LES EXTENSIONS QUADRATIQUES DES CORPS NON COMMUTATIFS ET LEURS APPLICATIONS.

Par

JEAN DIEUDONNÉ

à Nancy.

Introduction.[1]

Dans le premier chapitre de ce travail, nous étudions le type le plus simple de surcorps d'un corps non commutatif, les extensions de rang 2 (à gauche ou à droite); alors que la structure d'une telle extension est triviale lorsqu'il s'agit de corps commutatifs, il ne paraît nullement aussi facile de la réduire à une forme canonique dans le cas général et nos résultats ne s'appliquent que lorsque le corps de base est un sous-corps *galoisien* de son extension.

Les résultats de ce chapitre sont appliqués dans les chapitres suivants à diverses questions se rattachant à la théorie des groupes classiques. Soit E un espace vectoriel à droite (de dimension finie) sur un corps K; appelons *collinéation involutive* toute application semi-linéaire de E sur lui-même (collinéation) dont le carré est une homothétie; lorsque K est isomorphe à son opposé K^0, appelons de même *corrélation involutive* toute application semi-linéaire de E sur son dual E^* (corrélation) qui est égale à sa transposée, à un facteur scalaire près. Le groupe des transformations linéaires de E en lui-même qui reproduisent une forme bilinéaire hermitienne ou alternée, à un facteur scalaire près, peut encore être défini comme formé des transformations linéaires u telles que $\psi\cdot u = \lambda\cdot\check{u}\cdot\psi$, où $\check{u}$ est la contragrédiente de u, λ un scalaire (dépendant de u) et ψ une corrélation involutive. Dans d'assez nombreuses circonstances, on doit considérer plus généralement les transformations linéaires u de E qui «permutent projectivement» (c'est-à-dire au sens précédent) avec *plusieurs* corrélations involutives $\psi_i\,(0 \leq i \leq m)$, telles que les transformations semi-linéaires $\psi_i^{-1}\psi_j$ soient des *collinéations involutives;* il revient alors au même que u

[1] Les numéros entre crochets renvoient à la bibliographie placée à la fin de ce travail.

permute projectivement avec la corrélation ψ_0 et avec chacune des m collinéations involutives $\psi_0^{-1}\psi_i\,(1 \leq i \leq m)$. Or, comme on le constatera, les transformations linéaires de E permutant projectivement avec une collinéation involutive peuvent, dans de nombreux cas, être considérées comme des transformations linéaires pour une nouvelle structure d'espace vectoriel sur E, par rapport à une *extension quadratique* du corps K; d'où la possibilité d'étudier le groupe des transformations linéaires permutant projectivement avec les ψ_i en le considérant comme un groupe de transformations linéaires par rapport à un autre corps K_0, permutant projectivement avec *une seule* corrélation involutive. On connaît depuis longtemps des exemples d'applications de cette méthode: c'est ainsi que le groupe unitaire sur le corps des nombres complexes peut être considéré comme intersection d'un groupe orthogonal et d'un groupe symplectique sur le corps des nombres réels; et de même, le groupe unitaire quaternionique peut être considéré comme intersection d'un groupe unitaire et d'un groupe symplectique sur le corps des nombres complexes. Au chapitre II, nous étudierons ce procédé sous son aspect le plus général. Nous l'appliquerons ensuite en premier lieu pour compléter les résultats de van der Waerden [14] sur les groupes orthogonaux sur un espace de dimension ≤ 6, puis pour résoudre certains problèmes sur les groupes classiques, que nous avions laissés sans réponse dans nos travaux antérieurs sur ces questions ([8] et [10]).

I. Extensions quadratiques des corps non commutatifs.

1. Soient K un corps quelconque, L un sous-corps de K tel que K soit de rang 2 sur L quand on le considère comme espace vectoriel à droite sur L; on ignore si dans ce cas K est aussi de rang 2 en tant qu'espace vectoriel à gauche sur L; il en est bien ainsi toutefois quand L est un sous-corps *galoisien* de L (cf. [5], [13] et [7]). Nous nous limiterons en principe dans ce qui suit à l'étude des extensions quadratiques K d'un corps L, qui sont *galoisiennes* sur L. La théorie de Galois des corps non commutatifs (*loc. cit.*) montre alors que L peut être un sous-corps galoisien *extérieur* ou *intérieur* de K, suivant que le centre T de K contient ou non le centre Z de L.

2. Nous commencerons par étudier le cas où L est un sous-corps galoisien *extérieur* de K, c'est-à-dire où $Z \subset T$. La théorie de Galois (voir par exemple [5], p. 65) prouve alors que L est le corps des invariants d'un *automorphisme* τ de K, tel que τ^2 soit l'automorphisme identique de K. Soit alors θ un élément de K n'appartenant pas à L; les éléments 1 et θ forment une base de K sur L (considéré

comme espace vectoriel à droite ou à gauche), et on a en particulier $\theta^2 = \theta a + b$, avec $a \in L$ et $b \in L$. Remarquons maintenant que $\theta + \theta^\tau$ est invariant par τ, donc est un élément $c \in L$. Si K n'est pas de caractéristique 2, en remplaçant θ par $\theta + \frac{c}{2}$, on peut se ramener au cas où $\theta^\tau = -\theta$; on doit alors avoir $\theta^2 = -\theta a + b$, ce qui entraîne $2\theta a = 0$, c'est-à-dire $a = 0$. Si au contraire K est de caractéristique 2, on a $c \neq 0$, sans quoi τ serait l'automorphisme identique; en remplaçant θ par θc^{-1}, on peut se ramener au cas où $c = a = 1$, et par suite $\theta^\tau = \theta + 1$.

