h une représentation de l'anneau A dans un anneau A'; alors les lois de composition $(a,a') \to h(a)a'$ et $(a',a) \to a'h(a)$ $(a \in A,\ a' \in A')$ définissent sur A' une structure de duomodule sur A .

2. Soient M un module à gauche sur l'anneau A et s un antiautomorphisme de A . La loi de composition $(x,a) \to a^s x$ $(a \in A\ ,\ x \in M)$ définit alors sur M une structure de duomodule. Nous dirons qu'un duomodule défini de cette manière est "attaché à l'antiautomorphisme s " ; ces duomodules sont caractérisés par le fait que l'on a $xa = a^s x$ si $a \in A$, $x \in M$. Il est clair que, s étant donné, tout module à droite sur A est également le module à droite sous-jacent d'un duomodule attaché à s .

Soit M un duomodule. Une partie N de M qui est un sous-module à la fois de M_g et de M_d porte une structure de duomodule telle que N_g soit sous-module de M_g et N_d sous-module de M_d ; on dit que l'ensemble N, muni de cette structure, est un sous-duomodule de M. La somme d'une famille de sous-duomodules de M est la même qu'on considère ces duomodules comme des sous-modules de M_g ou de M_d, et c'est un sous-duomodule de M. De même, l'intersection d'une famille de sous-duomodules de M est un sous-duomodule. Si S est une partie quelconque de M, l'intersection de tous les sous-duomodules contenant S s'appelle le sous-duomodule engendré par S.

Définition 2. Soit M un duomodule. On appelle forme bilinéaire sur M une application de $M \times M$ dans A qui est une forme bilinéaire sur $M_g \times M_d$.

Toutes les notions introduites à propos des formes bilinéaires sur le produit de deux modules, l'un à gauche, l'autre à droite, s'appliquent en particulier au cas des formes bilinéaires sur un duomodule. Rappelons en particulier que, si B est une forme bilinéaire sur le duomodule M, un élément y de M est dit conjugué à droite (resp.: à gauche) à un élément x si $B(x,y)=0$ (resp.: $B(y,x)=0$).

Définition 3. Une forme bilinéaire B sur un duomodule M est dite réflexive si la relation " y est conjugué à droite à x (par rapport à B)" entre éléments x,y de M est équivalente à la relation "y est conjugué à droite à x (par rapport à B)" entre éléments x,y de M est équivalente à la relation " y est conjugué à gauche à x ".

Dans le cas d'une forme réflexive, on dira "conjugué" au lieu de "conjugué à droite" ou "conjugué à gauche".

Si B est une forme bilinéaire réflexive sur un duomodule M, et si S est une partie de M, l'ensemble des éléments de M qui sont conjugués à

tous les éléments de S (par rapport à B) est un sous-duomodule de M, qu'on appelle le conjugué de S ; il est clair que S est contenu dans le canjugué de son conjugué.

Définition 4. Soit B une forme bilinéaire réflexive sur un duomodule M. Un élément x de M est dit isotrope (par rapport à B) s'il est conjugué à lui-même. Un sous-module N de M est dit isotrope (par rapport à B) s'il a un élément $\neq 0$ en commun avec son conjugué. Un sous-module N de M est dit totalement isotrope (par rapport à B) s'il est contenu dans son conjugué.

Pour que x soit isotrope, il est donc nécessaire et suffisant que $B(x,x)=0$. Pour qu'un sous-module N de M soit isotrope, il faut et suffit qu'il existe un élément $x \neq 0$ de N tel que $B(x,y)=0$ pour tout $y \in N$; x est alors isotrope. La condition pour que N soit isotrope peut encore se formuler comme suit : la restriction de B à $N \times N$ est une forme bilinéaire dégénérée sur $N \times N$. Pour qu'un sous-module N de M soit totalement isotrope, il faut et suffit que B soit nulle sur $N \times N$. Si S est une partie de M telle que B soit nulle sur $S \times S$, le sous-duomodule N engendré par S est totalement isotrope. Soient en effet P le conjugué de S et Q celui de P ; on a $S \subset P \cap Q$, d'où $N \subset P \cap Q$; or l'intersection d'un duomodule avec son conjugué est évidemment un sous-duomodule totalement isotrope.

L'ensemble des parties S de M telles que B soit nulle sur $S \times S$, ordonné par inclusion, est évidemment inductif. Il en résulte en particulier que tout sous-duomodule totalement isotrope de M est contenu dans un sous-duomodule totalement isotrope maximal .

Soit N un sous-duomodule totalement isotrope maximal de M . Alors, si x est un élément isotrope du conjugué de N , la restriction de B à $(N \cup \{x\}) \times (N \cup \{x\})$ est nulle ; puisque N est maximal, on a $x \in N$. En particulier, si on a $B(y,y)=0$ pour tout $y \in N$ M (c'est le cas des formes alternées, que nous étudierons plus loin), N est son propre conjugué.

Soit N le conjugué du module M tout entier. C'est un sous-duomodule totalement isotrope de M. Puisque N est sous-module de M_g et de M_d , le groupe additif M/N se trouve muni de structures de modules à gauche et à droite sur A , qui en font un duomodule. Si x,y sont dans M , la valeur de $B(x,y)$ ne dépend que des classes $\overline{x}$, $\overline{y}$ de x,y modulo N ; si on la désigne par $\overline{B}(\overline{x},\overline{y})$, $\overline{B}$ est une forme bilinéaire, évidemment réflexive, sur M/N , et le conjugué de M/N par rapport à cette forme se réduit à $\{0\}$, ce qui signifie que $\overline{B}$ est non dégénérée. Si l'anneau de base A est un corps, $(M/N)_g$ et $(M/N)_d$ ont même dimension (finie ou infinie), égale au rang de B , qui est aussi le rang de $\overline{B}$.

Quand nous dirons qu'une forme bilinéaire est de rang >1, nous voudrons dire qu'elle est ou bien de rang infini ou, bien de rang fini >1.

Proposition 1. Soit M un duomodule sur un corps K et soit B une forme bilinéaire non dégénérée réflexive de rang >1 sur M . Le duomodule M est alors attaché à un antiautomorphisme s de K . Il existe un élément m de K tel que $B(y,x) = (B(x,y))^s m$ quels que soient x et y dans M . On a $mm^s=1$, et s^2 est l'automorphisme intérieur $a \to mam^{-1}$ de K .

Puisque B est non dégénérée, tout sous-espace de dimension finie de M_g (resp.: M_d) est le conjugué de son conjugué et est par suite un sous-espace de M_d (resp.: M_g). En particulier, si x est un élément $\neq 0$ de M , Kx (resp.: xK) est un sous-espace de M_d (resp.: M_g) contenant x ,

d'où $Kx \supset xK$, $xK \supset Kx$ et $xK = Kx$. Il existe donc une application biunivoque $s(x)$ de K sur lui-même telle que $xa = a^{s(x)}x$ pour tout $a \in K$. Soient x,x' des éléments $\neq 0$ de K ; si x,x' sont linéairement indépendants dans M_g , on a $x+x' \neq 0$, et $a^{s(x+x')}(x+x') = (x+x')a = xa + x'a = a^{s(x)}x + a^{s(x')}x'$ pour tout $a \in K$, ce qui entraîne $s(x') = s(x+x') = s(x)$. Si x,x' sont linéairement dépendants, il résulte du fait que B est de rang >1 qu'il y a un $y \in M_g$ linéairement indépendant de x , donc de x', d'où $s(x') = s(y) = s(x)$. Les opérations $s(x)$, pour tous les $x \neq 0$, sont donc égales entre elles ; soit s leur valeur commune. Si a,b sont dans K , et $x \neq 0$ dans M , on a $(a+b)^s x = x(a+b) = xa+xb = (a^s+b^s)x$, $(ab)^s x = x(ab) = (xa)b = = b^s(xa) = b^s a^s x$; on en conclut que s est un antiautomorphisme de K . Il est clair que M est un duomodule attaché à s .

Si $x \in M$, désignons par $f(x)$ l'application $y \to B(y,s)$ et par $f'(x)$ l'application $y \to (B(x,y))^s$. La première de ces applications est évidemment une forme linéaire sur M_g ; montrons qu'il en est de même de la seconde. Il est clair que $f'(x)$ est une représentation du groupe additif de M dans celui de K . Si $a \in A$, on a $(B(x,ay))^s = (B(x,ya^{s^{-1}}))^s = (B(x,y)a^{s^{-1}})^s = a(B(x,y))^s$, ce qui démontre notre assertion. De plus, l'espace des zéros de $f'(x)$ est le conjugué de $\{x\}$, donc aussi l'espace des zéros de $f(x)$. Il en résulte qu'uil y a un élément $m(x)$ de K tel que $f(x) = f'(x)m(x)$; si $x \neq 0$, on a $f(x) \neq 0$ puisque B est non dégénérée, et $m(x)$ est uniquement déterminé et $\neq 0$. Soient x,x' des éléments linéairement indépendants de M_d ; il est clair que $f(x+x') = f(x) + f(x')$, $f'(x+x') = f'(x)+f'(x')$, d'où $(f(x)+f(x'))(m(x+x'))^{-1} = f(x)(m(x))^{-1} + f(x')(m(x'))^{-1}$.

Par ailleurs, il est clair que, pour tout $a \in K$, $f(xa)$ est la forme linéaire $f(x)a$; il vient donc

$$f((x+x')(m(x+x'))^{-1} - x(m(x))^{-1} - x'(m(x'))^{-1}) = 0 .$$

Puisque B est non dégénérée, ceci entraîne $(x+x')(m(x+x'))^{-1} = x(m(x))^{-1} + x'(m(x'))^{-1}$ et par suite $m(x') = m(x+x') = m(x)$. Si maintenant x,x' sont des éléments $\neq 0$ linéairement dépendants l'un de l'autre dans M_d, il y a un $y \in M$ qui est linéairement indépendant de x, donc de x', et $m(x') = m(y) = m(x)$. Les éléments $m(x)$ relatifs à tous les $x \neq 0$ de M sont donc égaux ; soit m leur valeur commune. On a $B(y,x) = (B(x,y))^s m$ quels que soient x,y dans M. Donc $B(x,y) = (B(y,x))^s m = m^s (B(x,y))^{s^2} m$; or il est clair que, pour tout $a \in K$, il y a des éléments x,y de M tels que $a = B(x,y)$; on a donc $a = m^s a^{s^2} m$. Prenant $a=1$, il vient $m^s m = 1$, d'où $mm^s = 1$ et $a^{s^2} = mam^{-1}$. La prop.1 est donc démontrée.

Les notations étant celles de la prop.1, on a $B(x,x) = (B(x,x))^s m$. Supposons qu'il existe un $x_0 \in M$ tel que $b = B(x_0,x_0) \neq 0$; on a $b = b^s m$. Posons $B'(x,y) = B(x,y)b^{-1}$; on a $B'(y,x) = (B(x,y))^s mb^{-1} = (B'(x,y)b)^s (b^{-1})^s = b^s (B'(x,y))^s (b^s)^{-1}$. Soit t l'application $a \to b^s a^s (b^s)^{-1}$; étant composée d'un antiautomorphisme et d'un automorphisme (intérieur), t est un antiautomorphisme, et on a $B'(y,x) = (B'(x,y))^t$. Il est clair que $(x,y) \to B'(x,y)$ est une application de $M \times M$ sur K ; puisque $B'(x,y) = (B'(x,y))^{t^2}$, t^2 est l'automorphisme identique de K. L'application B' n'est pas en général une forme bilinéaire sur M : on a, pour $a \in K$, $B'(x,ya) = B(x,y)ab^{-1} = B'(x,y)\, bab^{-1}$. Mais, définissons une loi de composition externe entre éléments de M et de K par la formule $(y,a) \to y*a = y(b^{-1}ab) = -1$;

on voit tout de suite que cette loi définit, avec l'addition dans M, une structure de module à droite M'_d sur M. Les structures M_g et M'_d définissent sur M une nouvelle structure de duomodule M', et on a $B'(x,y*a) = B'(x,y)\ b(b^{-1})ab)b^{-1} = B'(x,y)a)$, d'où il résulte tout de suite que B' est une forme bilinéaire sur M'.

Si on a $B(x,x) = 0$ pour tout $x \in M$, on a $0 = B(x+y,x+y) = B(x,y) + B(y,x)$. Puisque $B(y,x) = (B(x,y))^s m$, on a $-a = a^s m$ pour tout $a \in K$. Prenant $a=1$, il vient $m = -1$, d'où $a = a^s$; s est l'application identique de K sur lui-même, et, comme s est un anti-automorphisme, K est commutatif.

Définition 4. Soient A un anneau commutatif et M un duomodule sur A attaché à l'automorohisme identique de A. Une forme bilinéaire B sur M est dite alternée si on a $B(x,x) = 0$ pour tout $x \in M$.

Si M est un module à gauche sur A, on peut le munir d'une structure de duomodule sur A en posant $xa = ax$ pour $a \in A$, $x \in M$; les formes bilinéaires alternées sur ce duomodule s'appellent aussi formes bilinéaires alternées sur le module à gauche M.

Définition 5. Soit M un duomodule sur un anneau A, attaché à un antiantomorphisme s de A dont le carré est l'application identique. Une forme bilinéaire B sur M est dite hermitienne si on a $B(y,x) = (B(x,y))^s$ quels que soient x,y dans M. Si A est commutatif et si s est l'application identique, on dit aussi "symétrique" au lieu de "hermitienne".

Si M est un module à gauche sur un anneau commutatif A, on appelle encore forme bilinéaire symétrique sur M une forme bilinéaire symétrique sur le duomodule déduit de M en posant $xa = ax$ pour tout $a \in A$, $x \in M$.

Il résulte de ce que nous avons dit que, si M est un duomodule sur un corps, l'étude des formes bilinéaires réflexives de rangs > 1 sur M se ramène dans une large mesure à l'étude des formes alternées et des formes hermitiennes. La prop.1 ne s'étend pas au cas des formes de rang 1 (cf. exerc.).

Soit M un duomodule sur un anneau A attaché à un antiautomorphisme s de A . Il est clair que tout sous-module de M_g est alors aussi un sous-module de M_d , et porte par suite une structure de duomodule. De même, toute base de M_g est aussi une base de M_d ; on dit aussi que c'est une base de M . Si N est un autre duomodule sur A, également attaché à s , toute application linéaire f de M_g dans N_g est aussi une application linéaire de M_d dans N_d ; nous dirons que c'est une application linéaire de M dans N . En particulier, nous appellerons endomorphisme (resp.: automorphisme) de M toute application linéaire de M dans lui-même.

Proposition 2. Soient M un duomodule sur A , attaché à un antiautomorphisme s de A , et B une forme bilinéaire non dégénérée sur M qui est soit alternée soit hermitienne (relativement à s). Si un endomorphisme u de M admet un adjoint u^* par rapport à B quand on le considère comme endomorphisme de M_g , u^* est aussi l'adjoint de u considéré comme endomorphisme de M_d et u est l'adjoint de u^* .

On a en effet $B(u.x,y) = B(x,u^*.y)$ quels que soient x,y dans M . Posons $e = -1$ si B est alternée, $e = 1$ dans le cas contraire. On a donc $B(y,u.x) = e(B(u.x,y))^s = e(B(x,u^*y))^s = B(u^*.y,x)$, et la prop.2 résulte immédiatement de cette formule.

Les notations étant celles de la prop.2, nous dirons que u^* est l'adjoint de u . L'ensemble des endomorphismes u de M qui admettent des adjoints est un sous-anneau de l'anneau des endomorphismes de M ,

et l'application $u \to u^*$ est un antiautomorphisme de cet anneau. Si l'application linéaire de M_g dans le dual de M_d associée à B est un isomorphisme du premier de ces modules sur le second, tout endomorphisme de M admet un adjoint ; il en est en particulier ainsi quand l'anneau de base est un corps et M_g est de dimension finie. Dans le cas général, l'ensemble des automorphismes de M qui admettent des adjoints qui sont également des automorphismes est un groupe , et l'application $u \to u^{-1*}$ est un automorphisme d'ordre 2 de ce groupe.

Soit M un duomodule attaché à un antiautomorphisme s de son anneau de base A et qui possède une base finie $(x_1,\dots,x_n)$. Soit B une forme bilinéaire sur M . La matrice qui représente B par rapport aux bases $(x_1,\dots,x_n)$ de M_g et $(x_1,\dots,x_n)$ de M_d s'appelle aussi la matrice qui représente B par rapport à la base $(x_1,\dots,x_n)$ de M . Soit $\underline{B}$ cette matrice. Si $x \in M$, on peut représenter x relativement à la base $(x_1,\dots,x_n)$ de M_d par une matrice à une colonne, dont les éléments sont les coefficients a_i de l'expression $x = \sum_{i=1}^{n} x_i a_i$ de x comme combinaison linéaire à droite des x_i ; soit $\underline{x}$ cette matrice. On a $x = \sum_{i=1}^{n} a_i^s x_i$, de sorte que la matrice qui représente x par rapport à la base $(x_1,\dots,x_n)$ quand on considère x comme élément de M_g est $\underline{x}^s$ (la matrice qui se déduit de $\underline{x}$ en appliquant l'opération s à ses éléments). Nous dirons que $\underline{x}$ et $\underline{x}^s$ sont les matrices représentatives de x à droite et à gauche respectivement. Soient y un autre élément de M , et $\underline{y}$ sa matrice représentative à droite ; on voit tout de suite que

$$(1) \qquad B(x,y) = {}^t\underline{x}^s . \underline{B} . \underline{y} \ .$$

Soit u un endomorphisme de M . Considéré comme endomorphisme de M_d , u est représenté par rapport à la base $(x_1,\dots,x_n)$ par une matrice $\underline{U}$; la matrice qui représente u par rapport à $(x_1,\dots,x_n)$ quand on considère u

comme endomorphisme de M_g est évidemment $\underline{U}^s$. Nous dirons que $\underline{U}$ et $\underline{U}^s$ sont les matrices représentatives de u à droite et à gauche respectivement. Si $(y_1,\dots,y_n)$ est une autre base de M , et $\underline{T}$ la matrice de transition de $(x_1,\dots,x_n)$ à $(y_1,\dots,y_n)$ quand on les considère comme bases de M_d , la matrice de transition de $(x_1,\dots,x_n)$ à $(y_1,\dots,y_n)$ quand on les considère comme bases de M_g est $\underline{T}^s$; nous dirons que $\underline{T}$ et $\underline{T}^s$ sont les matrices de transition de $(x_1,\dots,x_n)$ à $(y_1,\dots,y_n)$ à droite et à gauche respectivement. Il résulte immédiatement de la formule (1) ci-dessus que la matrice représentative de B par rapport à la base $(y_1,\dots,y_n)$ est

$$ {}^t\underline{T}^s.\underline{B}.\underline{T} \quad . $$

Définition 6. Les notations étant comme ci-dessus, supposons de plus que A soit commutatif. Le déterminant de la matrice B est alors appelé le discriminant de la forme B par rapport à la base $(x_1,\dots,x_n)$.