3. Pour tout élément $x \in L$, on peut écrire

$$x\theta = u(x) + \theta x^\sigma \tag{1}$$

où $u(x)$ et x^σ sont des éléments de L; en outre, comme 1 et θ forment une base de K considéré comme espace vectoriel à gauche sur L, $x \to x^\sigma$ est une application de L *sur* lui-même; si dans (1), on remplace x par xy, l'associativité de la multiplication dans K donne aussitôt les deux relations

$$(xy)^\sigma = x^\sigma y^\sigma \tag{2}$$

$$u(xy) = x\,u(y) + u(x)\,y^\sigma. \tag{3}$$

La relation (2) et la remarque précédente prouvent donc que $x \to x^\sigma$ est un *automorphisme* de L, et (3) signifie alors que u est une *antidérivation* de L, relative à l'automorphisme σ. Si on exprime en outre que $x\theta^2 = x\theta a + xb$, on obtient, en vertu de (2) et (3), les relations

$$u^2(x) - u(x)\,a = xb - b\,x^{\sigma^2} \tag{4}$$

$$u(x^\sigma) + (u(x))^\sigma = x^\sigma a - a\,x^{\sigma^2}. \tag{5}$$

Exprimons maintenant qu'on a $(x\theta)^\tau = x\theta^\tau$ pour tout $x \in L$. Supposons en premier lieu que K ne soit pas de caractéristique 2; alors comme $\theta^\tau = -\theta$, il vient $u(x) - \theta x^\sigma = -u(x) - \theta x^\sigma$, c'est-à-dire $2u(x) = 0$, d'où $u(x) = 0$ identiquement dans L; la relation (5) est identiquement vérifiée, et la relation (4) donne

$$x^{\sigma^2} = b^{-1} x b \tag{6}$$

identiquement dans L; en d'autres termes, σ^2 est un automorphisme *intérieur*. Comme tout élément du centre Z de L permute avec θ, on a $x^\sigma = x$ pour tout $x \in Z$; de même, $b = \theta^2$ permute avec θ, donc $b^\sigma = b$.

Si au contraire K est de caractéristique 2, on a $\theta^\tau = \theta + 1$, donc on obtient la relation $u(x) + \theta x^\sigma + x^\sigma = u(x) + \theta x^\sigma + x$, c'est-à-dire $x^\sigma = x$ identiquement dans L; la relation (5) est encore identiquement vérifiée, et (4) donne

$$u(x) + u^2(x) = x b + b x \tag{7}$$

identiquement dans L; en d'autres termes, $u + u^2$ est une dérivation *intérieure*. Comme tout élément du centre Z de L permute avec θ, on a $u(x) = 0$ pour $x \in Z$; on voit de même que $u(b) = 0$.

4. Lorsque K n'est pas de caractéristique 2, l'élément θ de K n'est pas entièrement déterminé par la condition $\theta^\tau = -\theta$; tout élément $\theta' = \theta w$, où $w \in L$, a la même propriété, et réciproquement; on a alors $\theta'^2 = b w^\sigma w$; il est clair qu'on ne peut avoir $\theta'^2 = 1$, puisque θ' n'appartient pas à L; on voit donc que b *n'est pas de la forme* $x x^\sigma$ (avec $x \in L$). On notera que lorsqu'on remplace θ par $\theta' = \theta w$, l'automorphisme σ est remplacé par $x \to w^{-1} x^\sigma w$.

Cherchons enfin si σ peut être un automorphisme *intérieur*; alors, en remplaçant θ par θw pour un $w \in L$ convenable, on peut se ramener au cas où σ est l'automorphisme *identique*. Dans ce cas, θ appartient au centre de K, qui est par suite égal à $Z(\theta)$, extension quadratique séparable de Z, et K est isomorphe au *produit tensoriel* $L \otimes Z(\theta)$ sur Z. Dans tout autre cas, σ est un automorphisme extérieur de L laissant invariants les éléments de Z, ce qui (en vertu du th. de Skolem-Noether) ne peut se produire que si L est de rang *infini* sur son centre Z.

Inversement, soit L un corps de caractéristique $\neq 2$; supposons donné un automorphisme σ de L (éventuellement égal à l'automorphisme identique), laissant invariant tout élément de Z, et satisfaisant à la relation (6); supposons en outre que $b^\sigma = b$, et que b ne soit pas de la forme $x x^\sigma$. Soit K un espace vectoriel à droite de dimension 2 sur L, et soit $\{e, \theta\}$ une base de K sur L; on définit une loi de composition dans K en prenant e comme élément unité (ce qui l'identifie à l'élément unité 1 de L) et en convenant que $(\theta x)(\theta y) = b x^\sigma y$, $x(\theta y) = \theta x^\sigma y$ et $(\theta y) x = \theta (y x)$ quels que soient x et y dans L; cette multiplication est associative en raison du fait que σ est un automorphisme, et des relations $b^\sigma = b$ et (6), comme on le vérifie aisément. Pour voir que l'anneau K ainsi défini est un *corps*, il faut vérifier que si r et s sont deux éléments de L, non tous deux nuls, il existe deux éléments x, y de L tels que l'on ait

$$(\theta x + y)(\theta r + s) = (\theta r + s)(\theta x + y) = 1. \tag{8}$$

Or la seconde de ces relations équivaut aux deux équations

(9)
$$\begin{cases} b\,r^\sigma x + s\,y = 1 \\ s^\sigma x + r\,y = 0. \end{cases}$$

On peut en outre se borner au cas où $r \neq 0$; alors on tire de la seconde équation (9) que $y = -r^{-1} s^\sigma x$, d'où pour x l'équation

(10)
$$(b\,r^\sigma - s\,r^{-1} s^\sigma)\,x = 1$$

qui admet une solution dans L, puisque $b \neq (s\,r^{-1})(s\,r^{-1})^\sigma$ par hypothèse. Quant à la première relation (8), elle équivaut aux équations $b\,x^\sigma r + y\,s = 1$, $y^\sigma r + x\,s = 0$, et la première de ces équations s'écrit aussi $x\,b\,r^\sigma + y^\sigma s^\sigma = 1$, d'après (6) et la relation $b^\sigma = b$; on en déduit pour x l'équation $x\,(b\,r^\sigma - s\,r^{-1} s^\sigma) = 1$, équivalente à (10).

Reste à montrer que l'application $\theta\,x + y \to -\theta\,x + y$ est un automorphisme τ de K, ce qui se vérifie immédiatement. Cela prouve que L est un sous-corps galoisien extérieur de K, et nous avons démontré le théorème suivant:

Théorème 1. *Pour tout sous-corps galoisien extérieur L d'un corps K de caractéristique $\neq 2$, tel que K soit de rang 2 sur L, il existe un élément θ de K, formant avec 1 une base (à gauche et à droite) de K sur L, tel que $\theta^2 = b \in L$, que l'application $x \to \theta^{-1} x\,\theta$ soit un automorphisme σ de L laissant invariants b et les éléments du centre Z de L, et que b ne soit pas de la forme $x\,x^\sigma$ (pour $x \in L$). Réciproquement, la donnée d'un automorphisme σ de L laissant invariants les éléments de Z, et d'un élément $b \in L$ tel que $b^\sigma = b$, satisfaisant à (6) et qui n'est pas de la forme $x\,x^\sigma$, détermine un surcorps K de L tel que K soit de rang 2 (à droite et à gauche) sur L, que L soit sous-corps galoisien extérieur de K, et qu'il existe dans K un élément θ ayant les propriétés précédentes.*

Si $\theta\,x + y$ appartient au centre T de K, il doit permuter, avec tout élément $z \in L$, ce qui donne $y \in Z$ et $z^\sigma x = x\,z$. Si σ n'est pas un automorphisme intérieur de L, cela n'est possible que pour $x = 0$, donc $T = Z$; au contraire, si σ est un automorphisme intérieur de L, on peut supposer que σ est l'automorphisme identique, et on voit que l'on doit avoir $x \in Z$, d'où $T = Z(\theta)$.

5. Donnons un exemple où L est sous-corps galoisien extérieur de K et où σ est un automorphisme *extérieur* de L. Soit K_0 un corps commutatif de caractéristique $\neq 2$, $K_1 = K_0((X))$ le corps des séries formelles en X à coefficients dans K_0, et soit K le corps des séries formelles $\sum_n a_n(X)\,Y^n$ en Y, où les coefficients appartiennent à K_1, avec la loi de multiplication $Y^n \alpha(X) = \alpha(2^n X)\,Y^n$ (corps non commutatif de Hilbert). Soit L le sous-corps de K formé des séries ne contenant que des puissances

paires de Y; il est clair que tout élément de K peut s'écrire d'une seule manière $Yv + w$, où v et w appartiennent à L; en outre, l'application changeant Y en $-Y$ est un automorphisme de K, dont le carré est l'identité, et qui laisse invariants les éléments de L. L est un sous-corps galoisien extérieur de K, car le centre commun de K et de L est ici K_0; l'automorphisme σ de L fait correspondre à l'élément $\sum_n a_n(X)\,Y^{2n}$ l'élément $\sum_n a_n(\frac{1}{2}X)\,Y^{2n}$.

6. Reprenons l'étude de l'extension quadratique K de L lorsque K est de caractéristique 2; alors l'élément θ n'est pas entièrement déterminé par la condition $\theta^\tau = \theta + 1$; tout autre élément $\theta' = \theta + w$, où $w \in L$, a la même propriété et réciproquement; on a alors $\theta'^2 = \theta' + b + u(w) + w^2 + w$; comme on ne peut avoir $\theta'^2 = \theta'$, on voit que *b n'est pas de la forme $u(x) + x + x^2$* (avec $x \in L$). Lorsqu'on remplace θ par $\theta' = \theta + w$, la dérivation $u(x)$ est remplacée par la dérivation $x \to u(x) + xw + wx$.

Cherchons si u peut être une dérivation *intérieure*; en remplacant θ par $\theta + w$, avec un $w \in L$ convenable, on peut se ramener au cas où u est identiquement nulle. Alors, θ appartient au centre de K, qui est par suite égal à l'extension quadratique séparable $Z(\theta)$ de Z; le corps K est donc isomorphe au produit tensoriel $L \otimes Z(\theta)$ sur Z. Dans tout autre cas, u est une dérivation extérieure de L, s'annulant pour tous les éléments de Z, ce que ne peut se produire que si L est de rang *infini* sur Z ([12], p. 103).

Inversement, soit L un corps de caractéristique 2; supposons donnée une dérivation u de L (éventuellement identiquement nulle), nulle dans Z et satisfaisant à la relation (7); supposons en outre que $u(b) = 0$ et que b ne soit pas de la forme $u(x) + x + x^2$ (avec $x \in L$). Soit K un espace vectoriel à droite de dimension 2 sur L, et soit $\{e, \theta\}$ une base de K sur L; on définit une loi de composition dans K en prenant e comme élément unité (identifié à l'élément unité 1 de L) et en convenant que $(\theta x)(\theta y) = \theta(x + u(x))y + bxy$, $x(\theta y) = \theta xy + u(x)y$ et $(\theta y)x = \theta(yx)$ quels que soient x et y dans L; cette multiplication est associative, comme on le vérifie sans peine en raison du fait que u est une dérivation, et des relations (7) et $u(b) = 0$. Pour voir que l'anneau K ainsi défini est un *corps*, il faut vérifier que si r et s sont deux éléments de L, non tous deux nuls, il existe deux éléments x, y de L tels que

$$(\theta x + y)(\theta r + s) = (\theta r + s)(\theta x + y) = 1. \tag{11}$$

Or, la seconde de ces relations équivaut aux deux équations

$$(12) \qquad \begin{cases} (u(r) + r + s)x + ry = 0 \\ (br + u(s))x + sy = 1. \end{cases}$$