Soit D ce discriminant. Pour que B soit non dégénérée, il faut et suffit que $D \neq 0$. Par ailleurs, le discriminant de B par rapport à une autre base $(y_1,\dots,y_n)$ est $t.t^s.D$ si t est le déterminant de la matrice de transition à droite de $(x_1,\dots,x_n)$ à $(y_1,\dots,y_n)$.

Ne supposant plus nécessairement l'anneau A commutatif, mais supposant que le carré de s soit l'identité, il est clair que, si B est hermitienne relativement à s , on a ${}^t\underline{B}^s = \underline{B}$. Réciproquement, si ${}^t\underline{B}^s = \underline{B}$, B est hermitienne relativement à s . Pour le voir, établissons le

Lemme 1. Soient s un antiautomorphisme d'un anneau A et P,Q des matrices rectangulaires à éléments dans A telles que P Q soit défini. On a alors ${}^t(\underline{P}\,\underline{Q})^s = ({}^t\underline{Q}^s)({}^t\underline{P}^s)$.

Soit en effet $\underline{P} = (p_{ij})_{1 \leqq i \leqq m, 1 \leqq j \leqq n}$, $\underline{Q} = (q_{jk})_{1 \leqq j \leqq n, 1 \leqq k \leqq r}$. L'élément d'indices k , i de la matrice ${}^t(\underline{P}\,\underline{Q})^s$ est alors $\sum_{j=1}^{n} q_{jk}^s p_{ij}^s = \sum_{j=1}^{n} q'^s_{kj}\, p'^s_{ji}$, si ${}^t\underline{Q} = (q'_{kj})$, ${}^t\underline{P} = (p'_{ji})$, ce qui démontre le lemme.

Ceci dit, supposons que ${}^t\underline{B}^s = \underline{B}$. Soient x,y des éléments de M , $\underline{x}$ et $\underline{y}$ leurs matrices représentatives à droite. On a $B(y,x) = {}^t\underline{y}^s . \underline{B} . \underline{x}$, d'où (B(y,x) étant considéré comme matrice à une ligne et à une colonne, donc identique à sa transposée)
$(B(y,x))^s = {}^t\underline{x}^s . {}^t\underline{B}^s . \underline{y} = {}^t\underline{x}^s . \underline{B} . \underline{y} = B(x,y)$ et B est hermitienne. Puisque le carré de s est l'identité, la relation ${}^t\underline{B}^s = \underline{B}$ peut aussi s'écrire ${}^t\underline{B} = \underline{B}^s$.

Définition 7. Soient A un anneau et s un antiautomorphisme de A dont le carré est l'identité. Une matrice B à éléments dans A est dite hermitienne (relativement à s) si ${}^t\underline{B} = \underline{B}^s$.

Supposons maintenant A commutatif. Soit $\underline{B} = (b_{ij})_{1 \leqq i,j \leqq n}$. Si B est alternée, on a manifestement ${}^t\underline{B} = -\underline{B}$, $b_{ii} = 0$ $(1 \leqq i \leqq n)$. Les conditions $b_{ii} = 0$ sont d'ailleurs des conséquences de la condition ${}^t\underline{B} = -\underline{B}$ si on suppose que 2.1 n'est pas diviseur de zéro dans A . Réciproquement, les conditions ${}^t\underline{B} = -\underline{B}$, $b_{ii} = 0$ sont suffisantes pour que B soit alternée. Supposons les en effet satisfaites, et soit $x = \sum_{i=1}^{n} x_i a_i$ un élément de M . On a $B(x,x) = \sum_{1 \leqq i,j \leqq n} a_i b_{ij} a_j = 0$ puisque $a_i b_{ii} a_i = 0$ et $a_i b_{ij} a_j + a_j b_{ji} a_i = 0$ si $i \neq j$.

Définition 8. Une matrice B à éléments dans un anneau commutatif A est dite alternée si ${}^t\underline{B} = -\underline{B}$ et si les éléments diagonaux de B sont nuls.

n° 2. FORMES HERMITIENNES ET QUADRATIQUES.

Désignons par A un anneau et par s un antiautomorphisme de A dont le carré est l'automorphisme identique. Soit M un duomodule sur A attaché à s . Si $a \in A$, nous poserons $S(a) = a+a^s$ si s n'est pas l'automorphisme identique, et $S(a) = a$ dans le cas contraire (qui ne peut d'ailleurs se présenter que si A est commutatif, s étant un antiautomorphisme).

Définition 9. Les notations étant comme ci-dessus, une application Q de M dans A s'appelle une forme hermitienne s'il existe une forme bilinéaire hermitienne B sur M telle que l'on ait

$$Q(ax+by) = aQ(x)a^s + bQ(y)b^s + S(aB(x,y)b^s)$$

quels que soient x,y dans M et a,b dans A . On dit que la forme hermitienne Q et la forme bilinéaire B sont associées l'une à l'autre. Si s est l'automorphisme identique de A , Q s'appelle aussi une forme quadratique.

Si M est un module à gauche ou à droite sur A ,,on peut toujours considérer M comme module sous-jacent d'un duomodule attaché à s ; et les formes hermitiennes ou quadratiques sur ce duomodule s'appellent aussi formes hermitiennes ou quadratiques sur M .

Exemples.- 1. Soit B une forme bilinéaire hermitienne quelconque sur M ; posons $Q(x) = B(x,x)$. On a alors

$$Q(ax+by) = aQ(x)a^s + bQ(y)b^s + eS(aB(x,y)b^s)$$

où e est 1 ou 2 suivant que s n'est pas ou est l'automorphisme identique de A ; Q est donc une forme hermitienne attachée à eB . On voit de même que, si s est l'automorphisme identique de A et B_0 une forme bilinéaire quelconque sur M , $x \to B_0(x,x)$ est une forme quadratique sur M , attachée à la forme bilinéaire symétrique $(x,y) \to B_0(x,y) + B_0(y,x)$.

2. Si Q est une forme hermitienne sur le duomodule M et N un sous-duomodule de M , la restriction de Q à N est une forme hermitienne sur N .

Soient Q une forme hermitienne et B une forme bilinéaire hermitienne associée à Q . On a alors d'une part $Q(2x)=2Q(x) + S(B(x,x))$ et d'autre part $Q(2x) = 4Q(x)$; de plus, $B(x,x) = (B(x,x))^s$ d'où $2Q(x) = 2B(x,x)$ si s n'est pas l'automorphisme identique, et $2Q(x)=B(x,x)$ dans le cas contraire. On voit donc que, si 2.1 n'est pas diviseur de zéro dans A , la donnée de B détermine entièrement Q . On peut aller plus loin dans le cas où s n'est pas l'automorphisme identique ; on a en effet le résultat suivant :

Proposition 3. Soient Q une forme hermitienne, B une forme bilinéaire hermitienne associée à Q . Supposons que A n'ait aucun diviseur de zéro $\neq 0$, et que s ne soit pas l'automorphisme identique. On a alors $Q(x) = B(x,x)$ pour tout $x \in M$, et la condition $Q = 0$ entraîne $B = 0$.

Soient a,b des éléments de A ; on a d'une part

$$Q((a+b)x) = (a+b)Q(x)(a+b)^s = aQ(x)a^s+bQ(x)b^s + aQ(x)b^s + bQ(x)a^s$$

et d'autre part

$$Q((a+b)x) = aQ(x)a^s + bQ(x)b^s + aB(x,x)b^s + bB(x,x)a^s$$

puisque $B(x,x) = (B(x,x))^s$. Si donc nous posons $u = B(x,x)-Q(x)$, on a $aub^s + bua^s = 0$ quels que soient a,b . En particulier, $au+ua^s = 0$ pour tout $a \in A$; nous allons voir que ceci entraîne $u=0$. En effet, on a, pour a,b dans A , $bau = -bua^s = ub^sa^s$, et $abu = -u(ab)^s = -ub^sa^s$, d'où $(ba+ab)u = 0$. Si on avait $u \neq 0$, on aurait $ba+ab = 0$, d'où, en particulier, $a+a = 0$, et par suite $ba-ab = 0$; A serait commutatif de caractéristique 2 , et la relation $au+ua^s= 0$ entraînerait $(a-a^s)u = 0$, $a=a^s$, de sorte que s serait l'automorphisme identique. On a donc $B(x,x) = Q(x)$. Supposons maintenant $Q = 0$; on aurait $B(x,x)=0$ pour tout x , d'où $(B(x,y))^s = B(y,x) = -B(x,y)$ quels que soient x,y .

Posons $v = B(x,y)$; puisque $B(ax,y) = av$, on a $(av)^s = -av$, d'où $v^s a^s = -av$ pour tout $a \in A$; puisque $v^s = -v$, ceci donne $va^s = av$, d'où, pour a,b dans A , $bav = bva^s = vb^s a^s = v(ab)^s = abv$. Si donc v était $\neq 0$, on aurait $ab = ba$, A serait commutatif, et $(a-a^s)v = 0$, $a=a^s$, de sorte que s serait l'identité.

On voit donc que, si A ne possède pas de diviseur de zéro $\neq 0$ et si s est distinct de l'automorphisme identique, les formes B et Q se déterminent mutuellement. Par ailleurs, si s est l'automorphisme identique, on a $B(x,y) = Q(x+y)-Q(x)-Q(y)$, de sorte que la donnée de Q détermine alors toujours B .

<u>Proposition 4</u>. <u>Supposons que</u> s <u>soit l'automorphisme identique et que</u> M <u>possède une base finie</u>. <u>Si</u> Q <u>est une forme quadratique sur</u> M , <u>il existe toujours une forme bilinéaire</u> B_0, <u>non nécessairement symétrique, sur</u> M <u>telle que</u> $Q(x) = B_0(x,x)$ <u>pour tout</u> $x \in M$.

Soient $(x_1,\dots,x_n)$ une base de M et B la forme bilinéaire associée à Q . Définissons une forme bilinéaire B_0 sur M par les conditions $B_0(x_i,x_i) = Q(x_i)$, $B_0(x_i,x_j) = B(x_i,x_j)$ si $i < j$, $B_0(x_i,x_j) = 0$ si $i > j$. Tenant compte des formules $B(x,y) = Q(x+y)-Q(x)-Q(y)$, $Q(ax) = a^2 Q(x)$ $(x \in M$, $a \in A)$, on obtient facilement l'expression suivante de Q :

$$Q\Big(\sum_{i=1}^{n} a_i x_i\Big) = \sum_{i=1}^{n} a_i^2 Q(x_i,x_i) + \sum_{i<j} a_i a_j B(x_i,x_j) ;$$

or le second membre est manifestement $B_0\Big(\sum_{i=1}^{n} a_i x_i , \sum_{i=1}^{n} a_i x_i\Big)$.

Par ailleurs, si A est un corps de caractéristique $\neq 2$, toute forme hermitienne sur M peut se mettre sous la forme $x \to B_0(x,x)$ où B_0 est une forme bilinéaire hermitienne uniquement déterminée. En effet, il n'existe qu'une seule forme bilinéaire hermitienne B associée à Q ; nous prendrons $B_0 = B$ si s n'est pas l'automorphisme identique, $B_0 = (1/2)B$ dans le cas contraire. Le fait que B_0 est uniquement déterminée résulte

du fait que B_0 est associée soit à Q soit à $(1/2)Q$. Si on suppose de plus que M est de dimension finie, la matrice représentative de B_0 par rapport à une base de M s'appelle aussi la matrice représentative de Q par rapport à cette base, et le rang de B_0 s'appelle aussi le <u>rang de la forme hermitienne</u> Q .

Supposons maintenant que A soit un corps commutatif de caractéristique 2 , M un espace vectoriel de dimension finie sur K et Q une forme quadratique sur M . Soit N le conjugué de M par rapport à la forme bilinéaire B associée à Q ; si x,y sont dans N , on a $Q(x+y)=Q(x)+Q(y)$; c'est ce qu'on exprime en disant que la restriction de Q à N est <u>quasi-linéaire</u>. Il en résulte tout de suite que l'ensemble N' des $x \in N$ tels que $Q(x)=0$ est un sous-espace de N ; soient n' sa dimension et m celle de M ; c'est alors le nombre m-n' qu'on appelle le <u>rang de</u> Q. Si n est la dimension de N , le nombre n-n' s'appelle le <u>défaut</u> de Q . On observera que m-n est le rang de la forme bilinéaire B associée à Q , laquelle est alternée en vertu de la formule générale $B(x,x)= 2Q(x)$; m-n est donc un nombre pair.

Soient A un anneau commutatif et M un module à gauche sur A qui possède une base $(x_i)_{i \in I}$. Donnons-nous une application $i \to q_i$ de I dans A et une application $\{i,j\} \to b_{\{i,j\}}$ dans A de l'ensemble $\mathfrak{P}$ des parties à 2 éléments de I . Il existe alors une forme quadratique Q sur M et une seule telle que l'on ait $Q(x_i) = q_i$ $(i \in I)$ et $B(i,j)=B(j,i) = b_{\{i,j\}}$ pour tout $\{i,j\} \in \mathfrak{P}$, B étant la forme bilinéaire associée à Q . En effet, l'application Q définie par la formule

$$Q(\sum_{i\in I} a_i x_i) = \sum_{i\in I} q_i a_i^2 + \sum_{\{i,j\}\in P} b_{\{i,j\}}\, a_i a_j$$

est évidemment une forme quadratique qui possède les propriétés requises ; réciproquement, on voit facilement que, pour toute forme quadratique Q satisfaisant aux conditions imposées, $Q(\sum_{i\in I} a_i x_i)$ doit avoir l'expression donnée ci-dessus. On notera qu'il résulte de cette expression que, si I est fini, toute forme quadratique est une fonction polynome homogène de degré 2 sur M . Réciproquement, toute fonction polynome homogène de degré 2 sur un module quelconque M sur A est une forme quadratique ; il suffit en effet de la vérifier dans le cas du produit de deux formes linéaires, ce qui ne présente aucune difficulté.

Soit par ailleurs f un homomorphisme de A dans un anneau commutatif A' ; les données de f et de M définissent un module $M^{A'}$ sur A' et une application canonique de M dans $M^{A'}$ que nous désignerons encore par f ; puisque M est libre, il en est de même de $M^{A'}$, et les $f(x_i)$ forment une base de $M^{A'}$. Il existe alors une forme quadratique $Q^{A'}$ sur $M^{A'}$ et une seule telle que l'on ait $Q^{A'}(f(x)) = f(Q^{A'}(x))$ pour tout $x\in M$. En effet, cette condition entraîne que $Q^{A'}(f(x_i)) = f(q_i)$ et $B'(f(x_i),f(x_j)) = f(b_{\{i,j\}})$, où $\{i,j\}$ est un élément quelconque de P , $q_i = Q(x_i)$, $b_{\{i,j\}} = B(x_i,x_j) = B(x_j,x_i)$, B et B' étant les formes bilinéaires associées à Q et $Q^{A'}$; et, réciproquement, la forme quadratique $Q^{A'}$ définie par ces dernières conditions possède évidemment la propriété requise. On dit que $Q^{A'}$ est la forme quadratique sur $M^{A'}$ qui se déduit de Q par <u>transfert à A' de l'anneau de base</u> au moyen de l'homomorphisme f ; sa forme bilinéaire associée est celle qui se déduit de B par transfert à A' de l'anneau de base.

§ 2. FORMES ALTERNÉES.

n°1. REDUCTION.

Théorème 1. Soient A un anneau principal, M un module à gauche sur A qui possède une base finie et B une forme bilinéaire alternée sur M. Il existe alors une base de M de la forme $(x_1,\dots,x_r,y_1,\dots,y_r, z_1,\dots,z_s)$ telle que l'on ait

$$B(x_i,x_j) = B(y_i,y_j) = B(x_i,z_k) = B(y_j,z_k) = 0 \quad (1\leqq i,\ j\leqq r,\ 1\leqq k\leqq s),$$

$$B(x_i,y_i)=0 \text{ si } i\neq j \quad (1\leqq i,j\leqq r)\ ;\ B(x_i,y_i)=a_i \quad (1\leqq i\leqq r)$$

où les a_i sont des éléments $\neq 0$ de A et a_i divise a_{i+1} $(1\leqq i\leqq r)$. Le nombre $2r$ est le rang de B ; les idéaux Aa_i $(1\leqq i\leqq r)$ sont uniquement déterminés par la donnée de B.

Nous procèderons par récurrence sur le rang n de M. Il n'y a rien à démontrer si $n=0$. Supposons que $n>0$ et que le théorème soit vrai pour les modules de rangs $<n$. Le théorème est évident si $B=0$; supposons donc $B\neq 0$. Soient M^* le dual de M et f l'application de M dans M^* qui fait correspondre à tout $x\in M$ la forme linéaire $y\to B(x,y)$ sur M. L'ensemble $f(M)$ est un sous-module de M^*, qui est un module libre de rang n. Il existe donc une base $(u_1^*,\dots,u_n^*)$ de M^* telle que $f(M)$ soit engendré par les éléments $u_1^*b_1,\dots,u_n^*b_n$, $b_1,\dots,b_n$ étant des éléments de A tels que $Ab_1\supset Ab_2\supset\dots\supset Ab_n$ (th.1, VII, § 4, n°2). Puisque M possède une base finie, il s'identifie canoniquement à son bidual, et $(u_1^*,\dots,u_n^*)$ est la base d'une base $(u_1,\dots,u_n)$ de M. Soit x_1 un élément de M tel que $f(x_1)=u_1^*b_1$; posons $a_1=b_1$, $y_1=u_1$, d'où $B(x_1,y_1)=a_1$. Si x est un élément quelconque de M, $f(x)$ appartient à M^*b_1 (car $f(M)\subset M^*b_1$), d'où il résulte que, pour tout $y\in M$, $B(x,y)$ est un multiple de $Ab_1=a_1$. Puisque $B\neq 0$, on a $a_1\neq 0$.