On peut se borner au cas où $r \neq 0$; alors on tire de la première équation (12) que $y = -r^{-1}(u(r) + r + s)x$, d'où pour x l'équation

$$(13) \qquad (b + u(s)r^{-1} + sr^{-1}u(r)r^{-1} + sr^{-1} + (sr^{-1})^2)rx = 1$$

qui admet une solution dans L, car on a par hypothèse

$$b + u(sr^{-1}) + sr^{-1} + (sr^{-1})^2 \neq 0, \text{ et } u(sr^{-1}) = u(s)r^{-1} + sr^{-1}u(r)r^{-1},$$

u étant une dérivation. Quant à la première relation (11), elle est équivalente aux équations

$$(14) \qquad \begin{cases} (u(x) + x)r + xs + yr = 0 \\ bxr + u(y)r + ys = 1. \end{cases}$$

Supposant encore que $r \neq 0$, on tire de la première équation (14) que $y = x + u(x) + xsr^{-1}$, d'où, en portant dans la seconde équation (14), et tenant compte de (7), l'équation pour x

$$x(b + u(s)r^{-1} + sr^{-1}u(r)r^{-1} + sr^{-1} + (sr^{-1})^2)r = 1$$

qui est équivalente à (13).

Reste à vérifier que l'application $\theta x + y \to \theta x + (x + y)$ est un automorphisme τ de K, ce qui est immédiat. Le corps L est donc un sous-corps galoisien extérieur de K, et nous avons obtenu le résultat suivant:

Théorème 2. *Pour tout sous-corps galoisien extérieur L d'un corps K de caractéristique 2, tel que K soit de rang 2 sur L, il existe un élément θ de K, formant avec 1 une base (à gauche et à droite) de K sur L, tel que $\theta^2 + \theta = b \in L$, que l'application $x \to x\theta + \theta x$ soit une dérivation u de L, nulle pour $x = b$ et pour les éléments du centre Z de L, et que b ne soit pas de la forme $x + x^2 + u(x)$ (pour $x \in L$). Réciproquement, la donnée d'une dérivation u de L s'annulant dans Z, et d'un élément $b \in L$ tel que $u(b) = 0$, satisfaisant à (7) et qui n'est pas de la forme $x + x^2 + u(x)$, détermine un surcorps K de L tel que K soit de rang 2 (à droite et à gauche) sur L, que L soit sous-corps galoisien extérieur de K, et qu'il existe dans K un élément θ ayant les propriétés précédentes.*

Si $\theta x + y$ appartient au centre T de K, il doit permuter avec tout élément $z \in L$, ce qui donne $x \in Z$ et $u(z)x + zy = yz$. Si u n'est pas une dérivation intérieure de Z, cela n'est possible que pour $x=0$, donc $T=Z$; au contraire, si u est une dérivation intérieure de L, on peut supposer que $u=0$, et on doit alors avoir $x \in Z$, d'où $T=Z(\theta)$.

Je n'ai pu obtenir d'exemple explicite de corps K et L satisfaisant aux conditions du th.2 et pour lesquels $Z=T$.

7. Etudions maintenant le cas où L est un sous-corps galoisien *intérieur* de K, c'est-à-dire le cas où le centre Z de L, *commutant* de L dans K, est une *extension quadratique* du centre T de K. Considérons les transformés $w Z w^{-1}$ de Z par les automorphismes intérieurs de K; le plus petit corps contenant tous ces corps est nécessairement K lui-même, en vertu d'un théorème de R. Brauer et L. K. Hua, généralisant un résultat antérieur de H. Cartan ([4], [5] et [11]). Il existe donc un élément $\theta \in K$, non contenu dans L et tel que $T(\theta)$ soit une extension quadratique de T; on peut par suite prendre pour base de K sur L (à gauche ou à droite) l'élément unité de L et l'élément θ.

Supposons en premier lieu que K ne soit pas de caractéristique 2. On peut alors supposer que $\theta^2=a$, où $a \in T$. On a encore alors les relations (1), (2) et (3), et les relations (4) et (5) deviennent ici

$$u^2(x)=a(x-x^{\sigma^2}) \tag{15}$$

$$u(x^\sigma)+(u(x))^\sigma=0. \tag{16}$$

On notera en outre que L est le corps commutant de Z dans K, donc on ne peut avoir identiquement $x\theta=\theta x$ dans Z.

Soit alors x un élément quelconque de Z, y un élément quelconque de L; appliquant la relation (3) à xy et à yx, il vient, puisque x est permutable à tout élément de L,

$$u(y)(x^\sigma-x)=u(x)y^\sigma-y\,u(x). \tag{17}$$

Nous allons montrer qu'on ne peut avoir identiquement $x^\sigma=x$ dans Z. En effet, s'il en était ainsi, on ne pourrait avoir identiquement $u(x)=0$ dans Z, car on aurait alors $x\theta=\theta x$ identiquement dans Z, ce qu'on a vu être impossible; si $x \in Z$ est tel que $u(x)=c \neq 0$, on aurait alors identiquement dans L, $y^\sigma=c^{-1}yc$. Remplaçons alors θ par $\theta'=\theta c^{-1}$; on a pour tout $y \in L$

$$y\theta'=u(y)c^{-1}+\theta' y=u'(y)+\theta' y$$

et le raisonnement du n° 3 montre que u' est une *dérivation* dans L.

Répétant le raisonnement du début de ce n°, on voit alors que pour $z \in Z$ et $y \in L$, on a

$$u'(z)\, y - y\, u'(z) = 0$$

autrement dit que $u'(z) \in Z$; la restriction de u' à Z est donc une *dérivation* de ce corps, qui est nulle dans T. Mais comme Z est une extension séparable de T, une telle dérivation est nécessairement identiquement nulle dans Z ([3], p. 140); on aurait donc $z\,\theta' = \theta' z$ pour tout $z \in Z$, et on a vu ci-dessus que c'est impossible.

On peut donc trouver $x \in Z$ tel que $x^\sigma \neq x$; d'ailleurs, comme σ est un automorphisme de L, on a $x^\sigma \in Z$; en posant $a = (x^\sigma - x)^{-1} u(x)$, la relation (17) donne identiquement

(18) $$u(y) = a\, y^\sigma - y\, a.$$

L'identité (16) s'écrit alors

(19) $$(a^\sigma + a)\, y^{\sigma^2} - y^\sigma (a^\sigma + a) = 0.$$

On va en déduire que $a^\sigma = -a$; dans le cas contraire, (19) montrerait que l'automorphisme σ de L est un automorphisme *intérieur*, qui laisserait en particulier invariant chaque élément de Z, et nous avons vu ci-dessus que c'est impossible.

Posons alors $\varrho = \theta + a$; la relation (18) donne identiquement dans L,

(20) $$y\,\varrho = \varrho\, y^\sigma.$$

D'après (18), on a $u(a) = a\,a^\sigma - a^2 = -2\,a^2$, d'où $a\,\theta = -2\,a^2 - \theta\, a$, et par suite $\varrho^2 = (\theta + a)^2 = \theta^2 + \theta\, a + a\,\theta + a^2 = \theta^2 - a^2 = \alpha - a^2 = c \in L$. Comme $c\,\varrho = \varrho\, c = \varrho^3$, on a $c^\sigma = c$; d'autre part la relation (4) donne

(21) $$y^{\sigma^2} = c^{-1} y\, c$$

dans L.

8. L'élément ϱ de K n'est pas entièrement déterminé par la condition que l'application $y \to \varrho^{-1} y\,\varrho$ soit un automorphisme de L (nécessairement *extérieur* comme on l'a vu). Si on écrit que $\varrho' = \varrho\, r + s$ est tel que $y\,\varrho' = \varrho' y^{\sigma'}$ où σ' est un automorphisme extérieur de L, il vient $y^\sigma r = r\, y^{\sigma'}$ et $y\, s = s\, y^{\sigma'}$ identiquement, ce qui n'est possible que si $s = 0$. Alors $y^{\sigma'} = r^{-1} y^\sigma r$ et $\varrho'^2 = \varrho^2 r^\sigma r = c\, r^\sigma r$. On notera qu'on a nécessairement $\varrho'^2 \neq 1$, puisque ϱ' n'appartient pas à Z; on en conclut que *c n'est pas de la forme $x\,x^\sigma$* (avec $x \in L$).

Inversement, soit L un corps de caractéristique $\neq 2$; supposons donné un automorphisme σ de L, dont la restriction à Z ne soit pas l'automorphisme identique, et qui satisfasse à la relation (21); supposons en outre que $c^\sigma = c$, et que c ne soit pas de la forme $x x^\sigma$. Si K est un espace vectoriel à droite de dimension 2 sur L, on définit sur K une structure de corps de la même façon qu'au n° 4; on voit en outre qu'un élément du centre T de K est nécessairement contenu dans L et invariant par σ, et réciproquement; Z est donc une extension quadratique du centre T de K, et par suite L est sous-corps galoisien *intérieur* de K. En résumé, nous avons démontré le théorème suivant:

Théorème 3. *Pour tout sous-corps galoisien intérieur L d'un corps K de caractéristique $\neq 2$, tel que K soit de rang 2 sur L, il existe un élément ϱ de K, formant avec 1 une base (à gauche et à droite) de K sur L, tel que $\varrho^2 = c \in L$, que l'application $x \to \varrho^{-1} x \varrho$ soit un automorphisme σ de L laissant invariant c et dont la restriction à Z ne soit pas l'identité, et que c ne soit pas de la forme $x x^\sigma$ (pour $x \in L$). Réciproquement, la donnée d'un automorphisme σ de L dont la restriction à Z n'est pas l'identité, et d'un élément $c \in L$ tel que $c^\sigma = c$, satisfaisant à (21), et qui n'est pas de la forme $x x^\sigma$, détermine un surcorps K de L tel que K soit de rang 2 (à droite et à gauche) sur L, que L soit sous-corps galoisien intérieur de K, et qu'il existe dans K un élément ϱ ayant les propriétés précédentes.*

Il résulte en outre de ce qui précède qu'il y a lieu d'identifier deux extensions quadratiques K_1, K_2 de L, du type décrit dans le th.3, lorsque les automorphismes extérieurs σ_1, σ_2 correspondants de L ne diffèrent que par un automorphisme intérieur de L.

9. Cette dernière remarque montre en particulier que lorsque L est de rang *fini* sur son centre, la donnée de la *restriction* à Z de l'automorphisme σ (qui est un automorphisme de Z de carré l'identité, formant avec l'identité le groupe de Galois de Z sur T) détermine complètement l'extension quadratique K: il résulte en effet du th. de Skolem-Noether que deux automorphismes extérieurs σ_1, σ_2 de L qui coïncident dans Z ne diffèrent que par un automorphisme intérieur.

Il resterait à savoir si tout automorphisme involutif de Z est la restriction à Z d'un automorphisme σ de L satisfaisant aux conditions du th.3, lorsque L est un corps quelconque ou plus particulièrement lorsque L est de rang fini sur Z: problème que nous ne savons pas aborder actuellement.