Soit N le sous-module engendré par x_1, y_1, et soit P le conjugué de N. Montrons que M est somme directe de N et de P. Soit z un élément quelconque de M ; cherchons à déterminer des éléments a,b de A tels que $z-(ax_1+by_1)=z'$ appartienne à P. Il suffira que $B(x_1,z')=B(y_1,z')=0$, ce qui donne les conditions $B(x_1,z)-ba_1 = 0$, $B(y_1,z)+aa_1=0$. Ce système d'équations en a,b ne peut avoir plus d'une seule solution ; on en conclut que ax_1+by_1 ne peut être dans P que si $a=b=0$, ce qui montre que $N \cap P = \{0\}$ et que x_1, y_1 sont linéairement indépendants. De plus, nous avons vu que, quels que soient x,y dans M, $B(x,y)$ est divisible par a_1, ce qui montre que notre système d'équations a une solution, donc que $M = N+P$. Puisque x_1, y_1 sont linéairement indépendants, N est de rang 2 et P est par suite de rang n-2. Faisant usage de l'hypothèse inductive, on voit que P admet une base $(x_2,\dots,x_r,y_2,\dots,y_r,z_1,\dots,z_s)$ telle que l'on ait

$$B(x_i,x_j) = B(y_i,y_j) = B(x_i,z_k) = B(y_j,z_k)=0 \quad (2 \leqq i, j \leqq r, 1 \leqq k \leqq s)$$

$B(x_i,y_j)=0$ si $i \neq j$ $(2 \leqq i, j \leqq r)$; $B(x_i,y_i)=a_i$ $(2 \leqq i \leqq r)$

où les a_i sont des éléments $\neq 0$ et a_i divise a_{i+1} $(2 \leqq i < r)$. On a $B(x_1,x_i)=B(x_1,y_j)=B(x_1,z_k)=B(y_1,x_i)=B(y_1,y_j)=B(y_1,z_k)=0$ si $2 \leqq i,j \leqq r$, $1 \leqq k \leqq s$ parce que P est le conjugué de N. Puisque a_1 divise tous les éléments de la forme $B(x,y)$, a_1 divise a_2 si $i > 1$. Nous avons donc démontré l'existence d'une base possédant la propriété requise. Soit $(x_1^*,\dots,x_r^*,y_1^*,\dots,y_r^*,z_1^*,\dots,z_k^*)$ la base de M^* duale de la base que nous avons construite dans M. Il est alors clair que $f(x_i)= a_i y_i^*$, $f(y_i) = -a_i x_i^*$ $(1 \leqq i \leqq r)$, $f(z_k)=0$. Les facteurs invariants $Ae_1,\dots,Ae_n$ du sous-module $f(M)$ de M^* sont donc déterminés par les formules $Ae_{2p-1} = Ae_{2p} = Aa_p$ $(1 \leqq p \leqq r)$, $Ae_q = 0$ si $q > 2r$. On voit donc que le rang de B est 2r, et que les idéaux $Aa_1,\dots,Aa_r$ sont uniquement déterminés par la donnée de B.

Définition 1. Les notations étant celles du th.1, les idéaux Aa_i $(1 \leqq i \leqq r)$ sont appelés les diviseurs élémentaires de la forme B .

Supposons que, pour tout idéal $\mathfrak{a}$ de A on ait déterminé un élément $a(\mathfrak{a})$ de A qui l'engendre. On peut alors supposer, dans l'énoncé du th.1, que $a_i = a(Aa_i)$: si en effet $A(a_i) = u_i a_i$, les u_i étant des éléments inversibles de A, il suffit de remplacer les y_i par les éléments $y_i' = u_i y_i$. Si on a $a_i = a(Aa_i)$ $(1 \leqq i \leqq r)$, on dit que la base $(x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_k)$ est une base réduite de M relativement à B (et au choix des générateurs $a_i(\mathfrak{a})$).

Proposition 1. Soient A un anneau principal, M un module à gauche sur A qui possède une base finie et B une forme bilinéaire alternée sur M . Pour qu'une autre forme bilinéaire alternée sur M soit équivalente à B , il faut et suffit qu'elle ait mêmes diviseurs élémentaires que B .

La condition est manifestement nécessaire. Si elle est satisfaite, et si on choisit des bases réduites de M relativement à B et à B' (et à un choix de générateurs des idéaux principaux de A), les matrices qui représentent B et B' par rapport à ces bases sont identiques, ce qui montre que B,B' sont équivalentes.

Corollaire.- Soit M un espace vectoriel de dimension finie sur un corps commutatif. Pour que deux formes bilinéaires sur M soient équivalentes, il faut et suffit qu'elles aient même rang.

n° 2. PUISSANCES RÉDUITES.

Soient A un anneau commutatif, M un A-module à gauche et E l'algèbre tensorielle sur A . Désignons par E_p (resp.: E_i) le sous-module de E engendré par les éléments homogènes de degrés pairs (resp.: impairs) et par E_p^+ le sous-module de E_p engendré par les éléments homogènes de degrés pairs >0. L'ensemble E_p est donc une sous-algèbre du centre de E , et E_p^+ en est un idéal. Soit k un entier >1. On a alors $x^k = 0$ pour tout $x \in E_i$. Il suffit de le montrer dans le cas où $k=2$. Il est clair que x peut se mettre sous la forme $\sum_{i=1}^{h} x_i$, où les x_i sont des éléments décomposables de E_i ; on a $x_i \wedge x_i = 0$, $x_i \wedge x_j + x_j \wedge x_i = 0$ puisque x_i et x_j sont homogènes de degrés impairs, d'où $x^2=0$. Considérons maintenant x^k dans le cas où $x \in E_p^+$; nous allons voir que cet élément est multiple de k ! . Ecrivons $x = \sum_{i=1}^{h} x_i$, où les x_i sont des éléments décomposables de E_p ; puisque E_p est commutative, on peut calculer x^k par la formule du multinome. De plus, on a $x_i^m = 0$ si $m > 1$ puisque x_i est décomposable. Il vient donc

$$(1) \qquad x^k = (k!) \sum x_{i(1)} \cdots x_{i(k)}$$

où la somme est étendue à toutes les applications strictement croissantes $j \to i(j)$ de $\{1,\dots,k\}$ dans $\{1,\dots,h\}$.

Nous allons montrer qu'il est possible, d'une manière et d'une seule, de définir une application $(k,x) \to x^{(k)}$ de $\underline{\mathbb{N}} \times E_p^+$ dans E_p qui possède les propriétés suivantes :

a) on a $x^k = (k!)x^{(k)}$ pour tout $k \in \underline{\mathbb{N}}$ et tout $x \in E_p^+$;

b) on a $x^{(k)}=0$ si $k > 1$ et si x est un élément décomposable de E_p^+ ;

c) si x,y sont des éléments de E_p^+ , on a, pour $k \in \underline{\mathbb{N}}$,

$$(x+y)^{(k)} = \sum_{i=0}^{k} x^{(k-i)} \wedge y^{(i)} \quad .$$

Supposons définie une application qui possède ces propriétés. Il résulte de a) que $x^{(0)} = 1$, $x^{(1)} = x$. Il résulte facilement de c), par récurrence sur h , que, si $x_1, \ldots, x_h$ sont dans E_p^+ ,

$$(2) \quad (x_1 + \ldots + x_h)^{(k)} = \sum x_1^{(e(1))} \wedge \ldots \wedge x_h^{(e(h))} \quad ,$$

la sommation étant étendue à toutes les suites finies $(e(1), \ldots, e(h))$ d'entiers $\geqq 0$ telles que $e(1) + \ldots + e(h) = k$. Si x est décomposable, on a $x^{(k)} = 0$ pour tout $k > 1$; si donc les x_i sont des éléments décomposables de E_p^+ , $(x_1 + \ldots + x_h)^{(k)} = \sum_G \left(\prod_{i \in G} x_i \right)$, la sommation étant étendue à toutes les parties G de $\{1, \ldots, h\}$ qui contiennent k éléments. Puisque tout élément de E_p^+ est somme d'éléments décomposables de cet ensemble, on voit que l'application $(k,x) \to x^{(k)}$ est déterminée de manière unique. De plus, nous n'avons utilisé la condition a) que dans les cas $k = 0, 1$, et la formule à laquelle nous sommes arrivés pour $(x_1 + \ldots + x_h)^{(k)}$ dans le cas où les x_i sont décomposables montre que $x^k = (k!)\, x^{(k)}$ (cf. formule (1) ci-dessus). On voit donc qu'il suffit de postules a) pour les valeurs $k = 0, 1$.

Pour démontrer l'existence d'une application ayant les propriétés requises, nous considérerons d'abord le cas où le module M admet une base $(u_i)_{i \in I}$. Pour toute partie finie H de I , soit x_H un élément de E qui est le produit des u_i pour les $i \in H$, ces éléments ayant été rangés dans un ordre d'ailleurs arbitraire. Les x_H forment donc une base de E . Soit $\mathcal{H}$ l'ensemble de ceux des H qui ne sont pas vides et dont les nombres d'éléments sont pairs ; les x_H pour $H \in \mathcal{H}$ forment donc une base de E_p^+ . Pour tout $k \geqq 0$, soit $S(k)$ l'ensemble des parties finies à k éléments de $\mathcal{H}$. Soit $x = \sum_{H \in \mathcal{H}} a(H) x_H$ un élément quelconque de E_p^+ ; posons

$$x^{(k)} = \Sigma_{S \in \mathcal{S}(k)} \left(\prod_{H \in S} a(H)\right) \prod_{H \in S} x_H \ .$$

[Cette somme a un sens, car, si S_0 est l'ensemble fini des $H \in \mathcal{H}$ tels que $a(H) \neq 0$, on a $\prod_{H \in S} a(H) = 0$ si S n'est pas contenu dans S_0.]

Il est clair que $x^{(0)}=1$, $x^{(1)}=x$. Soit $y = \Sigma_{H \in \mathcal{H}} a'(H) x_H$ un nouvel élément de E^+_p. Développant le produit $\prod_{H \in S} (a(H)+a'(H))$, il vient

$$(x+y)^{(k)} = \Sigma_{S,S'} \left(\prod_{H \in S} a(H)\right)\left(\prod_{H \in S'} a'(H)\right) \prod_{H \in S} x_H \prod_{H \in S'} x_H \ ,$$

où la sommation est étendue aux couples de parties disjointes S,S' de $\mathcal{H}$ tels que $S \cup S'$ possède k éléments. Si S' est une partie de $\mathcal{H}$ contenant $1 \leqq k$ éléments, soit T(S') la somme des termes relatifs aux couples (S,S') possédant les propriétés requises et dont le second terme est S'. Si on observe que $x_H^2 = 0$ pour tout $H \in \mathcal{H}$, on voit que l'on peut laisser décrire à S tout l'ensemble $\mathcal{S}(k-1)$ sans modifier la somme T(S') ; on a donc $T(S') = x^{(k-1)} \prod_{H \in S'} a'(H) \prod_{H \in S'} x_H$. On en conclut tout de suite que $(x+y)^{(k)} = \sum_{\ell=0}^{k} x^{(k-1)} \wedge y^{(1)}$, ce qui montre que la condition c) est satisfaite. Il en résulte comme plus haut que la formule(2) est vraie et en particulier que si $x_i^{(2)} = 0$ $(1 \leqq i \leqq h)$, $(x_1+\ldots+x_h)^{(k)}$ appartient à l'idéal engendré par les produits de k éléments pris parmi $x_1,\ldots,x_h$. Il résulte immédiatement de notre définition de $x^{(k)}$ que si $x = \Sigma_{H \in \mathcal{H}} a(H) x_H$ est un élément de E^+_p multiple de l'un des éléments u_i, et si $k > 1$, on a $x^{(k)}=0$ (en effet, si x est multiple de u_i, $a(H)=0$ si i n'est pas dans H). Considérons maintenant un élément x de la forme $(\Sigma_{i \in I} a_i u_i) \wedge v$, où $v \in E_i$. Soit $k > 1$; puisque $(u_i \wedge v)^{(2)}=0$, $x^{(k)}$ appartient à l'idéal engendré par les produits de k éléments pris parmi les $u_i \wedge v$. Mais on a $v^2=0$, $(u_i \wedge v) \wedge (u_j \wedge v) = -u_i \wedge u_j \wedge v^2 = 0$, et par suite $x^{(k)}=0$.

On voit donc que $x^{(k)}=0$ toutes les fois que x est multiple d'un élément de M , donc, a fortiori, quand x est décomposable. Notre opération possède donc bien les propriétés requises. De plus, si I est l'idéal engendré dans E par un sous-module N de M , on a $x^{(k)} \in I$ pour tout $x \in E_p^+ \cap I$ si $k \geq 1$. Ecrivons en effet $x = \sum_{j=1}^{r} y_j \wedge v_j$, où les y_j sont dans N et les v_j dans E_i . Si $k=1$, $x^{(k)} = x$; si $k > 1$, les $(y_j \wedge v_j)^{(2)}$ étant nuls pour $\ell > 1$, $x^{(k)}$ appartient à l'idéal engendré par les produits de k des éléments $y_j \wedge v_j$, idéal qui est manifestement contenu dans I .

Passons maintenant au cas général. Il existe un module libre L sur A et une application linéaire f de L sur M . Soient E(L) l'algèbre extérieure de L , et $E_p(L)$, $E_p^+(L)$ les modules définis dans E(L) comme E_p, E_p^+ l'ont été dans E . L'application f se prolonge en une représentation de E(L) sur E , que nous désignerons encore par f ; f applique $E_p^+(L)$ sur E_p^+ . Si R est le noyau de l'application f de L sur M , le noyau de la représentation f de E(L) est l'idéal I engendré par R dans E(L). Soient x un élément de E_p^+ et X un élément de $E_p^+(L)$ tel que $f(X) = x$; k étant un entier ≥ 0 , montrons que $f(X^{(k)})$ ne dépend que de x , pas du choix de X . C'est évident si $k=0$; supposons que $k > 0$. Tout autre élément de $E_p^+(L)$ qui est appliqué sur x par f est de la forme $X+Y$, où $Y \in E_p^+(L) \cap I$. On a donc $Y^{(\ell)} \in I$ pour tout $\ell > 0$, et il résulte de la condition c) dans E(L) que $(X+Y)^{(k)} \equiv X^{(k)} \pmod{I}$, ce qui démontre notre assertion. Posons donc $x^{(k)} = f(X^{(k)})$. Si x est décomposable, on peut prendre pour X un élément décomposable ; il en résulte que les conditions a),b) c) sont satisfaites.

Nous appellerons puissance k-ième réduite d'un élément $x \in E_p^+$ l'image de cet élément par l'application $x \to x^{(k)}$ que nous venons de définir.

Si x est homogène de degré h , $x^{(k)}$ est homogène de degré hk . En effet, x peut alors s'écrire comme somme d'éléments homogènes décomposables de degré h, et $x^{(k)}$ est une somme de produits de k éléments homogènes de degré h .

Soit f une application linéaire de M dans un module à gauche M' sur A . Désignons encore par f la représentation de E(M) dans l'algèbre extérieure E(M') de M' qui prolonge f . Si $x \in E_p^+$, on a, pour tout $k \geq 0$, $f(x^{(k)}) = (f(x))^{(k)}$. Mettons en effet x sous la forme $x = x_1 + \ldots + x_h$, les x_i étant des éléments décomposables homogènes de degrés pairs ; on a $f(x)=f(x_1)+\ldots+f(x_h)$, et les $f(x_i)$ sont homogènes, décomposables et de degrés pairs. On a $x^{(k)} = \sum_G \prod_{i \in G} x_i$, $(f(x))^{(k)} = \sum_G \prod_{i \in G} f(x_i)$, G décrivant l'ensemble des parties à k éléments de $\{1,\ldots,h\}$, ce qui démontre notre assertion.

n°3. LE PFAFFIEN.

Soient K un corps commutatif et M un espace vectoriel de dimension finie paire 2n sur K . On désignera par M^* le dual de M , par $E(M)$ et $E(M^*)$ les algèbres extérieures de M et M^*, par $E^h(M)$ et $E^h(M^*)$ les espaces d'éléments homogènes de degré h de $E(M)$, $(E(M^*)$, par $(x,x^*) \to \langle x,x^* \rangle$ la forme bilinéaire canonique sur $E(M) \times E(M^*)$. Soit B une forme bilinéaire alternée sur M ; B définit donc une forme linéaire sur $E^2(M)$, et on sait qu'il y a un élément uniquement déterminé β de $E^2(M^*)$ tel que

$$B(x,y) = \langle x \wedge y , \beta \rangle$$

quels que soient x et y dans M ; β s'appelle l'<u>élément représentatif</u> de la forme bilinéaire B . La puissance n-ième réduite $\beta^{(n)}$ de β est un élément de l'espace vectoriel $E^{2n}(M^*)$, qui est de dimension 1 ; cet élément s'appelle le pfaffien de la forme bilinéaire B .