10. Un cas particulier intéressant du th.3 correspond au cas où l'élément c de L appartient au *centre* Z, ou est produit d'un élément de Z et d'un élément de la forme $x x^\sigma$. Alors σ est un automorphisme *involutif* de L, ou ne diffère d'un tel automorphisme que par un automorphisme intérieur. On peut toujours supposer

alors que σ est involutif; le corps M des invariants de σ est alors un *sous-corps galoisien extérieur* de L, de centre T, et L est isomorphe au produit tensoriel $Z \otimes M$ (par rapport à T). Si R est l'extension quadratique (non commutative) de Z engendrée par ϱ, on voit aussitôt alors que K est isomorphe au produit tensoriel $R \otimes M$ (par rapport à T), et que R est un *corps de quaternions généralisé* sur le corps T.

On peut se demander si le cas précédent n'est pas le cas général lorsque L est de rang fini sur son centre Z; nous ne savons pas non plus répondre à cette question, mais nous allons montrer par un exemple que, lorsque L est de rang *infini* sur Z, l'élément c n'est pas toujours le produit d'un élément du centre Z par un élément de la forme $x x^{\sigma}$.

Soit K_0 un corps commutatif de caractéristique $\neq 2$, admettant un automorphisme involutif $\xi \to \bar{\xi}$ distinct de l'identité (par exemple le corps des nombres complexes); soit $K_1 = K_0((X))$ le corps des séries formelles en X à coefficients dans K_0, auquel on étend l'automorphisme involutif de K_0 en le faisant agir sur les coefficients de chaque série formelle; on notera encore $u \to \bar{u}$ l'automorphisme de K_1 ainsi défini. Soit L le corps non commutatif de séries formelles $\sum_n \alpha_n(X) Y^n$ en Y, à coefficients dans K_1, et où la multiplication est définie par $Y^n \alpha(X) = \alpha(4^n X) Y^n$. Le centre de L est le corps K_0. Soit alors σ l'automorphisme de L qui, à toute série formelle $\sum_n \alpha_n(X) Y^n$, fait correspondre la série formelle $\sum_n 2^n \bar{\alpha}_n(X) Y^n$; comme $X^{-1} Y X = 4 Y$, σ^2 est l'automorphisme intérieur $z \to c^{-1} z c$, avec $c = X$; il résulte aussitôt de la définition de σ que c ne peut être de la forme $u u^{\sigma}$, avec $u \in L$, car u ne devrait pas dépendre de Y, c'est-à-dire appartenir à K_1, et dans K_1, X n'est pas de la forme $v \bar{v}$, comme le montre l'examen des termes de plus bas degré du produit $v \bar{v}$.

11. Continuons l'étude du cas où L est sous-corps galoisien *intérieur* de K, en considérant maintenant les cas où K est de caractéristique 2. Alors Z peut être une extension séparable ou une extension inséparable de T; nous commencerons par examiner le cas où Z est une extension *séparable* de T. On peut alors supposer que $\theta^2 = \theta + \alpha$, où $\alpha \in T$ (θ ayant le même sens qu'au n° 7); les relations (4) et (5) deviennent

$$u^2(x) + u(x) = \alpha(x^{\sigma^2} + x) \tag{22}$$

$$(u(x))^{\sigma} + u(x^{\sigma}) = x^{\sigma^2} + x^{\sigma}. \tag{23}$$

Comme au n° 7, on voit qu'on ne peut avoir identiquement $x^{\sigma} = x$ dans Z, parce que Z est une extension séparable de T. Procédant comme au n° 7, on voit alors qu'il existe $a \in L$ tel que l'on ait identiquement

$$u(y) = a y^{\sigma} + y a. \tag{24}$$

L'identité (23) donne alors

$$(a^{\sigma} + a + 1) y^{\sigma^2} = y^{\sigma} (a^{\sigma} + a + 1).$$

On en déduit que $a^{\sigma} = a + 1$, sans quoi σ serait un automorphisme intérieur, laissant donc invariant chaque élément de Z, ce qu'on a vu être impossible. En posant $\varrho = \theta + a$, la relation (24) montre qu'on a identiquement dans L la relation (20). D'autre part, on a $u(a) = a a^{\sigma} + a^2 = a^2 + a + a^2 = a$, d'où $a \theta = a + \theta (a + 1)$, et par suite $\varrho^2 = (\theta + a)^2 = \theta^2 + \theta a + a \theta + a^2 = \theta + \alpha + \theta a + a + \theta (a + 1) + a^2 = a^2 + a + \alpha = c \in L$. On a évidemment encore $c^{\sigma} = c$, et la relation (21) dérive encore de (4).

Les considérations du n° 8 sont alors valables sans aucune restriction, et par suite:

Théorème 4. *L'énoncé du théorème 3 demeure valable sans modification lorsque K est de caractéristique 2 et que le centre Z de L est une extension séparable du centre T de K.*

Les remarques faites aux n^{os} 9 et 10 s'appliquent aussi au cas envisagé ici: il faut seulement, dans l'exemple donné au n° 10, remplacer le nombre 2 par un élément inversible et $\neq 1$ du corps K_1.