Soit maintenant $(x_1,\dots,x_{2n})$ une base de M , et soit $\underline{B} = (b_{ij})$ la matrice qui représente B par rapport à cette base. Soit $(x_1^*,\dots,x_{2n}^*)$ la base de M^* duale de la base $(x_1,\dots,x_{2n})$ de M . Si $i<j$, $k<\ell$ on a $\langle x_i \wedge x_j , x_k^* \wedge x_\ell^* \rangle = \delta_{ik}\,\delta_{j\ell}$; il en résulte tout de suite que

$$\beta = \sum_{k<\ell} x_k^* \wedge x_\ell^* \; b_{k\ell} \; .$$

On en déduit l'expression du pfaffien de B :

$$\beta^{(n)} = \sum_S \Big(\prod_{(k,\ell)\in S} x_k^* \wedge x_\ell^* \Big) \cdot \prod_{(k,\ell)\in S} b_{k\ell}$$

où S décrit tous les ensembles de n couples (k,ℓ) d'entiers tels que $1 \leqq k < \ell \leqq n$. Soit $e^* = x_1^* \wedge \dots \wedge x_{2n}^*$; pour tout ensemble $S = \{(k_1,\ell_1),\dots,(k_n,\ell_n)\}$, on a $\prod_{(k,\ell)\in S} x_k^* \wedge x_\ell^* = f(S)e^*$, où $f(S)$ est un entier rationnel égal à 0 si l'ensemble $\{k_1,\ell_1,\dots,k_n,\ell_n\}$ n'est pas $\{1,\dots,2n\}$ tout entier, et égal dans

le cas contraire à 1 ou à -1 suivant que la permutation qui applique k_i sur $2i-1$, ℓ_i sur $2i$ $(1 \leqq i \leqq n)$ est paire ou impaire. Introduisons $n(2n-1)$ indéterminées $X_{k\ell}$ indexées au moyen des couples (k,ℓ) tels que $1 \leqq k < \ell \leqq 2n$, et posons

$$P(..,X_{k\ell},...) = \Sigma_S f(S) \prod_{(k,\ell)\in S} X_{k\ell} .$$

Si $\underline{A} = (a_{ij})$ est une matrice alternée à éléments dans un anneau commutatif quelconque, l'élément $P(...,a_{k\ell},...)$ obtenu en substituant aux $X_{k\ell}$ dans P les éléments $a_{k\ell}$ de $\underline{A}$ d'indices k,ℓ tels que $k<\ell$ s'appelle le <u>pfaffien de la matrice A</u>, et se désigne par $Pf(\underline{A})$. Revenant aux notations utilisées plus haut, on voit que $\beta^{(n)} = e^*.Pf(\underline{B})$.

<u>Proposition 2.</u> <u>Soit A une matrice alternée à</u> 2n <u>lignes et colonnes à éléments dans un anneau commutatif</u> A, <u>et soit</u> $\underline{R} = (r_{ij})$ <u>une matrice carrée quelconque à</u> 2n <u>lignes et colonnes et à éléments dans</u> A. <u>La matrice</u> ${}^t\underline{R}.\underline{A}.\underline{R}$ <u>est alors alternée, et son pfaffien est</u> $(\det \underline{R}).Pf(\underline{A})$. <u>On a</u> $\det \underline{A} = (Pf(\underline{A}))^2$.

Il existe des polynomes A'_{ij} $(1 \leqq i, j \leqq 2n)$ en $2(2n)^2$ indéterminées $Y_{k\ell}, Z_{k\ell}$ $(1 \leqq k, \ell \leqq 2n)$, à coefficients entiers rationnels, tels que les coefficients de ${}^t\underline{R}.\underline{A}.\underline{R}$ soient les éléments $A'_{ij}(...,a_{k\ell},...,r_{k\ell},...)$. En vertu du principe de permanence des identités algèbriques, il suffira donc de démontrer la prop. dans le cas où A est un corps K et où $\det \underline{R} \neq 0$. Soient alors M un espace vectoriel de dimension 2n sur K, et $(x_1,...,x_{2n})$ une base de M. Relativement à cette base, $\underline{A}$ représente une matrice forme bilinéaire alternée B sur M. Par ailleurs, $\underline{R}$ est la matrice de transition de $(x_1,...,x_{2n})$ à une autre base $(y_1,...,y_{2n})$. La matrice ${}^t\underline{R}.\underline{A}.\underline{R}$ est

celle qui représente B par rapport à la base $(y_1,\dots,y_{2n})$ et est par suite alternée. Soient $(x_1^*,\dots,x_{2n}^*)$ et $(y_1^*,\dots,y_{2n}^*)$ les bases du dual M^* de M duales de $(x_1,\dots,x_{2n})$ et $(y_1,\dots,y_{2n})$; soit $e^* = x_1^* \wedge \dots \wedge x_{2n}^*$, $f^* = y_1^* \wedge \dots \wedge y_{2n}^*$. La matrice de transition de $(y_1^*,\dots,y_{2n}^*)$ à $(x_1^*,\dots,x_{2n}^*)$ est donc ${}^t\underline{R}$, d'où $e^* = f^* (\det {}^t\underline{R}) = f^*(\det \underline{R})$. Par ailleurs, le pfaffien de B est e^* Pf($\underline{A}$) et aussi f^* (Pf ${}^t\underline{R}.\underline{A}.\underline{R}$), d'où Pf (${}^t\underline{R}.\underline{A}.\underline{R}$) = (Pf $\underline{A}$) (det $\underline{R}$) . Soit par ailleurs 2r le rang de B ; il résulte du th.1, n°1 qu'il y a une base $(z_1,\dots,z_{2n})$ de M telle que

$$B(z_{2i-1},z_{2i})=1 \quad , \quad B(z_{2i},z_{2i-1}) = -1 \quad (1 \leqq i \leqq r)$$

et $B(z_k,z_l)=0$ si (k,l) n'est pas de l'une ou l'autre des formes $(2i-1,2i)$ ou $(2i,2i-1)$, avec un $i \leqq r$. La matrice $\underline{B}$ qui représente B par rapport à cette base est donc

$$\begin{pmatrix} J & 0 & \dots & 0 & \dots & 0 & \dots \\ 0 & J & \dots & 0 & \dots & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & J & \dots & 0 & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots \end{pmatrix}$$

où J est la matrice

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

Il en résulte immédiatement que $\det \underline{B} = 1$ si $r=n$, $\det \underline{B} = 0$ si $r < n$. Soit $(z_1^*,\dots,z_{2n}^*)$ la base duale de $(z_1,\dots,z_{2n})$; l'élément représentatif de B est alors $\sum_{i=1}^{r} z_{2i-1}^* z_i^*$. Si on pose $g^* = z_1^* \wedge \dots \wedge z_{2n}^*$, on voit tout de suite que le pfaffien de B est g^* si $r=n$, 0 si $r < n$. Le pfaffien de $\underline{B}$ est donc 1 ou 0 suivant que

$r=n$ ou $r < n$. Soit maintenant $\underline{T}$ la matrice de transition de la base $(z_1,\ldots,z_{2n})$ à la base $(x_1,\ldots,x_{2n})$. On a donc $\underline{A} = {}^t\underline{T}.\underline{B}.\underline{T}$, d'où $\mathrm{Pf}\ (\underline{A}) = (\det \underline{T})\ \mathrm{Pf}\ (\underline{B})$ et $\det \underline{A} = (\det \underline{T})^2\ (\det \underline{B})$ ce qui montre que $\det \underline{A} = (\mathrm{Pf}\ (\underline{A}))^2$. La prop.2 est ainsi démontrée.

Proposition 3. Soit A une matrice alternée à éléments dans un anneau commutatif A . Si le nombre de lignes de $\underline{A}$ est impair, on a $\det(\underline{A})=0$. Si ce nombre est pair, $\det \underline{A}$ est le carré d'un élément de A ; et, si A est un corps, une condition nécessaire et suffisante pour que $\underline{A}$ soit inversible est que $\mathrm{Pf}\ (\underline{A}) \neq 0$.

Supposons d'abord que le nombre de lignes de $\underline{A}$ soit impair. Le déterminant de $\underline{A}$ pouvant s'exprimer comme un polynome à coefficients entiers rationnels en les éléments de A , pour démontrer que $\det \underline{A} = 0$, il suffit de considèrer le cas où A est un corps. Soit alors n le nombre de lignes de $\underline{A}$; soit M un espace vectoriel de dimension n sur A , et soit $(x_1,\ldots,x_n)$ une base de cet espace. La matrice $\underline{A}$ représente par rapport à cette base une forme bilinéaire B sur M . Le rang de B , étant pair, est $< n$, ce qui montre que $\det \underline{A} = 0$. Les autres assertions de la prop.3 résultent immédiatement de la prop.2 .

§ 3. CAS OU L'ANNEAU DE BASE EST UN CORPS.

Dans ce § , on désignera par K un corps, par s un antiautomorphisme de K dont le carré est l'identité, par M un duomodule sur K attaché à l'antiautomorphisme s et de dimension finie. On désignera par B une forme bilinéaire sur M , donc on supposera qu'elle est non dégénérée et soit hermitienne soit alternée (le second cas ne pouvant se produire que si s est l'automorphisme identique et K commutatif).

On supposera de plus que la condition suivante est satisfaite :

D. si x est un élément quelconque de M , il existe un $a \in K$ tel que $B(x,x) = a+a^s$.

Cette condition est toujours satisfaite si K n'est pas de caractéristique 2 ; car, puisque $B(x,x) = (B(x,x))^s$, on peut prendre $a = (1/2)B(x,x)$. Supposons K de caractéristique 2 . La condition D . est satisfaite trivialement si B est alternée ; réciproquement, dans ce cas, la condition D. implique que s ne peut être l'automorphisme identique que si B est alternée. Enfin, la condition D. est satisfaite s'il existe un sous-corps commutatif L de K qui possède les propriétés suivantes : on a $L^s = L$, mais s ne laisse pas tous les éléments de L fixes ; on a $B(x,x) \in L$ pour tout $x \in M$. En effet, B(x,x) appartient alors toujours au sous-corps L_0 des éléments de L invariants par s , et, L étant une extension quadratique séparable de L_0, tout élément de L_0 est trace de L à L_0 d'un élément de L .

Tout espace vectoriel à gauche ou à droite sur K pouvant être muni d'une structure de duomodule attaché à s et d'une seule, nous emploierons librement la terminologie de la théorie des espaces vectoriels même quand il s'agira de duomodules.

Rappelons les faits suivants, qui seront utilisés constamment et qui résultent du fait que B est non dégénérée. Si M est de dimension m et si N est un sous-espace de dimension n de M , le conjugué N' de N est de dimension m-n. Si N n'est pas isotrope, N' n'est pas isotrope, et M est somme directe de N et de N'.

n° 1. FORMES NORMALES.

Proposition 1. Soient N un sous-espace totalement isotrope de M et $(x_1,\dots,x_r)$ une base de N. Il existe alors un sous-espace totalement isotrope P de M et une base $(y_1,\dots,y_r)$ de P tels que l'on ait $B(x_i,y_j) = \delta_{ij}$ $(1 \leqq i, j \leqq r)$. La somme N+P est directe, et la restriction de B à N+P est non dégénérée.

Nous allons construire les éléments y_i par récurrence. Supposons déjà construits des éléments y_j pour $j < i$, où i est un indice entre 1 et r, de telle manière que $B(x_k,y_j) = \delta_{kj}$ pour $1 \leqq k \leqq r$, $j < i$ et $B(y_j,y_{j'})=0$ pour $j,j' < i$. Les éléments $x_1,\dots,x_r,y_j$ $(j < i)$ sont linéairement indépendants. Supposons en effet que l'on ait $y = \sum_{k=1}^{r} c_k x_k + \sum_{j<i} d_j y_j = 0$, les c_k, d_j étant dans K. Il vient $0 = B(y,x_j) = d_j$ $(j < i)$ et par suite $c_1=\dots=c_r=0$ puisque $x_1,\dots,x_r$ sont linéairement indépendants. Pour tout $x \in M$, soit $f(x)$ la forme linéaire $y \to B(x,y)$ sur M_d ; puisque B est non dégénérée, f est un isomorphisme de M_g sur le dual de M_d, et les formes $f(x_k)$ $(1 \leqq k \leqq r)$, $f(y_j)$ $(j < i)$ sont linéairement indépendantes. Il existe donc un $y_i' \in M$ tel que $\langle f(x_k), y_i' \rangle = \delta_{ki}$ $(1 \leqq k \leqq r)$, $\langle f(y_j), y_i' \rangle = 0$ $(j < i)$. Il existe par hypothèse un élément $a_i \in K$ tel que $B(y_i', y_i') = a_i + a_i^s$. Posons $y_i = y_i' - x_i a_i$. Puisque N est totalement isotrope, on a $B(x,y_i) = B(x,y_i')$ pour $x \in N$, d'où $B(x_k,y_i) = \delta_{ki}$ $(1 \leqq k \leqq r)$; puisque $B(x_i,y_j)=0$ pour $j < i$, on a aussi alors $B(y_j,x_i)=0$ et $B(y_j,y_i) = B(y_j,y_i')=0$. Si B est alternée, on a $B(y_i,y_i)=0$. Si B est hermitienne, on a $B(y_i',x_i) = (B(x_i,y_i'))^s = 1$ et $B(y_i,y_i) = B(y_i',y_i') - B(y_i',x_i a_i) - B(x_i a_i,y_i') = B(y_i',y_i') - a_i - a_i^s = 0$, et y_i possède les propriétés requises. Il y a donc des éléments $y_1,\dots,y_r$

tels que $B(x_i,y_j) = \delta_{ij}$, $B(y_i,y_j)=0$ $(1 \leqq i, j \leqq r)$. L'espace P engendré par $y_1,\dots,y_r$ est manifestement totalement isotrope. Soient a_i,b_i $(1 \leqq i \leqq r)$ des éléments de K tels que $x = \sum_{i=1}^{r} a_i x_i + \sum_{i=1}^{r} b_i y_i$ soit dans le conjugué de N+P. On a alors $0 = B(x,y_i) = a_i$, $0 = B(x_i,x) = b_i$ $(1 \leqq i \leqq r)$. Il en résulte que la restriction de B à N+P est non dégénérée et que $x_1,\dots,x_r,y_1,\dots,y_r$ sont linéairement indépendants, donc que $y_1,\dots,y_r$ forment une base de P et que la somme N+P est directe.

Remarque. Supposons que N soit totalement isotrope maximal. La prop.1 montre qu'il existe un sous-espace totalement isotrope P de dimension r tel que $N \cap P = \{0\}$. Si P est un espace quelconque possédant ces propriétés, il existe une base $(y_1,\dots,y_r)$ de P telle que $B(x_i,y_j) = \delta_{ij}$ $(1 \leqq i, j \leqq r)$. Désignons en effet, si $y \in P$, par $g(y)$ la restriction à N de la forme linéaire $x \to B(x,y)$. Si $g(y)=0$, y est un élément isotrope du conjugué de N, donc appartient à N, ce qui entraîne $y=0$ puisque $N \cap P = \{0\}$. Il en résulte que g est un isomorphisme de P_d sur le dual de N_g, et par suite qu'il y a une base $(y_1,\dots,y_r)$ de P telle que $B(x_i,y_j) = \delta_{ij}$.

Proposition 2. Supposons la forme B non alternée. Il y a alors une base de M telle que la matrice qui représente B par rapport à cette base soit diagonale. Tout ensemble maximal d'éléments non isotropes mutuellement conjugués de M est une pareille base.

Soient $x_1,\dots,x_h$ des éléments non isotropes mutuellement conjugués de M, et soit X l'espace engendré par ces éléments. Si les a_i sont des éléments de K tels que $x = \sum_{i=1}^{r} a_i x_i$ soit dans le conjugué de X, on a $0 = B(x,x_i) = a_i B(x_i,x_i)$ d'où $a_i=0$ $(1 \leqq i \leqq h)$.

Ceci montre que $x_1,\dots,x_h$ forment une base de X (donc que h est au plus égal à la dimension de M) et que la restriction de B à X est non dégénérée. Supposons maintenant que $\{x_1,\dots,x_h\}$ soit maximal dans l'ensemble des ensembles d'éléments non isotropes mutuellement conjugués, et soit X' le conjugué de X . Il est clair que X' ne contient aucun élément non isotrope ; de plus, la restriction de B à $X' \times X'$ est non dégénérée. Si donc X' est totalement isotrope, on a $X'=\{0\}$, et la prop.2 est vraie. Or, X' est bien totalement isotrope en vertu du

Lemme 1. Soit B non alternée. Tout sous-espace N de M dont tous les éléments sont isotropes est totalement isotrope.

Supposons en effet qu'il n'en soit pas ainsi. Si x_0,y_0 sont des éléments de N tels que $B(x_0,y_0) \neq 0$, la formule $B(ax_0,y_0)= aB(x_0,y_0)$ montre que, pour tout $b \in K$, il y a des éléments x,y de N tels que $B(x,y) = b$. Or les relations $B(x,x) = B(y,y) = B(x+y, x+y)=0$ entraînent $B(x,y) + B(y,x) = 0$, d'où $b^s = B(y,x) = -B(x,y) = -b$. Appliquent ceci au cas où b=1, on voit que K est de caractéristique 2 . On a donc $b^s = b$ pour tout $b \in K$, et s est l'application identique. Or, pour tout $u \in M$, $B(u,u)$ se met sous la forme $c + c^s = 2c = 0$, et B est alternée, contrairement à l'hypothèse.

Théorème 2. Les conditions énoncées au début de ce § étant supposées satisfaites, tous les sous-espaces totalement isotropes maximaux de M ont même dimension r . Soit N l'un de ces espaces, et soit $(x_1,\dots,x_r)$ une base de N . Il existe alors une base de M de la forme $(x_1,\dots,x_r,y_1,\dots,y_r,z_1,\dots,z_q)$ par rapport à laquelle la matrice représentative de B est de la forme

$$\begin{matrix} 0 & I_r & 0 \\ eI_r & 0 & 0 \\ 0 & 0 & D \end{matrix}$$

où I_r est la matrice unité de degré r , e est -1 si B est alternée, 1 dans le cas contraire, q=0 si B est alternée, et, sinon, D est une matrice diagonale inversible. De plus, l'espace de base $(z_1,\dots,z_q)$ ne contient aucun vecteur isotrope $\neq 0$.

Soient P un sous-espace totalement isotrope et $(y_1,\dots,y_r)$ une base de P qui possèdent les propriétés énoncées dans la prop.1 . Soit Q le conjugué de N+P , t soit q sa dimension. La restriction de B à $(N+P)\times(N+P)$ étant non dégénérée, il en est de même de sa restriction à $Q\times Q$, et N est somme directe de N+P et de Q . Le conjugué de N contient N+Q et est de dimension $(2r+q)-r = r+q$ égale à celle de N+Q ; ce conjugué est donc N+Q . Puisque N est totalement isotrope maximal, tout élément isotrope du conjugué de N est dans N , et Q ne contient aucun élément isotrope $\neq 0$. Il existe en vertu de la prop.2 une base $(z_1,\dots,z_q)$ de Q telle que la matrice représentative par rapport à cette base de la restriction de B à $Q\times Q$ soit diagonale. Il est clair que $(x_1,\dots,x_r,y_1,\dots,y_r,z_1,\dots,z_q)$ est une base de M et que la matrice qui représente B par rapport à cette base a la forme indiquée. Soit maintenant N' un sous-espace totalement isotrope maximal de M , et soient r',p les dimensions de N', $N\cap N'$. Soit N_1 un supplémentaire de $N\cap N'$ dans N ; N_1 est de dimension r-p, et son conjugué X est de codimension r-p ; $X\cap N'$ est donc de dimension $\geq r'-(r-p) = r'-r+p$. L'espace $X\cap N'$ contient $N\cap N'$ puisque N est totalement isotrope. Si $u\in X\cap N'$, u est dans le conjugué de $N\cap N'$ puisque $u\in N'$ et que N' est totalement isotrope ; x est aussi dans

le conjugué de N_1, donc dans celui de $N \cap N' + N_1 = N$. Puisque $u \in N'$, u est isotrope ; étant dans le conjugué de N, il est dans N, d'où $X \cap N' = N \cap N'$ et par suite $r' - r \leqq 0$. Comme N était un sous-espace totalement isotrope maximal quelconque, il en résulte que tous les sous-espaces totalement isotropes maximaux ont même dimension.

Définition 1. On appelle indice de la forme B la dimension commune de tous les sous-espaces totalement isotropes maximaux de M.

Il résulte donc du th.2 que l'indice de B est au plus égal à la moitié de la dimension de M.

Définition 2. On dit qu'une base $(x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_q)$ de M est normale si r est l'indice de B et si la matrice représentative de B par rapport à cette base est de la forme indiquée dans l'énoncé du th.2.

Ces conditions étant supposées satisfaites, soit Q l'espace engendré par $z_1, \ldots, z_q$. Alors la restriction de B à $Q \times Q$ est non dégénérée d'indice 0. En effet, la matrice D doit être inversible puisque B est non dégénérée. De plus, si z est un élément isotrope de Q, z est dans le conjugué de l'espace N engendré par $x_1, \ldots, x_r$; N étant totalement isotrope maximal, on a $z=0$.

Remarque. Dans le cas des formes alternées, le th.2 redonne le cas particulier du th.1, § 2, n°1 relatif au cas où l'anneau de base est un corps.

Proposition 3. Supposons que K soit commutatif et algèbriquement clos et que s soit l'automorphisme identique. Si, r est l'indice de B, la dimension de M est $2r$ ou $2r+1$. Si elle est $2r+1$, il y a une base normale $(x_1, \ldots, x_r, y_1, \ldots, y_r, z)$ telle que $B(z,z)=1$.

Utilisant les notations du th.2, nous allons montrer qu'il est impossible que $q > 1$. Supposons en effet que $q > 1$. Si $a \in K$, on a $B(z_1+az_2, z_1+az_2) = b_1 + a^2 b_2$, si $b_1 = B(z_1, z_1)$. Or, puisque $b_2 \neq 0$ et K est algébriquement clos, il y a un $a \in K$ tel que z_1+az_2 soit isotrope, ce qui est impossible. Soit de plus c_1 tel que $c_1^2 = B(z_1, z_1)$; si $q=1$, on a $B(c_1^{-1}z_1, c_1^{-1}z_1) = 1$.

Corollaire. Si K est commutatif et algébriquement clos, toutes les formes bilinéaires symétriques non dégénérées sur M sont équivalentes.

Cela résulte immédiatement de la prop.3 .

n°2. APPLICATION AUX FORMES HERMITIENNES ET QUADRATIQUES.

Soit maintenant Q une forme hermitienne sur M , associée à la forme bilinéaire B . Si B est alternée, s est l'automorphisme identique et la formule $2Q(x) = B(x,x)$ montre que $Q = 0$, d'où $B=0$ et $M = \{0\}$. La prop.2 n°1 donne donc le résultat suivant :

Proposition 4. Si s n'est pas l'automorphisme identique ou si K n'est pas de caractéristique 2, il existe une base $(x_1,\dots,x_n)$ de M telle que l'on ait

$$Q(\sum_{i=1}^{m} a_i x_i) = \sum_{i=1}^{m} a_i q_i a_i^s ,$$

quels que soient les a_i dans K , les q_i étant des éléments de K invariants par s .

On a en effet $Q(x) = B(x,x)$ si s n'est pas l'automorphisme identique (prop.3, § 1,n°2) et $Q(x) = (1/2)B(x,x)$ dans le cas contraire, il suffit donc de prendre pour $(x_1,\dots,x_m)$ une base de M composée de vecteurs non isotropes mutuellement conjugués par rapport à B .

De même, il résulte du th.2, n°1 que l'on a la

Proposition 5. Les hypothèses étant les mêmes que celles de la prop.4, il existe une base $(x_1,\dots,x_r,y_1,\dots,y_r,z_1,\dots,z_q)$ de M qui possède les propriétés suivantes : on a

$$Q(\sum_{i=1}^{r} (a_i x_i + b_i y_i) + \sum_{j=1}^{q} c_j z_j) = \sum_{i=1}^{r} (a_i b_i^s + b_i a_i^s) + \sum_{j=1}^{q} c_j q_j c_j^s$$

si s n'est pas l'automorphisme identique, et

$$Q(\sum_{i=1}^{r} (a_i x_i + b_i y_i) + \sum_{j=1}^{q} c_j z_j) = \sum_{i=1}^{r} a_i b_i + \sum_{j=1}^{q} q_j c_j^2$$

dans le cas contraire ; dans ces formules, les a_i, b_i, c_j représentent des éléments quelconques de K et les q_j sont dans K et invariants par s ; de plus, la relation $Q(\sum_{j=1}^{q} c_j x_j)=0$ entraîne $c_j=0$ $(1 \leqq j \leqq q)$.

De plus, on a le résultat suivant :

Proposition 6. Supposons que K soit un corps commutatif algèbriquement clos de caractéristique 2 et que s soit l'automorphisme identique. Il existe alors une base $(x_1,\dots,x_r,y_1,\dots,y_r)$ de M telle que l'on ait

$$Q(\sum_{i=1}^{r}(a_ix_i + b_iy_i) = \sum_{i=1}^{r} a_ib_i$$

quels que soient les a_i,b_i dans K .

Pour l'établir, nous allons montrer qu'il existe deux sous-espaces totalement isotropes supplémentaires N et P de M tels que Q s'annulle identiquement sur chacun de ces espaces. Supposons que l'on ait deux sous-espaces totalement isotropes N_o et P_o de même dimension p qui possèdent les propriétés suivantes : Q s'annulle identiquement sur chacun de ces espaces et N_o+P_o n'est pas isotrope. On a alors $N_o \cap P_o = \{0\}$; si $N_o+P_o \neq M$, soit Q_o le conjugué de cet espace, qui est $\neq \{0\}$ et non isotrope. Puisque B est alternée, Q_o contient deux vecteurs z_1,z_1' tels que $B(z_1,z_1') \neq 0$. Le corps K étant algèbriquement clos, on voit tout de suite qu'il existe des éléments a,b tous deux nuls de K tels que l'on ait $Q(az_1+bz_1') = Q(z_1)a^2 + B(z_1,z_1')ab + Q(z_1')b^2 = 0$; soit $z = az_1+bz_1'$, et soit z_2' un vecteur de Q_o tel que $B(z,z_2')= 1$. Posons $z'= z_2'-Q(z_2')z$: on vérifie alors tout de suite que $Q(z')=0$, $B(z,z')=1$. Posons $N_1=N_o+Kz$, $P_1=P_o+Kz'$. Si $x\in N_o$, $k\in K$, on a $Q(x+kz) = Q(x) + kB(x,z) + k^2Q(z) = 0$; Q est donc nulle sur N_1 , ce qui entraîne que N_1 est totalement isotrope ; on voit de même que Q est nulle sur P_1 et que P_1 est totalement isotrope. Les espaces N_1 et P_1 sont de dimension p+1 . Un élément u de N_1+P_1 qui est aussi dans le conjugué de cet espace appartient à $Q_o \cap (N_1+P_1) = Kz+Kz'$; mais, puisque $B(z,z')=1$, $Kz+Kz'$ n'est évidemment pas isotrope, d'où $u=0$: N_1+P_1 n'est pas isotrope. Répétant un certain nombre de fois cette construction à partir du couple $N_o=\{0\}$, $P_o=\{0\}$, on obtient finalement deux

sous-espaces totalement isotropes supplémentaires N et P sur chacun desquels Q est identiquement nulle. Si $(x_1,\dots,x_r)$ est une base de N, il y a une base $(y_1,\dots,y_r)$ de P telle que $B(x_i,y_j) = \delta_{ij}$ $(1 \leqq i, j \leqq r)$, et la base $(x_1,\dots,x_r,y_1,\dots,y_r)$ de M possède évidemment la propriété requise.

Dans le cas où s n'est pas l'automorphisme identique ou K n'est pas de caractéristique 2, on définit l'<u>indice</u> de la forme hermitienne Q comme étant égal à celui de la forme bilinéaire B associée à Q. Par contre, si Q est une forme quadratique et si K est de caractéristique 2, il convient de donner une définition différente de l'indice de Q : c'est ce que nous ferons au § suivant.

§ 3. LE GROUPE D'UNE FORME BILINÉAIRE.

n°1. DÉFINITION. REPRÉSENTATION PARAMÉTRIQUE DE CAYLEY.

Définition 1. Soit B une forme bilinéaire sur un duomodule M . On appelle automorphisme de la forme B tout automorphisme u de la structure de duomodule de M tel que l'on ait $B(u.x,u.y) = B(x,y)$ quels que soient x,y dans M . Ces automorphismes forment évidemment un groupe ; ce groupe s'appelle le groupe de la forme B .

Supposons que M soit attaché à un antiautomorphisme s de son anneau de base A et possède une base finie $(x_1,\dots,x_n)$; soit $\underline{B}$ la matrice qui représente B par rapport à cette base. Soit u un automorphisme de M ; considéré comme automorphisme de M_d , il est représenté par une matrice $\underline{U}$ relativement à la base $(x_1,\dots,x_n)$. Si on pose $u.x_i = y_i$ $(1 \leqq i \leqq n)$, $y_1,\dots,y_n$ forment une nouvelle base de M , et $\underline{U}$ est la matrice de transition de $(x_1,\dots,x_n)$ à $(y_1,\dots,y_n)$ dans M_d . Pour que u soit un automorphisme de la forme B , il est nécessaire et suffisant que la matrice qui représente B par rapport à la base $(y_1,\dots,y_n)$ soit égale à $\underline{B}$. Mais cette matrice est ${}^t\underline{U}^s.\underline{B}.\underline{U}$, d'où la condition

$$ {}^t\underline{U}^s.\underline{B}.\underline{U} = \underline{B} \ .$$

Proposition 1. Soit M un duomodule sur un anneau commutatif A ; supposons que M soit attaché à un automorphisme s de A et possède une base finie. Soit B une forme bilinéaire non dégénérée sur M . Si d est le déterminant d'un automorphisme u de la forme B , on a $dd^s = 1$.

Utilisant les mêmes notations que plus haut, la relation ${}^t\underline{U}^s.\underline{B}.\underline{U} = \underline{B}$ entraîne en effet $d^s d \ (\det \underline{B}) = \det \underline{B}$, d'où le résultat puisque $\det \underline{B} \neq 0$.

Soit B une forme bilinéaire non dégénérée sur un duomodule M .

Soit u un automorphisme du duomodule M . Pour que u soit un automorphisme de la forme B , il faut et suffit que l'on ait $B(u.x,y) = B(x, {}^{-1}u.y)$ quels que soient x,y dans M , donc que ${}^{-1}u$ soit l'adjoint de u (u étant considéré comme automorphisme de M_g).

Supposons maintenant que M soit attaché à un antiautomorphisme s de son anneau de base et que B soit ou hermitienne (relativement à s) ou alternée. Ceux des automorphismes de M qui admettent des adjoints qui sont également des automorphismes forment alors un groupe Γ , et l'application $u \to {}^{-1}u^*$ est un automorphisme d'ordre 2 de Γ . Le groupe de la forme B est le groupe des éléments de Γ invariants par cet automorphisme. On en déduit le résultat suivant :

Proposition 2. Soient K un corps, s un antiautomorphisme de K , M un duomodule sur K attaché à s qui possède une base finie, B une forme bilinéaire non dégénérée sur M qui est hermitienne (relativement à s) ou alternée. Il existe alors un automorphisme θ d'ordre 2 du groupe des automorphismes de M tel que le groupe de la forme B soit le groupe des automorphismes de M invariants par θ .

Soit M un duomodule sur un anneau A , attaché à un antiautomorphisme s de A et possédant une base finie $(x_1,\dots,x_n)$. Soient B une forme bilinéaire sur M , et $\underline{B}$ sa matrice représentative par rapport à la base $(x_1,\dots,x_n)$. Désignons par $\underline{I}$ la matrice unité et par $\underline{U}$ et $\underline{X}$ des matrices carrées à n lignes et colonnes à coefficients dans A telles que

$$\underline{U}\,\underline{X} - \underline{U} + \underline{X} + \underline{I} = 0 .$$

Nous allons montrer que

$$(\underline{I} - {}^t\underline{X}^s)({}^t\underline{U}^s\underline{B}\,\underline{U} - \underline{B})(\underline{I}-\underline{X}) = 2({}^t\underline{X}^s\underline{B} + \underline{B}\,\underline{X}) .$$

On a (lemme 1 , § 1, n° 1) ${}^t\underline{X}^s.{}^t\underline{U}^s - {}^t\underline{U}^s + {}^t\underline{X}^s + \underline{I} = 0$, ou encore $(\underline{I}-{}^t\underline{X}^s){}^t\underline{U}^s = \underline{I} + {}^t\underline{X}^s$; puisque $\underline{U}(\underline{I}-\underline{X}) = \underline{I}+\underline{X}$, il vient

$(\underline{I}-{}^t\underline{X}^s).{}^t\underline{U}^s\underline{B}\,\underline{U}(\underline{I}-\underline{X}) = (\underline{I}+{}^t\underline{X}^s)\underline{B}(\underline{I}+\underline{X}) = {}^t\underline{X}^s\underline{B} + \underline{B}\,\underline{X} + \underline{B} + {}^t\underline{X}^s\underline{B}\,\underline{X}$,

tandis que $(\underline{I}-{}^t\underline{X}^s)\underline{B}(\underline{I}-\underline{X}) = -({}^t\underline{X}^s\underline{B} + \underline{B}\,\underline{X}) + \underline{B} + {}^t\underline{X}^s\underline{B}\,\underline{X}$, ce qui démontre notre formule.

Ceci dit, supposons que $\underline{X}$ soit une matrice telle que ${}^t\underline{X}^s\underline{B} + \underline{B}\,\underline{X} = 0$ et que la matrice $\underline{I}-\underline{X}$ soit inversible. On voit alors que, si on pose $\underline{U} = (\underline{I}+\underline{X})(\underline{I}-\underline{X})^{-1}$, on a ${}^t\underline{U}^s.\underline{B}.\underline{U} = \underline{B}$. De plus, on a $\underline{I} + \underline{U} = 2(\underline{I}-\underline{X})^{-1}$, d'où il résulte que, si 2.1 a un inverse dans A . $\underline{I} + \underline{U}$ est inversible. Supposons à partir de maintenant que 2.1 soit inversible dans A . Si $\underline{U}$ est une matrice telle que ${}^t\underline{U}^s\underline{B}\,\underline{U} = \underline{B}$ et que $\underline{I} + \underline{U}$ soit inversible, posons $\underline{X} = (\underline{U} - \underline{I})(\underline{U}+\underline{I})^{-1}$; on a alors ${}^t\underline{X}^s\underline{B} + \underline{B}\,\underline{X} = 0$, et $\underline{I} - \underline{X} = 2(\underline{U} + \underline{I})^{-1}$ est inversible. On voit donc que, sous les hypothèses faites,

$$\underline{X} \longrightarrow (\underline{I}+\underline{X})(\underline{I}-\underline{X})^{-1}$$

est une application biunivoque de l'ensemble des matrices $\underline{X}$ telles que ${}^t\underline{X}^s\underline{B} + \underline{B}\,\underline{X} = 0$ et que $\underline{I}-\underline{X}$ soit inversible sur l'ensemble des matrices $\underline{U}$ telles que ${}^t\underline{U}^s\underline{B}\,\underline{U} = \underline{U}$ et que $\underline{I} + \underline{U}$ soit inversible. Cette application s'appelle la <u>représentation paramètrique de Cayley</u>. Si on suppose de plus que $\underline{I} + \underline{X}$ est inversible, la matrice $\underline{U}$ correspondante sera inversible et définira un automorphisme de la forme B.

Soit maintenant Q une forme hermitienne sur un duomodule M attaché à un antiautomorphisme s de l'anneau de base A dont le carré est l'identité. On appelle <u>automorphisme de la forme</u> Q tout automorphisme σ du duomodule M tel que $Q(\sigma .x) = Q(x)$ pour tout $x \in M$. Ces automorphismes forment évidemment un groupe, qu'on appelle le groupe de la forme Q . Supposons que A ne contienne aucun diviseur de zéro $\neq 0$; il résulte alors immédiatement de la prop.3, § 1, n°2 que, si s n'est pas l'automorphisme identique, le groupe de la forme Q est identique

au groupe de la forme bilinéaire B associée à Q . Si s est l'automorphisme identique, la formule $B(x,y) = Q(x+y)-Q(x)-Q(y)$ montre que le groupe de la forme Q est toujours contenu dans celui de la forme B ; de plus, ces deux groupes sont identiques si A n'est pas de caractéristique 2, comme il résulte de la formule $B(x,x) = 2Q(x)$.

n°2. EXTENSION DES B-ISOMORPHISMES.

Nous supposerons à partir de maintenant, et jusqu'à la fin de ce § , que M est un espace vectoriel à gauche de dimension finie sur un corps K muni d'un antiautomorphisme s tel que s^2 soit l'identité ; nous désignerons encore par M le duomodule attaché à s et admettant M comme module à gauche sous-jacent. Nous désignerons par B une forme bilinéaire non dégénérée sur M qui est soit hermitienne (relativement à s) soit alternée, et nous supposerons que la condition D . du § 2 est satisfaite. Nous désignerons par G le groupe de la forme B .

Si N est un sous-espace de M , nous désignerons par B_N la restriction de B à N×N . On dit qu'un isomorphisme σ d'un sous-espace N de M sur un sous-espace P est un B-isomorphisme si on a $B_P(\sigma .x, \sigma .y) = B_N(x,y)$ quels que soient x,y dans N .

Nous considèrerons aussi le cas où on a une forme quadratique Q sur M admettant B comme forme bilinéaire associée. Nous désignerons alors par G_Q le groupe de la forme Q ; c'est un sous-groupe de G . Nous dirons qu'un isomorphisme σ d'un sous-espace N de M sur un sous-espace P est un Q-isomorphisme si $Q(\sigma .x) = Q(x)$ pour tout $x \in N$; σ est alors aussi un B-isomorphisme.

Théorème 3. Soit σ un B-isomorphisme d'un sous-espace N de M sur un sous-espace P ; il existe alors une opération du groupe de la forme B qui prolonge σ . Si B est une forme bilinéaire associée à une forme quadratique Q sur M , tout Q-isomorphisme de N sur P se prolonge en un Q-automorphisme de M .

Nous procéderons par récurrence sur la dimension n de N . Si n=0, le résultat est trivial. Supposons donc que $n > 0$ et que le théorème soit vrai pour les B- (resp.: Q-) isomorphismes de sous-espaces de dimension n-1 de M . Soit U un sous-espaces de dimension n-1 de N ; la restriction de σ à U se prolonge donc en une opération de G (resp.: G_Q), soit σ_o Posons $\sigma'(x) = \sigma_o^{-1}(\sigma .x)$ pour $x \in N$; σ' est donc un B- (resp : Q-) isomorphisme de N qui laisse les éléments de U fixes. S'il existe une opération σ'_o de G (resp.: G_Q) qui prolonge σ' , l'opération $\sigma_o \sigma'_o$ prolonge σ . On est donc ramené au cas où σ laisse les éléments de U fixes : supposons désormais qu'il en soit ainsi.

Soit $\mathcal{V}$ l'ensemble des sous-espaces V de M qui possèdent la propriété suivante : σ se prolonge en un B- (resp.: Q-) isomorphisme de V+N qui laisse les éléments de V fixes. Soit V_1 un élément maximal de $\mathcal{V}$; posons $N_1 = V_1+N$, $U_1=V_1+U$ et soit σ_1 le B- (resp.: Q-) isomorphism de N_1 qui prolonge σ et qui laisse les éléments de V_1 fixes ; σ_1 laisse donc les éléments de U_1 fixes ; nous poserons $P_1 = \sigma_1(N_1)$. Soient x_1 un élément de N_1 non contenu dans U_1 et $y_1 = \sigma .x_1$. Supposons qu'il y ait des éléments z,z' de M qui possèdent les propriétés suivantes : z n'est pas dans N_1 , z' n'est pas dans P_1 , $B(z,z)=B(z',z')$ (resp.: $Q(z) = Q(z')$) , $B(z,x_1) = B(z',y_1)$ et z'-z est dans le conjugué U'_1 de U_1 . Il existe alors un isomorphisme σ_2 de $Kz+N_1$ sur $Kz'+P_1$ qui prolonge σ_1 et applique z sur z'. Tout $x \in N_1$ peut se mettre sous la forme $u+ax_1$, $u \in U_1$, $a \in K$; il résulte des formules

$\sigma_1 \cdot u = u$, $B(z'-z,u) = 0$, $B(z,x_1) = B(z',y_1)$ que $B(z,x) = B(z', \sigma_1 \cdot x)$, $B(x,z) = B(\sigma_1 \cdot x, z')$. Un calcul facile montre alors que $B(bz+x, b'z+x') = B(bz'+\sigma_1 \cdot x, b'z'+\sigma_1 \cdot x')$ si b,b' sont dans K et x,x' dans N_1 ; σ_2 est donc un B-isomorphisme. De plus, si B est associée à une forme quadratique Q et si σ_1 est un Q-isomorphisme, on a $Q(bz+x)=b^2Q(z)+Q(x)+bB(z,x) = b^2Q(z')+Q(\sigma_1 \cdot x)+bB(z', \sigma_1 \cdot x)$, et σ_2 est un Q-isomorphisme. Ceci dit, il résulte du caractère maximal de V_1 dans V qu'ils est impossible que l'on ait $z'=z$. Or, soit H le conjugué de $K(y_1-x_1)$; on voit qu'il est impossible qu'un $z \in H$ ne soit ni dans N_1 ni dans P_1. Si $H \cap N_1$ et $H \cap P_1$ étaient tous deux $\neq H$, il y aurait des éléments z_1, z_1' de ces espaces tels que z_1 ne soit pas dans $H \cap P_1$ et que z_1' ne soit pas dans $H \cap N_1$; mais z_1+z_1' serait alors un élément de H n'appartenant ni à N_1 ni à P_1, ce qui est impossible ; H est donc contenu dans l'un des espaces N_1 ou P_1. Si $N_1=M$, la démonstration est terminée. Sinon, H est identique à l'un des espaces N_1, P_1, et l'un au moins des éléments x_1, y_1 est dans H. Si par exemple $x_1 \in H$, on a $B(x_1, y_1-x_1)=0$, i.e. $B(x_1,y_1)=B(x_1,x_1)$; mais on a $B(x_1,x_1) = B(y_1,y_1)$, d'où $B(y_1-x_1,y_1)= 0$ et $y_1 \in H$; on a donc $N_1=P_1=H$. Soit z un élément de M non situé dans H ; nous allons montrer qu'on peut construire un élément z' tel que les conditions indiquées plus haut soient satisfaites. Puisque H est un hyperplan, on a $H+Kz = M$, et la démonstration sera alors terminée. Il est clair que y_1 n'est pas dans U_1 ; U_1' contient donc un élément qui n'est pas dans le conjugué de Ky_1 ; d'où on déduit tout de suite qu'il y a un $u \in U_1'$ tel que $B(u,y_1) = B(z,x_1-y_1)$. Cet élément est $\neq 0$; puisque x_1-y_1 appartient à l'intersection de H et de son conjugué,

on a $B(x_1-y_1,x_1-y_1)=0$, de sorte que u n'est pas dans le conjugué $K(x_1-y_1)$ de $H = N_1$. Puisque $N_1 = U_1+Kx_1$ et $u\in U_1^!$, on a $B(u,x_1)\neq 0$, d'où $b = B(z+u,x_1-y_1) = B(u,x_1) \neq 0$. L'élément z' sera de la forme $z+u+c(x_1-y_1)$, c étant un élément de K que nous allons déterminer dans un moment. Quel que soit c, on a $B(z',x_1-y_1) = b \neq 0$, de sorte que z' n'est pas dans $P_1=H$. De plus, x_1-y_1 étant dans $U_1^!$, on a $z'-z\ U_1^!$. Puisque $B(x_1-y_1,y_1)=0$, on a $B(z',y_1) = B(z,y_1) + B(u,y_1)= B(z,x_1)$. Il ne reste donc qu'à choisir c de telle manière que $B(z',z')=B(z,z)$ (resp.: $Q(z') = Q(z)$). Puisque $B(x_1-y_1,x_1-y_1)=0$, on a

$$B(z',z') = B(z+u,z+u) + bc^s + cb^s$$

si B est hermitienne (si B est alternée, la condition $B(z',z')= B(z,z)$ est automatiquement satisfaite). Or il résulte de la condition D. que $B(z+u,z+u)-B(z,z)$ est de la forme $a+a^s$, $a\in K$; il suffira donc de prendre $c = a(b^s)^{-1}$ pour que $B(z',z')=B(z,z)$. Si B est associée à une forme quadratique Q, on a $Q(x_1-y_1) = Q(x_1)+Q(y_1)-B(x_1,y_1) = 2Q(x_1)-B(x_1,y_1) = B(x_1,x_1)-B(x_1,y_1) = 0$ si σ_1 est un Q-automorphisme. On a donc

$$Q(z') = Q(z+u) + bc ,$$

et il suffira de prendre $c = b^{-1}(Q(z)-Q(z+u))$ pour que $Q(z') = Q(z)$. Le th.3 est donc démontré.

Corollaire. Soient N et P des sous-espaces non isotropes de M, N' et P' leurs conjugués. Si les restrictions de B à $N\times N$ et à $P\times P$ sont équivalentes, il en est de même des restrictions de B à $N'\times N'$ et à $P'\times P'$. Si B est la forme bilinéaire associée à une forme quadratique Q dont les restrictions à N et à P sont équivalentes, les restrictions de Q à N' et à P' sont équivalentes.

Il existe par hypothèse un B- (resp.: Q-) isomorphisme de M sur P ; cet isomorphisme se prolonge en une opération σ de G (resp.: G_Q) , et il est clair que σ applique M' sur P', d'où le résultat.

Considérons maintenant le cas où B est une forme alternée associée à une forme quadratique Q , la caractéristique de K étant 2 . On appelle alors <u>totalement singulier</u> tout sous-espace de M sur lequel Q s'annulle identiquement. La formule $B(x+y)= Q(x+y)-Q(x)-Q(y)$ montre qu'un espace totalement singulier est totalement isotrope, mais la réciproque n'est pas vraie. Il résulte du th.3 que deux sous-espaces totalement singuliers de même dimension peuvent toujours être transformés l'un en l'autre par une opération de G_Q. On en conclut immédiatement que tous les sous-espaces totalement singuliers maximaux ont même dimension r et peuvent être transformés les uns en les autres par les opérations de G_Q : c'est le nombre r que l'on appelle l'<u>indice</u> de la forme quadratique Q .

n°3. LE CENTRE DU GROUPE G.

Proposition 3. Supposons que M soit de dimension ≥ 1 et que l'on ne se trouve pas dans le cas particulier suivant : M est de dimension 2, K est un corps à 3 éléments, B est symétrique d'indice 1. Soient K_0 le centre de K et M_0 l'espace vectoriel sur K_0 déduit de M par restriction à K_0 du corps de base. Si θ est un endomorphisme de M_0 qui commute avec toutes les opérations de G, il existe un élément t de K tel que $\theta.x = tx$ pour tout $x \in M$.

Nous établirons d'abord le lemme suivant :

Lemme 2. Soient x et y des éléments linéairement indépendants de M. Supposons qu'on ne soit pas dans le cas particulier suivant : M est de dimension 2, B est symétrique, x est isotrope. Il y a alors une opération de G qui laisse x, mais non y, fixe.

Posons $N = Kx+Ky$; il suffira, en vertu du th.3, n°2 de montrer qu'il y a un B-isomorphisme de N sur un sous-espace de M qui laisse x fixe, mais non y ; de plus, toute application linéaire de N dans M qui transforme x en lui-même et est distincte de l'application identique transforme y en un vecteur $\neq y$. Soit Z l'intersection de N et du conjugué de Kx. Si $Z=N$, N est totalement isotrope et tout automorphisme d'espace vectoriel de N est un B-automorphisme, ce qui prouve le lemme dans ce cas. Si $Z \neq N$, Z est de dimension 1 ; supposons d'abord que $Z \neq Kx$, donc que x ne soit pas isotrope. Soit z un élémen de base de Z, et soit $a = B(z,z)$. Si K est de caractéristique $\neq 2$, posons $e = -1$. Si K est de caractéristique 2 et $a=0$, il résulte du fai que x n'est pas isotrope que B n'est pas alternée, donc (condition D.) que s est distinct de l'identité, et par suite que K contient un élément distinct de 0,1 ; soit e un pareil élément. Si K est de caractéristique 2 et $a \neq 0$, soit b un élément de K tel que $a = b+b^s$; on a $b \neq 0$,

$b \neq b^s$ (car, sinon, on aurait $a = 2b = 0$) ; posons $e = b^{-1}b^s$, d'où $e \neq 1$, $e^s ae = bb^{-s}(b+b^s)b^{-1}b^s = b+b^s = a$. Les relations $e \neq 1$, $e^s ae = a$ sont donc vraies dans tous les cas ; l'automorphisme de N qui laisse x fixe et change z en ze est donc un B-automorphisme distinct de l'identité. Supposons maintenant que $Z = Kx$; x est alors isotrope, et $B(x,y) \neq 0$. Si $\overset{s}{\times}$ n'est pas l'identité, K contient un $a \neq 0$ tel que $a+a^s = 0$: il suffit en effet de prendre $a = f-f^s$, où f est un élément de K non invariant par s . Si s est l'identité et si B est alternée, posons a=1. Soit $y' = ax+y$; on a $B(x,y') = B(x,y)$. Si s n'est pas l'identité $B(y',y') = (a+a^s)B(x,y)+B(y,y) = B(y,y)$; si s est l'identité et B est alternée, $B(y',y') = B(y,y) = 0$. On en conclut que l'automorphisme de N qui laisse x fixe et change y en $ax+y$ est un B-automorphisme distinct de l'identité. Supposons maintenant que $Z = Kx$, que s soit l'identité, que B ne soit pas alternée et que $\dim M > 2$. Il résulte de la condition D. que K est de caractéristique $\neq 2$. Le conjugué de Kx , qui est de dimension > 1, contient un vecteur z linéairement indépendant de x . Si $a \in K$, on a $B(x,ax+y+z) = B(x,y)$, $B(ax+y+z,ax+y+z) = 2aB(x,y)+B(y+z, y+z)$. Puisque $2B(x,y) \neq 0$, on peut déterminer de telle manière que $B(ax+y+z, ax+y+z) = B(y,y)$. L'application linéaire de N qui transforme x en x et y en $ax+y+z$ est alors un B-sionorphisme distinct de l'identité. Le lemme 2 est donc démontré.

Passons maintenant à la démonstration de la prop.3 . Si x est un élément $\neq 0$ de M, soit G_x l'ensemble des $\sigma \in G$ tels que $\sigma \cdot x = x$, et soit H l'ensemble des x' tels que $\sigma \cdot x' = x'$ pour tout $\sigma \in G_x$. Puisque 0 commute avec toutes les opérations de G_x , il est clair que 0 permute entre eux les éléments de H .

Or, sauf si x est isotrope, dim M = 2 et B symétrique non alternée, il résulte du lemme 2 que $H = Kx$, d'où $\theta.x \in Kx$. Nous allons voir que cette conclusion subsiste même si x est isotrope, dim M = 2 et B est symétrique non alternée pourvu que K ne soit pas un corps à 3 éléments. L'espace M possède une base (u,v) composée de deux éléments non isotropes conjugués ; posons $a = B(u,v)$, $b = B(v,v)$. Puisque u et v sont non isotropes, on a $\theta.u = cu$, $\theta.v = c'v$, où c,c' sont dans K. De plus, K est commutatif, de sorte que θ est un endomorphisme de M ; pour établir notre assertion, il suffit de montrer que $c=c'$. Puisque B est symétrique non alternée, K est de caractéristique $\neq 2$; n'étant pas un corps à 3 éléments, il en contient au moins 5, et il y a un $k \in K$ tel que $k^2 \neq 1,0$. Il en résulte qu'on peut choisir un $k \neq 0$ dans K tel que $B(kv, kv) = bk^2 \neq -a$, d'où $B(u+kv, u+kv) = a+bk^2 \neq 0$. Puisque $u+kv$ n'est pas isotrope, $\theta(u+kv) = cu+c'kv$ appartient à $K(u+kv)$, d'où $c = c'$. Ceci dit, la prop.3 résulte du

Lemme 3. Soient V un espace vectoriel sur un corps K et θ un endomorphisme du groupe additif de V qui applique tout sous-espace de dimension 1 de V dans lui-même. Si V est de dimension >1, il y a un $t \in K$ tel que $\theta.x = tx$ pour tout $x \in V$.

Si x est un élément $\neq 0$ de V, il y a un $t(x)$ bien déterminé de K tel que $\theta.x = t(x)x$. Si y n'est pas dans Kx, on a $t(x+y)(x+y) = \theta.(x+y) = \theta.x + \theta.y = t(x)x+t(y)y$, d'où $t(x) = t(y) = t(x+y)$. Si $y \in Kx$, $y \neq 0$, il y a par hypothèse un $z \in V$ qui n'est pas dans $Kx = Ky$, d'où $t(x) = t(z) = t(y)$; les $t(x)$ pour $x \neq 0$ sont donc tous égaux entre eux, ce qui démontre le lemme 3 et par suite aussi la prop.3.

Corollaire 1. Les notations et hypothèses étant celles de la prop.3 , les seuls sous-espaces de M qui sont appliqués dans eux-mêmes par toutes les opérations de G sont $\{0\}$ et M .

Parmi les sous-espace $\neq\{0\}$ de M qui soht appliqués dans eux-mêmes par toutes les opérations de G, soit N l'un de ceux dont la dimension est la plus petite, et soit N' le conjugué de N . Il est clair que les opérations de G appliquent $N\cap N'$ dans lui-même ; on a donc ou bien $N\cap N' =\{0\}$ ou bien $N\cap N' = N$. Il est impossible que $N\cap N' = N$; N serait alors en effet totalement isotrope, et il existerait un sous-espace P totalement isotrope de même dimension que N tel que $N\cap P = \{0\}$ tout isomorphisme de N sur P serait un B-isomorphisme et se prolongerait par suite en une opération de G ne transformant pas N en lui-même. On a donc $N\cap N' = \{0\}$ et M est somme directe de N et de N'. L'endomorphisme θ de M qui applique sur eux-mêmes les éléments de N et sur 0 ceux de N' commute évidemment avec les opérations de G ; il y a donc un $t\in K$ tel que $\theta.x = tx$ pour tout $x\in M$. Puisque $N \neq \{0\}$, on a $t=1$, $N' = \{0\}$ et $N = M$.

Corollaire 2. Les notations et hypothèses étant celles de la prop.3, le centre de G se compose de celles des homothéties centrales de M qui appartiennent à G .

Soit en effet θ une opération du centre de G . Il y a donc un $t\in K$ tel que $\theta.x = tx$ pour tout $x\in M$. Puisque θ est un automorphisme de M , t est dans le centre de K .

Soit $x \to cx$ une homothétie centrale de M , c étant un élément du centre de K . On a, pour x,y dans M, $B(cx, cy) = c^{s}B(x,y)c = cc^{s}B(x,y)$.

Si donc $B \neq \{0\}$ (i.e. si $M \neq \{0\}$), une condition nécessaire et suffisante pour que l'homothétie en question soit dans G est que $\alpha\alpha^s = 1$. En particulier, si B est symétrique ou alternée, le centre de G est d'ordre 2 ou 1 suivant que la caractéristique de K est différente de 2 ou égale à 2 , sauf si $M = \{0\}$ ou si M est de dimension 2, K n'a que 3 éléments et B est symétrique d'indice 1 .

Ce dernier cas est d'ailleurs effectivement un cas exceptionnel. En effet, M admet alors une base (x,y) composée de deux vecteurs isotropes tels que $B(x,y) = 1$ et on voit facilement que G se compose des homothéties de rapports $\neq 0$ de M et des deux opérations σ_a définies par $\sigma_a \cdot x = ay$, $\sigma_a y = ax$ $(a = \pm 1)$: G est abélien d'ordre 4 , et chacun des sous-espaces $K(x+y)$ et $K(x-y)$ de M est appliqué dans lui-même par toutes les opérations de G . Si M est de dimension 1 et si K n'est pas commutatif, on (du moins le rédacteur) ignore si le centre de G est identique à l'ensemble des homothéties centrales qui y sont contenues.

n° 4. LE GROUPE G^+ .

En plus des hypothèses faites précédemment, nous supposerons dans ce n° que K est un corps commutatif. Nous désignerons par G^+ le groupe des éléments de G dont les déterminants sont égaux à 1 .

Proposition 4. Si la forme B est alternée, on a $G^+ = G$. Dans le cas contraire, soit H un hyperplan non isotrope de M , et soit D le groupe des opérations de G qui laissent tous les éléments de H fixes. Tout élément de G se met alors d'une manière et d'une seule sous la forme du produit d'un élément de G^+ par un élément de D . Le groupe G^+ est distingué dans G , et G/G^+ est isomorphe au groupe multiplicatif des éléments c de K tels que $c.c^s = 1$.

Supposons d'abord B alternée, et soit $\underline{B}$ la matrice représentative de B par rapport à une base de M ; on a donc $\det \underline{B} \neq 0$, d'où $\mathrm{Pf}.\underline{B} \neq 0$. Si $\underline{U}$ est la matrice représentative par rapport à la base choisie d'une opération de G , on a ${}^t\underline{U}.\underline{B}.\underline{U} = \underline{B}$, d'où $(\mathrm{Pf}.\underline{B})(\det \underline{U}) = \mathrm{Pf}.\underline{B}$, et par suite $\det \underline{U} = 1$. Supposons maintenant que B ne soit pas alternée. Soit H un hyperplan non isotrope de M (il en existe au moins un, à savoir le conjugué d'un élément non isotrope de M). Soient σ une opération de G et d son déterminant ; on a $dd^s = 1$ (prop.1, n°1). Soit x un élément $\neq 0$ du conjugué de H ; puisque $dd^s = 1$, il est clair que l'automorphisme τ de M qui transforme x en dx et laisse les éléments de H fixes appartient au groupe D de l'énoncé. Le déterminant de τ étant d , on a $\sigma\tau^{-1} \in G^+$, d'où $\sigma \in G^+D$. Une opération de D transforme en lui-même le conjugué Kx de H ; si elle change x en dx , elle est de déterminant d , et n'appartient à G^+ que si $d=1$, ce qui montre que $G^+ \cap D$ ne contient que l'élément neutre. Enfin, si $c \in K$ est tel que $cc^s = 1$,

l'automorphisme de M qui change x en cx et qui laisse les éléments de H fixes appartient à D, ce qui montre que $\tau \to \det \tau$ est un isomorphisme de D sur le groupe des $c \in K$ tels que $cc^s = 1$. Il est clair que G^+ est un sous-groupe distingué de G et que G/G^+ est isomorphe à D ; la prop.4 est donc démontrée.

Nous allons maintenant déterminer la structure du groupe G^+ dans le cas où B est symétrique mais non alternée et où M est de dimension 2. L'espace M a une base composée de deux vecteurs non isotropes conjugués u,v. Posons $a = B(u,u)$, $b = B(v,v)$; posons $c = -a^{-1}b$. On peut définir sur M une structure d'algèbre commutative sur K par les conditions suivantes : u est l'élément unité de M et $v^2 = cu$. Pour tout $x = eu+fv$ de M (e,f dans K), posons $\bar{x} = eu-fv$; il est clair que $x \to \bar{x}$ est un automorphisme de M, dont le carré est l'identité, mais qui est lui-même distinct de l'automorphisme identique, car, B étant symétrique mais non alternée, K est de caractéristique $\neq 2$. On a $(e^2-cf^2)u = a^{-1}B(x,x)u$, et, si $y \in M$, $y=e'u+f'v$, $x\bar{y} = a^{-1}B(x,y)u + (e'f-ef')v$. Soit x_1 un élément de M tel que $x_1\bar{x}_1 = u$, et soit $R(x_1)$ l'opération de multiplication par x_1 dans M. On a, pour $x,y \in M$, $(xx_1)(\overline{yx_1}) = x\bar{y}$, d'où $B(xx_1,yx_1) = B(x,y)$ et $R(x_1) \in G$. De plus, si $x_1 = e_1u+f_1v$, $\bar{x}_1 = e_1u+f_1v$, $vx_1 = cf_1+e_1v$, et le déterminant de $R(x_1)$ est $e_1^2 - cf_1^2 = 1$ puisque $x_1\bar{x}_1 = u$, et $R(x_1) \in G^+$. Soit réciproquement σ une opération de G^+, et soit $x_1 = \sigma.u$. On a $B(x_1,x_1) = B(u,u)= a$, d'où $x_1\bar{x}_1 = u$. L'opération $(R(x_1))^{-1}\sigma$ est dans G^+ et laisse fixes les éléments de l'hyperplan non isotrope Ku : c'est l'identité (prop.4), et $\sigma = R(x_1)$. L'application $x_1 \to R(x_1)$ est donc un isomorphisme du groupe multiplicatif des $x_1 \in M$ tels que $x_1\bar{x}_1 = 1$ sur G^+, ce qui montre que G^+ est abélien. On voit tout de suite que l'opération τ : $x \to \bar{x}$ est dans G et que son déterminant est -1 ;

G est donc $G^+ \cup G^+\tau$. On sait que, si c n'est pas un carré dans K , M est un corps, extension quadratique de K , et G^+ est alors isomorphe au groupe multiplicatif des nombres de ce corps de norme 1 par rapport à K . Dans le cas contraire, soit $c = d^2$, $d \in K$; posons $x = (2d)^{-1}(du+v)$, $y = (2d)^{-1}(du-v)$. Alors, x et y sont isotropes, on a $x^2=x$, $y^2=y$, $xy=0$, $M = Kx+Ky$, $\bar{x} = y$. Un élément $x_1 \in M$ étant mis sous la forme $tx+t'y$, une condition nécessaire et suffisante pour que $x_1\bar{x}_1 = 1$ est que $tt'=1$. L'application $t \to R(tx+t^{-1}y)$ est alors un isomorphisme du groupe multiplicatif des éléments $\neq 0$ de K sur G^+ .

Proposition 5. Supposons que l'on ne soit pas dans le cas où M est de dimension 2 et B est symétrique. Si θ est un endomorphisme de M qui commute avec tous les éléments de G^+, θ est une homothétie.

On peut supposer que B n'est pas alternée, car, sinon, la prop.5 résulte des prop.3 et 4. Soit $(x_1,\dots,x_m)$ une base de M composée de vecteurs non isotropes mutuellement conjugués. Si s n'est pas l'identité, il existe un $c_1 \in K$ tel que $c_1 c_1^s = 1$, $c_1 \neq c_1^{-1}$. Soit en effet u_1 un élément de K tel que $u_1^s \neq u_1$; si $(u_1^2)^s \neq u_1^2$, on peut prendre $c_1 = u_1^{-1}u_1^s$; si $(u_1^2)^s = u_1^2$, K est obtenu par adjonction de u_1 au corps des invariants K_0 de s ; étant séparable sur K_0 , il n'est pas de caractéristique 2, et $(1+u_1)^2$ n'est pas dans K_0, de sorte qu'on peut prendre $c = (1+u_1)^{-1}(1+u_1^s)$. Si s est l'identité, soit $c_1=1$. Soit y un élément linéairement indépendant de x ; montrons qu'il y a un $\sigma \in G^+$ tel que $\sigma \cdot x = c_1 x$, $\sigma \cdot y \neq c_1 y$. Soit $y = \sum_{i=1}^{m} a_i x_i$, $a_i \in K$; il y a un indice $k > 1$ tel que $a_k \neq 0$. Si s n'est pas l'identité, posons $c_k = c_1^{-1}$, $c_i=1$ pour $i \neq 1,k$. Si s est l'identité, on a $m > 2$; soit ℓ

un indice distinct de 1 et de k entre 1 et m ; posons $c_k = c_\ell = -1$, $c_i = 1$ pour $i \neq 1, k, \ell$. On a donc dans tous les cas $c_i^s = c_i^{-1}$ $(1 \leqq i \leqq m)$, $c_1 \cdots c_m = 1$. L'automorphisme σ de M qui change x_i en $c_i x_i$ $(1 \leqq i \leqq m)$ appartient donc à G^+ ; de plus on a $c_k \neq c_1$ (car, B n'étant pas alternée, s ne peut être l'identité si K est de caractéristique 2), d'où il résulte que $\sigma . y \neq c_1 y$. Soit G_1 l'ensemble des $\tau \in G^+$ tels que $\tau . x_1 = c_1 x_1$; on voit que l'ensemble E des $y \in M$ tels que $\tau . y = c_1 y$ pour tout $\tau \in G_1$ est Kx_1 . Or, puisque θ est un endomorphisme de M et commute avec les opérations de G_1, il est clair que θ permute entre eux les éléments de E , d'où $\theta . x_1 \in Kx_1$. On verrait de la même manière que $\theta . x_i \in Kx_i$ pour $i > 1$. Soit H l'hyperplan non isotrope engendré par $x_2, \ldots, x_m$: on voit que θ commute avec tout automorphisme de M qui laisse les éléments de H fixes et qui transforme Kx_1 en lui-même. Or, Kx_1 étant le conjugué de H , toute opération de G qui transforme H en lui-même transforme aussi Kx_1 en lui-même. Il résulte alors de la prop.4 que θ commute avec toutes les opérations de G , donc de la prop.3, que θ est une homothétie.

Corollaire. Les notations et hypothèses étant celles de la prop.5 , le centre de G^+ se compose des homothéties qui y sont contenues.

En particulier, si B est symétrique mais non alternée, le centre de G^+ est d'ordre 2 . Si B est hermitienne et de rang m , le rapport d'une homothétie de M appartenant à G est une racine m-ième de l'unité, de sorte que le centre de G est un groupe cyclique fini.

Proposition 6. Soit N un sous-espace de M qui est contenu dans un sous-espace non isotrope $Q \neq M$ de M ; tout B-isomorphisme de N sur un sous-espace P de M se prolonge alors en une opération de G^+ .

Un B-isomorphisme σ de M sur P se prolonge en une opération σ_1 de G (th.3,n°2) ; soit $d = \det \sigma_1$, d'où $dd^s = 1$. Posons $Q_1 = \sigma_1(Q)$; Q_1 est un sous-espace non isotrope $\neq M$ de M ; soit Q_1' son conjugué. Puisque $Q_1' \neq \{0\}$; $dd^s = 1$, il y a un B-automorphisme σ_0 de Q_1' de déterminant d^{-1} ; σ_0 se prolonge en une opération $\sigma' \in G$ qui laisse fixes les éléments de Q_1, donc de P . Il est clair que $\det \sigma' = d^{-1}$; $\sigma'\sigma_1$ est donc une opération de G^+ qui prolonge σ.

Proposition 7. Soit m la dimension de M ; si $2r < m$, ou si B est alternée ou si s est distinct de l'identité, les opérations de G^+ permutent transitivement entre eux les sous-espaces totalement isotropes de dimension r de M . Si B est symétrique mais non alternée et d'indice $m/2$, l'ensemble des sous-espaces totalement isotropes de dimension $m/2$ se décompose en deux classes, les espaces de chaque classe étant permutés entre eux transitivement par les opérations de G^+ ; pour que deux espaces appartiennent à la même classe, il faut et suffit que la dimension de leur intersection ait même parité que $m/2$.

Soient N un sous-espace totalement isotrope de dimension r de M et $(x_1,\dots,x_r)$ une base de N . Il existe alors un sous-espace totalement isotrope P et une base $(y_1,\dots,y_r)$ de P tels que $B(x_i,y_j) = \delta_{ij}$ (prop.1, § 3,n°1). Il est clair que N+P n'est pas isotrope et est de dimension 2r . Si donc $2r < m$, la conclusion de la prop.7 découle de la prop.6. Supposons que $2r = m$; si B est alternée, $G^+ = G$ et la conclusion de la prop.7 résulte du th.3,n°2. Supposons maintenant que $2r = m$ et que B ne soit pas alternée. Soit N' un sous-espace totalement isotrope de dimension r de M ; il y a une opération σ de G qui transforme N en N' (th.3, n°2) ; soit $d = \det \sigma$. S'il y a une opération τ de G de déterminant d^{-1} qui conserve N , $\sigma\tau$ sera

une opération de G^+ transformant N en N'. Cherchons à quelle condition il en est ainsi. Les éléments $x_1,\dots,x_r,y_1,\dots,y_r$ forment une base de M relativement à laquelle B est représentée par la matrice

$$\underline{B} = \begin{pmatrix} 0 & \underline{I} \\ \underline{I} & 0 \end{pmatrix}$$

où $\underline{I}$ est la matrice unité de degré r . Un automorphisme de M qui conserve N est représenté par une matrice de la forme

$$\underline{X} = \begin{pmatrix} \underline{U} & \underline{W} \\ 0 & \underline{V} \end{pmatrix}$$

où $\underline{U},\underline{V},\underline{W}$ sont des matrices carrées de degré r , $\underline{U}$ et $\underline{V}$ étant inversibles. Ecrivant que ${}^t\underline{X}^s\underline{B}.\underline{X} = \underline{B}$, on trouve les conditions suivantes pour que l'automorphisme appartienne à G :

$${}^t\underline{U}^s.\underline{V} = \underline{I} \; ; \quad {}^t\underline{V}^s\underline{W} + {}^t\underline{W}^s.\underline{V} = 0 \; .$$

Si on désigne par c le déterminant de $\underline{U}$, celui de $\underline{X}$ sera donc c^{1-s} . Ceci dit, on a $d^{-1}(d^{-1})^s = 1$; si donc s est distinct de l'identité, il y a un $c \in K$ tel que $d^{-1} = c^{1-s}$. Prenant pour $\underline{U}$ une matrice carrée quelconque de déterminant c , posant $\underline{V} = {}^t(\underline{U}^{-1})^s$, $\underline{W} = 0$, on obtient un automorphisme de déterminant d^{-1} qui conserve N et qui appartient à G . Si au contraire s est l'identité, on a $\det \underline{X} = 1$, et tout élément de G qui transforme N en lui-même est de déterminant 1. Si τ est une opération de G de déterminant -1, τ transforme N en un sous-espace totalement isotrope N' tel qu'il n'existe aucune opération de G^+ transformant N en N'. Puisque G^+ est alors d'indice 2 dans G , l'ensemble des sous-espaces totalement isotropes de dimension r ne peut se décomposer en plus de deux classes de transitivité relativement à G^+ ; il en contient donc exactement deux. Cherchons à quelle condition un sous-espace totalement isotrope maximal est dans la même classe que N .

Soit $N_1 = N \cap N'$; on peut supposer que les éléments $x_{s+1},\dots,x_r$ forment une base de N_1 ($r-s$ étant la dimension de N_1). Soit P_1 le sous-espace engendré par $y_{s+1},\dots,y_r$; il est clair que N_1+P_1 n'est pas isotrope. Soit Q le conjugué de cet espace ; l'espace $N_2 = Q \cap N$ est l'espace de base $(x_1,\dots,x_s)$. L'espace $N' \cap Q$ est l'ensemble des éléments de N' qui sont conjugués à $y_{s+1},\dots,y_r$ (car tout élément de N' est dans le conjugué de $N_1 = N \cap N'$) ; il est donc de codimension $\leqq r-s$ dans N', et n'a que 0 en commun avec $N_2 = N \cap N'$. On en conclut que $N_2' = N' \cap Q$ est un supplémentaire de N_1 dans N'. On a $N_2 \cap N_2' = \{0\}$ puisque $N \cap N' = N_1$; N_2+N_2' est donc de dimension 2s égale à celle du conjugué Q de N_1+P_1 ; Q est donc somme directe de N_2 et N_2'. Comme N_2' est totalement isotrope, cet espace a une base $(z_1,\dots,z_s)$ telle que $B(x_i,z_j)=0$ $(1 \leqq i, j \leqq s)$. Il est clair que l'automorphisme θ_1 de Q qui transforme x_i en z_i et z_i en x_i $(1 \leqq i \leqq s)$ est un B-automorphisme ; il se prolonge en un automorphisme θ appartenant à G qui laisse fixes les éléments de N_1+P_1 et qui transforme par suite N en N'. Le déterminant de θ est le même que celui de θ_1, à savoir $(-1)^s$; N' appartient donc ou non à la même classe que N suivant que s est pair ou impair, ce qui achève la démonstration de la prop.7 .

Proposition 8. Sauf dans le cas où M est de dimension 2 et où B est symétrique d'indice 1 mais non alternée, les seuls sous-espaces de M qui sont appliqués dans eux-mêmes par toutes les opérations de G^+ sont $\{0\}$ et M .

Parmi les sous-espaces de M qui sont $\neq \{0\}$ et qui sont appliqués dans eux-mêmes par toutes les opérations de G^+, choisissons en un, soit N , de dimension minimale. On voit alors comme dans la démonstration de la prop. , n° que N est ou bien non isotrope ou bien totalement isotrope. Si N n'était pas isotrope était et $\neq M$, la restriction à N de toute opération de G se prolongerait en une opération de G^+ (prop.6) et conserverait par suite N , ce qui est impossible en vertu de la prop. , n° . Si N est totalement isotrope, soit r sa dimension. Puisque $r > 0$, il résulte de la prop. , § , n° que N n'est pas le seul sous-espace totalement isotrope de dimension r . Il résulte donc de la prop.7 que M est de dimension 2r, que B est symétrique mais non alternée et qu'il n'y a que deux sous-espaces totalement isotropes de dimension r , soient N et P . Soit N_1 un sous-espace de dimension 1 de N . Si on avait $r > 1$, il résulterait de la prop.7 qu'il existe une opération de G^+ transformant N_1 en un sous-espace de P non situé dans N , ce qui est impossible ; on a donc $r=1$, et la prop.8 est démontrée.

n°5. INVOLUTIONS DU GROUPE G .

Nous appellerons <u>involution</u> tout endomorphisme de M dont le carré est l'identité. Nous nous proposons de rechercher les involutions appartenant au groupe G . Soit θ l'une d'elles ; désignons par N le sous-espace de M formé des éléments invariants par θ . Si x est un élément quelconque de M , l'élément $\theta.x + x$ appartient à N , et on a $\theta.(\theta.x-x) = -(\theta.x-x)$. Si K n'est pas de caractéristique 2 , soit P l'ensemble des $y \in M$ tels que $\theta.y = -y$; on a $N \cap P = \{0\}$ et la formule $x = (1/2)((\theta.x+x)-(\theta.x-x))$ montre que $x \in N+P$; M est donc somme directe de N et de P . De plus, les conditions $x \in N$, $y \in P$ entraînent $B(x,y) = B(\theta.x,\theta.y) = -B(x,y)$, d'où $B(x,y)=0$. Il en résulte immédiatement que N n'est pas isotrope et que P est son conjugué. Si K est de caractéristique 2, on a $\theta.x - x \in N$ pour tout $x \in M$; les éléments de N de la forme $\theta.x-x$ forment un sous-espace N_0 de N . Si $y \in N$, on a $B(\theta.x,y) = B(\theta.x,\theta.y) = B(x,y)$, d'où $B(\theta.x-x,y) = 0$; N_0 est donc contenu dans le conjugué de N , et est par suite totalement isotrope. Soient p la dimension de N_0, m celle de M ; $x \to \theta.x-x$ étant une application linéaire de M sur N_0, son noyau N est de dimension m-p égale à celle du conjugué de N_0 ; le conjugué de N_0, qui contient N , lui est donc identique.

Dans le cas où K n'est pas de caractéristique 2, soit réciproquement N un sous-espace non isotrope de M , et soit P son conjugué. L'autonorphisme θ de M qui applique tout $x \in N$ sur x et tout $y \in P$ sur -y est une involution. Soient x,x' des éléments de N, y+y' des éléments de P ; on a $B(x+y,x'+y') = B(x,x')+B(y,y') = B(x-y,x'-y')$, ce qui montre que $\theta \in G$.

Dans le cas où K est de caractéristique 2, soit N_0 un sous-espace totalement isotrope et soit N son conjugué. Il existe alors au moins une application linéaire g de M sur N_0, de noyau N, telle que l'endomorphisme θ de M défini par $\theta.x = x+g(x)$ $(x \in M)$ soit une involution appartenant à G. Observons d'abord que, puisque $\theta.g(x) = g(x)$ pour tout $x \in M$, θ est une involution, donc un automorphisme de M. Soit P un supplémentaire de N dans M ; puisque N est le conjugué de N_0, la restriction de B à $N_0 \cap P$ est non dégénérée. Soit $(x_1,\dots,x_h)$ une base de P ; il existe alors une base $(u_1,\dots,u_h)$ de N_0 telle que $B(x_i,u_i) = \delta_{ij}$ $(1 \leqq i, j \leqq h)$. Soit g l'application linéaire de M sur N_0 qui applique N sur $\{0\}$ et x_i sur u_i $(1 \leqq i \leqq h)$. Soient $x = z + \sum_{i=1}^{h} a_i x_i$, $x' = z' + \sum_{i=1}^{h} a_i' x_i$ des éléments de M, avec z,z' dans N, a_i, a_i' dans K. On a, en posant $\theta.x = x+g(x)$, $\theta.x = x + \sum_{i=1}^{h} a_i u_i$, $\theta.x' = x' + \sum_{i=1}^{h} a_i' u_i$ et $B(\theta.x,\theta.x') = B(x,x') + \sum_{i=1}^{h} B(x,u_i)a_i'^{s} + \sum_{i=1}^{h} a_i B(u_i,x')^{s} = B(x,x')$ puisque K est de caractéristique 2 et $B(x,u_i) = a_i$, $B(u_i,x') = a_i'^{s}$.

Nous limitant maintenant au cas où K n'est pas de caractéristique 2, cherchons à quelle condition deux éléments donnés x,y de M peuvent être transformés l'un en l'autre par une involution de G. Si $x \neq 0$, $y \in Kx$, on doit avoir $y = \pm x$, car, si θ est une involution telle que $\theta.x = kx$, on a $x = \theta^2.x = k^2 x$, d'où $k = \pm 1$. Réciproquement, si $k = \pm 1$, l'application $z \to kz$ $(z \in M)$ est une involution de G transformant x en kx. Supposons maintenant x,y linéairement indépendants. Il est alors évidemment nécessaire que $B(x,x) = B(y,y)$ et que $B(x,y) = B(y,x)$. Ces conditions sont suffisantes. Supposons les en effet satisfaites, et désignons par H le conjugué de $K(x-y)$; il résulte immédiatement des conditions que nous supposons satisfaites que $B(x-y,x+y)=0$, d'où $x+y \in H$. Si $x-y$ n'est pas isotrope, H n'est pas isotrop

et nous poserons alors $N = H$. Dans le cas contraire, observons qu'il résulte du fait que x et y sont linéairement indépendants qu'il en est de même de x-y et x+y ; soit N un sous-espace de H supplémentaire à K(x-y) et contenant x+y . Ce sous-espace n'est pas isotrope. Soit en effet z un élément de l'intersection de N et de son conjugué. Le conjugué de Kz contient alors N et K(x-y), donc H tout entier, et z appartient au conjugué K(x-y) de H , d'où z=0 puisque $N \cap K(x-y) = \{0\}$. Dans les deux cas, soit θ l'involution appartenant à G qui laisse fixes les éléments de N et transforme en leurs opposés ceux du conjugué de N . On a donc $\theta.(x+y) = x+y$, $\theta.(x-y) = y-x$, d'où $\theta.x = y$.

Proposition 9. Supposons que B soit symétrique mais non alternée. Toute opération de G peut alors se représenter comme un produit d'involutions appartenant à G .

Nous procèderons par récurrence sur la dimension de M . La proposition est évidente si M est de dimension 1 . Supposons la vraie pour les espaces de dimensions strictement inférieure à celle de M . Soit σ une opération de G , et soit x un vecteur non isotrope de M ; posons $\sigma.x = y$. On a $B(x,x) = B(y,y)$ et $B(x,y) = B(y,x)$. Si $y \in Kx$, la relation $B(x,x) = B(y,y)$ entraîne que $y = \pm x$. Il existe donc une involution θ de G qui transforme y en x ; l'opération $\sigma' = \sigma\theta$ appartient à G et laisse x fixe. Elle transforme donc en lui-même le conjugué N de Kx . L'espace N est de dimension strictement inférieure à celle de M , et la restriction de B à $N \times N$ est symétrique mais non alternée. La restriction de σ' à N se représente donc comme un produit d'involutions de l'espace N qui sont des B-automorphismes.

Si θ' est l'une quelconque de ces involutions, θ' se prolonge en un automorphisme θ'_1 de M laissant x fixe ; il est clair que θ'_1 est une involution appartenant à G et que σ' est le produit de ces involutions prolongées, ce qui montre que σ est un produit d'involutions.

Supposant toujours B symétrique mais non alternée, soit N un sous-espace non isotrope de M , et soit θ l'involution qui laisse fixes les éléments de N et change en leurs opposés ceux du conjugué N' de N . L'opération θ s'appelle la <u>symétrie</u> par rapport à N . Si p est la codimension de N , on a $\det \sigma = (-1)^p$, de sorte que σ appartient ou non à G^+ suivant que p est pair ou impair. Soit $(x_1,\dots,x_p)$ une base de N' composée de vecteurs non isotropes mutuellement conjugués, et soit H_i l'hyperplan engendré par N et par les x_j pour $j \neq i$. Il est alors clair que la symétrie par rapport à N est le produit des symétries par rapport aux H_i . Il résulte donc de la prop.9 que toute opération de G peut se représenter comme un produit de symétries par rapport à des hyperplans. On peut même montrer que, si $m = \dim M$, toute opération de G peut se représenter comme un produit d'au plus m symétries par rapport à des hyperplans (cf. exerc.).

[N.B. du rédacteur. Considérons maintenant le cas où s n'est pas l'identité mais où K est commutatif de caractéristique $\neq 2$. Il n'est alors pas vrai, comme dit dans une rédaction antérieure, que toute opération de G de déterminant 1 puisse se représenter comme produit d'au plus m "symétries" par rapport à des hyperplans. Supposons en effet que M soit de dimension 2 , engendré par des vecteurs conjugués x,y tels que $B(x,x) = 1$, $B(y,y) = m$ où m est un élément du corps K_0

des éléments invariants par s qui n'est norme d'un élément de K . Soit k un élément de K distinct de ± 1 et de norme 1 par rapport à K_0, et soit σ l'automorphisme défini par $\sigma.x = kx$, $\sigma.y = k^{-1}y$. Je dis que σ ne peut se représenter sous la forme $\theta_1\theta_2$, où θ_1, θ_2 sont des symétries par rapport à des hyperplans. Supposons en effet le contraire, et soit $ax+by$ un vecteur $\neq 0$ invariant par θ_2 , d'où $akx + bk^{-1}y = \theta_1(ax+by)$. Ceci entraîne $B(ax+by, akx+bk^{-1}y) = B(akx+bk^{-1}y, ax+by)$, d'où $k^{-1}aa^s+kbb^sm = kaa^s + k^{-1}bb^sm$, i.e. $(k-k^{-1})(aa^s-bb^sm)$ et par suite $aa^s-bb^sm = 0$, contrairement à l'hypothèse que m n'est pas norme d'un élément de K . La question de savoir si les symétries par rapport aux hyperplans engendrent le groupe des opérations de déterminants 1 ou -1 dans le cas hermitien non symétrique me semble rester ouverte.]

n° 5. DÉCOMPOSITION EN SYMÉTRIES.

En plus des hypothèses faites au début du n°2, nous supposerons dans ce n° que K est un corps commutatif et que B est une forme bilinéaire symétrique associée à une forme quadratique Q sur M. Nous désignerons par G_Q le groupe de la forme Q.

Soit H un hyperplan de M dont le conjugué contient un élément z tel que $a = Q(z) \neq 0$. Pour tout $x \in M$, posons

$$\sigma_H \cdot x = x - a^{-1}B(x,z)z \quad ;$$

σ_H est un endomorphisme de M qui ne dépend que de H, non du choix de z ; car si on remplace z par kz, où k est un élément $\neq 0$ de K, Q(z) est remplacé par k^2z et B(x,z) par kB(x,z). Il est clair que σ_H laisse les éléments de H fixes. Si K n'est pas de caractéristique 2 on a $M = H + Kz$ et $\sigma_H \cdot z = -z$, de sorte que σ_H est une involution appartenant au groupe G de la forme B, qui est alors identique à G_Q. Si K est de caractéristique 2, B est alternée, et $z \in H$; puisque $\sigma_H \cdot x - x \in H$ pour tout $x \in M$, σ_H est une involution. De plus on a

$$Q(\sigma_H \cdot x) = Q(x) + a^{-2}B^2(x,z)Q(z) - a^{-1}B^2(x,z) = Q(x)$$

de sorte que σ_H appartient au groupe G_Q. Dans les deux cas, nous dirons que σ_H est la <u>symétrie par rapport à</u> H.

<u>Proposition 10. Supposons que le corps</u> K <u>contienne plus de deux éléments. Tout élément de</u> G_Q <u>peut alors se représenter comme produit d'un certain nombre de symétries par rapport à des hyperplans.</u>

Nous procéderons par récurrence sur la dimension m de M. La proposition est évidente si $m = 0$. Supposons la vraie pour les espaces de dimensions $< m$. Soient θ un élément de G_Q et L l'ensemble des éléments de M laissés fixes par θ. Supposons d'abord que L contienne

un sous-espace $L_1 \neq \{0\}$ non isotrope ; θ transforme alors en lui-même le conjugué L_1' de L_1 . La restriction de B à $L_1' \times L_1'$ n'étant pas dégénérée, la restriction θ_1 de θ à L_1' se représente comme produit de symétries par rapport à des hyperplans de L_1' , relativement à la restriction de Q à L_1' . Soit τ_1 l'une de ces symétries, et soit H_1 l'hyperplan de L_1' dont les points sont laissés fixes par τ_1 . Posons $H = H_1 + L_1$; H est un hyperplan de M . Le conjugué de H_1 par rapport à la restriction de B à $L_1' \times L_1'$ contient un vecteur z tel que $Q(z) \neq 0$; puisque z est dans le conjugué de L_1, il est dans celui de H . Il est clair que la symétrie par rapport à H prolonge τ_1 et laisse les éléments de L_1 fixes. Puisque θ laisse les éléments de L_1 fixes, on en déduit que θ se représente comme produit de symétries par rapport à des hyperplans de M . Supposons maintenant que L soit totalement isotrope. Observons que, si x et y sont des vecteurs tels que $Q(x) = Q(y)$ et $B(x,x-y) \neq 0$, il y a une symétrie par rapport à un hyperplan qui transforme x en y . On a en effet, en posant $z = x-y$, $Q(z) = 2Q(x)-B(x,y) = B(x,x-y) \neq 0$; soit H le conjugué de Kz , et soit σ_H la symétrie par rapport à H . On a

$$\sigma_H \cdot x = x - (Q(z))^{-1} B(x,x-y)(x-y) = y \quad ,$$

ce qui démontre notre assertion. Ceci dit, si $L = \{0\}$, il y a toujours une symétrie τ par rapport à un hyperplan telle que $\tau\theta$ laisse fixe un vecteur $x \neq 0$. En effet, l'application linéaire $x \to \theta.x - x$, dont le noyau se réduit à $\{0\}$, applique M sur M . Il y a donc un $x \in M$ tel que $Q(\theta.x-x) \neq 0$; puisque $Q(\theta.x) = Q(x)$, le raisonnement fait plus haut montre que la symétrie τ par rapport au conjugué de $K(\theta.x-x)$ transforme x en $\theta.x$, donc que $\tau\theta$ laisse

x fixe. Supposons donc que θ laisse au moins un vecteur $x \neq 0$ fixe. Si x n'est pas isotrope, nous sommes dans le cas qui a été traité plus haut. Supposons donc x isotrope. S'il existe un $y \in M$ tel que $B(x,y) \neq 0$, $B(y,\theta.y-y) \neq 0$, la symétrie τ par rapport au conjugué de $K(\theta.y-y)$ change y en $\theta.y$. De plus, on a $B(x,\theta.y) = B(\theta.x,\theta.y) = B(x,y)$, d'où $B(x,\theta.y-y)=0$ et $\tau.x = x$. Il en résulte que $\tau\theta$ laisse x et y fixes ; puisque $B(x,x) = 0$, $B(x,y) \neq 0$, on voit tout de suite que $Kx+Ky$ n'est pas isotrope, et nous sommes dans le cas traité plus haut. Supposons maintenant que la condition $B(x,y) \neq 0$ entraîne $B(y,\theta.y-y)=0$. Si M est de dimension 2, soit y un vecteur tel que $B(x,y)=1$; on a $B(x,\theta.y)=1$, d'où $\theta.y = y+kx$, $k \in K$, et la condition $B(y,\theta.y-y)=0$ donne $k=0$, de sorte que θ est l'identité. Supposons que $m > 2$. Le conjugué de Kx, qui est de dimension m-1, n'est alors pas totalement isotrope et contient un vecteur z tel que $Q(z)\neq 0$. Soit τ la symétrie par rapport au conjugué de Kz ; ce conjugué contenant x , on a $\tau.x = x$, de sorte que $\tau\theta$ conserve x . Si nous pouvons montrer qu'il existe un y tel que $B(x,y) \neq 0$, $B(y, \tau\theta.y-y) \neq 0$, le raisonnement fait plus haut montre qu'il existe une symétrie τ' par rapport à un hyperplan telle que $\tau'\tau\theta$ laisse fixes les points d'un espace non isotrope $\neq \{0\}$. Or, nous allons montrer qu'il en est bien ainsi. Supposons en effet le contraire. Pour tout y tel que $B(x,y) \neq 0$, on a alors $B(y,\theta.y-y) = B(y, \tau\theta.y-y)=0$, et par suite $B(y, \tau\theta.\overbrace{y)}^{-\theta.y} = -(Q(z))^{-1}B(y,z)B(\theta.y,z) = 0$; soient ℓ_1 , ℓ_2 , ℓ_3 les formes linéaires $y \to B(x,y)$, $y \to B(y,z)$, $y \to B(\theta.y,z)$: on a $\ell_1\ell_2\ell_3 = 0$. Si ℓ_1, ℓ_2, ℓ_3 étaient linéairement indépendantes, il existerait un y tel que $\ell_i(y) = 1$ $(i=1,2,3)$, ce qui est impossible.

Supposons que $\ell_i = a\ell_j + b\ell_k$, avec $\{i,j,k\} = \{1,2,3\}$. Comme aucune des formes ℓ_1, ℓ_2, ℓ_3 n'est identiquement nulle, il est manifestement impossible qu'elles soient toutes des multiples scalaires de l'une d'elles, et ℓ_j, ℓ_k sont linéairement indépendantes. On en conclut que, si c,d sont des éléments $\neq 0$ quelconques de K, on a $ac+bd = 0$, ce qui implique évidemment que K ne contient que 2 éléments, hypothèse que nous avons exclue.

Remarque. Un raisonnement un peu plus poussé montre que, sous les hypothèses de la prop.10, toute opération de G_Q peut se représenter comme produit d'au plus m symétries par rapport à des hyperplans, où $m = \dim M$ (cf. exer.). Par ailleurs, si K contient seulement deux éléments, on peut montrer que la conclusion de la prop. 10 reste valable sauf dans le cas où M est de dimension 4 et Q d'indice 2 (cf. exerc.).