12. Supposons à présent que Z soit une extension *inséparable* de T; on peut alors supposer que $\theta^2 = \alpha \in T$; en outre, la restriction à Z de l'automorphisme σ est nécessairement l'identité, et Z est engendré par un élément x_0 tel que $x_0^2 = \alpha$; comme on ne peut avoir identiquement $\theta x = x \theta$ dans Z, on a nécessairement $\theta x_0 \neq x_0 \theta$, c'est-à-dire $a = u(x_0) \neq 0$. La formule (17) donne alors identiquement $y^{\sigma} = a^{-1} y a$. Remplaçant θ par $\varrho = \theta a^{-1}$, on a identiquement dans L

$$y \varrho = v(y) + \varrho y \tag{26}$$

où v est une *dérivation* de L; cette dérivation est nécessairement *extérieure*, sans quoi elle s'annulerait dans Z, et par suite on aurait $x \varrho = \varrho x$ pour tout $x \in Z$, ce qui est impossible. D'ailleurs, pour tout $x \in Z$, et tout $y \in L$, la relation (17) (appliquée à ϱ et v) montre qu'on a $v(x) y - y v(x) = 0$, donc $v(x) \in Z$; autrement dit, la restriction de v à Z est une *dérivation* de ce corps, et l'ensemble des $x \in Z$ tels que $v(x) = 0$ est le centre T de K. D'ailleurs, on a $a^{\sigma} = a$ et d'autre part, en vertu de (15), $u(a) = u^2(x_0) = 0$, ce qui montre que a est permutable avec θ; on en conclut que $\varrho^2 = \alpha a^{-2} = b \in L$. La formule (4) montre d'ailleurs que

$$v^2(x) = xb + bx \tag{27}$$

dans L; en d'autres termes, v^2 est une dérivation *intérieure*; comme ϱ et b sont permutables, on a enfin $v(b) = 0$.

13. Cherchons à déterminer tous les éléments $\varrho' = \varrho r + s$ de K tels que $y \to y\varrho' + \varrho' y$ soit une dérivation de L (nécessairement extérieure) et que $\varrho'^2 \in L$. En écrivant que $y\varrho' = v'(y) + \varrho' y$, où v' est une dérivation de L, il vient $yr = ry$ et $v'(y) = v(y)r + ys + sy$ identiquement; la première de ces relations montre donc que $r \in Z$. On a ensuite $\varrho'^2 = br^2 + v(s)r + s^2 + \varrho v(r)r$, et il faut donc $v(r) = 0$, c'est-à-dire $r \in T$. On a évidemment $\varrho' \neq 0$; comme $v(s)r^{-1} = v(sr^{-1})$ et $s^2 r^{-2} = (sr^{-1})^2$, puisque $r \in T$, on voit que b *n'est pas de la forme* $x^2 + v(x)$ (avec $x \in L$).

Inversement, soit L un corps de caractéristique 2; supposons donnée une dérivation v de L, dont la restriction au centre Z ne soit pas nulle, et qui satisfasse à la relation (27); supposons en outre que $v(b) = 0$, et que b ne soit pas de la forme $x^2 + v(x)$. Soit K un espace vectoriel à droite de dimension 2 sur K, dont 1 et ϱ forment une base; on définit une loi de composition dans K en convenant que $(\varrho x)(\varrho y) = \varrho v(x)y + bxy$, $x(\varrho y) = \varrho xy + v(x)y$, et $(\varrho y)x = \varrho(yx)$ quels que soient x et y dans L; cette multiplication est associative, en raison du fait que v est une dérivation, et des relations (27) et $v(b) = 0$. Pour voir que l'anneau K ainsi défini est un *corps*, il faut vérifier que si r et s sont deux éléments de L, non tous deux nuls, il existe deux éléments x, y de L tels que

$$(\varrho x + y)(\varrho r + s) = (\varrho r + s)(\varrho x + y) = 1. \tag{28}$$

La seconde de ces relations équivaut aux deux équations

$$\begin{cases} (v(r) + s)x + ry = 0 \\ (br + v(s))x + sy = 1. \end{cases} \tag{29}$$

On peut se borner au cas où $r \neq 0$; on tire de la première équation (29) que $y = -r^{-1}(v(r) + s)x$, d'où pour x l'équation

$$(b + v(s)r^{-1} + sr^{-1}v(r)r^{-1} + (sr^{-1})^2)rx = 1 \tag{30}$$

qui admet une solution dans L, car on a par hypothèse

$$b + v(sr^{-1}) + (sr^{-1})^2 \neq 0, \text{ et } v(sr^{-1}) = v(s)r^{-1} + sr^{-1}v(s)r^{-1},$$

v étant une dérivation. Quant à la première relation (28), elle équivaut aux équations

$$(31) \qquad \begin{cases} v(x)r + xs + yr = 0 \\ bxr + v(y)r + ys = 1. \end{cases}$$

Supposant encore que $r \neq 0$, on en tire $y = v(x) + x s r^{-1}$, d'où, en portant dans la seconde équation (31), et tenant compte de (27), l'équation pour x

$$x(b + v(s)r^{-1} + sr^{-1}v(r)r^{-1} + (sr^{-1})^2)r = 1$$

qui est équivalente à (30).

On voit en outre qu'un élément $\varrho r + s$ du centre T de K est tel que $v(x)r = xs + sx$ pour tout $x \in L$; cela entraîne d'abord $r = 0$, puisque v n'est pas une dérivation intérieure, puis $s \in Z$; en outre, en écrivant que $\varrho s = s\varrho$, on voit qu'on doit avoir $v(s) = 0$, et on vérifie aisément que ces conditions sont suffisantes; T est par suite l'ensemble des éléments de Z où s'annule la dérivation v (qui n'est pas identiquement nulle dans Z et est telle que $v^2(x) = 0$ dans Z); on sait [3] que cela signifie que Z est une extension quadratique *inséparable* de T, et par suite L est sous-corps galoisien *intérieur* de K. En résumé, on a le théorème suivant:

Théorème 5. *Pour tout sous-corps galoisien intérieur L d'un corps K de caractéristique 2, tel que K soit de rang 2 sur L, et Z une extension inséparable de T, il existe un élément ϱ de K, formant avec 1 une base (à gauche et à droite) de K sur L, tel que $\varrho^2 = b \in L$, que l'application $x \to x\varrho + \varrho x$ soit une dérivation v de L s'annulant en b et non identiquement nulle dans Z, et que b ne soit pas de la forme $v(x) + x^2$ (pour $x \in L$). Réciproquement, la donnée d'une dérivation v de L, non identiquement nulle dans Z, et d'un élément $b \in L$ tel que $v(b) = 0$, satisfaisant à (27), et qui n'est pas de la forme $v(x) + x^2$, détermine un surcorps K de L tel que K soit de rang 2 (à droite et à gauche) sur L, que L soit sous-corps galoisien intérieur de K, dont le centre est une extension inséparable du centre de K, et qu'il existe dans K un élément ϱ ayant les propriétés précédentes.*

En outre, il y a lieu d'identifier deux extensions quadratiques K_1, K_2 de L du type décrit dans le th.5, lorsque les dérivations extérieures v_1, v_2 correspondantes ne diffèrent que par une dérivation intérieure de L, ou par un facteur nul pour chacune d'elles et appartenant au centre de L. En particulier, si L est de rang *fini* sur son centre Z, la donnée de la *restriction* à Z de la dérivation v détermine complètement (à un isomorphisme près) l'extension quadratique K, car deux dérivations de L qui coïncident dans Z ne diffèrent alors que par une dérivation intérieur ([12], p. 103).

Lorsque $b \in Z$, la dérivation v est involutive; le sous-corps R de K engendré par Z et ϱ est alors, comme on le vérifie aussitôt, une extension quadratique (non commutative) de Z (parce que $\varrho^2 \in Z$ et que $\varrho z + z\varrho \in Z$ pour tout $z \in Z$). Le sous-corps M de L formé des x tels que $v(x) = 0$ peut aussi être considéré comme le *commutant* de R dans K, et comme ϱ n'appartient pas à L, $R \cap M$ est identique à $Z \cap M$, c'est-à-dire au centre T de K. Par suite, K est alors isomorphe au produit tensoriel $R \otimes M$ (par rapport à T), et R est un *corps réflexif* ([8], p. 72) de rang 4 sur T.

Je ne suis pas parvenu à obtenir des exemples où b n'appartienne pas à Z lorsque L est de caractéristique 2.

14. Dans tout ce qui suit, nous allons nous limiter aux corps *de caractéristique* $\neq 2$. Soit K un tel corps, et L un sous-corps galoisien de K tel que K soit de rang 2 sur L; les th. 1 et 3 montrent donc qu'il existe un élément $\varrho \in K$, formant avec 1 une base de K sur L, tel que $\varrho^2 = c \in L$, que $x \to \varrho^{-1} x \varrho$ soit un automorphisme σ de L laissant invariant c, c n'étant pas de la forme $x x^\sigma$ (avec $x \in L$). Supposons en outre donné un *antiautomorphisme involutif* de K, que nous noterons $z \to \bar{z}$, et supposons que cet antiautomorphisme *laisse L invariant*; nous allons étudier sa restriction à L.

Remarquons d'abord que l'on doit avoir $\bar{\varrho}^2 = \bar{c} \in L$, et que l'automorphisme $z \to \bar{\varrho}^{-1} x \bar{\varrho}$ laisse invariant L; on doit donc avoir $\bar{\varrho} = \varrho b$, où $b \in L$. Si on écrit alors que $\overline{\overline{\varrho x}} = \varrho x$ et $\overline{\varrho x} = \bar{x} \cdot \bar{\varrho}$ pour tout $x \in L$, ainsi que la relation $\bar{\varrho}^2 = \bar{c}$, on aboutit sans peine, après quelques transformations, aux conclusions suivantes: dans L, l'automorphisme σ et l'antiautomorphisme $x \to \bar{x}$ sont permutables «à un automorphisme intérieur près», c'est-à-dire qu'il existe $h \in L$ tel que l'on ait

$$\overline{x^\sigma} = h \cdot \bar{x}^\sigma \cdot h^{-1} \tag{32}$$

les constantes c et h vérifiant les trois relations

$$c^\sigma = c, \quad \bar{h} = h, \quad \bar{c}\, c = h\, h^\sigma \tag{33}$$

et étant liées à b par la relation

$$b = h^{-1} \bar{c} \tag{34}$$

qui entraîne en particulier, compte tenu de (33), que

$$b^\sigma = c^{-1} h, \quad \bar{b} = c\, h^{-1}, \quad \overline{b^\sigma} = h\, \bar{c}^{-1}, \quad \bar{b}^\sigma = \bar{c}^{-1} h.$$

Inversement, supposons donné sur L un antiautomorphisme involutif $x \to \bar{x}$ satisfaisant à (32), les constantes c et h étant liées par (33). On constate sans peine qu'on *prolonge* cet antiautomorphisme en un antiautomorphisme involutif $z \to \bar{z}$ de K, en posant, pour $z = x + \varrho y$, $\bar{z} = \bar{x} + \varrho \bar{y}^\sigma b$, où $b = h^{-1} \bar{c}$.

15. On raisonne de même lorsqu'il existe un automorphisme τ de K laissant invariant L. On doit encore avoir $\varrho^\tau = \varrho a$, avec $a \in L$. En écrivant que $(x \varrho)^\tau = x^\tau \varrho a$ pour tout $x \in L$, ainsi que la relation $(\varrho^\tau)^2 = c^\tau$, on voit que dans L les automorphismes σ et τ sont permutables «à un automorphisme intérieur près»; de façon précise on a

$$x^{\sigma\tau} = a^{-1} x^{\tau\sigma} a \tag{35}$$

les constantes a et c étant liées par la relation

$$a^\sigma a = c^{-1} c^\tau. \tag{36}$$

Inversement, si on s'est donné sur L un automorphisme τ, satisfaisant à (35), avec la relation (36) entre a et c, on vérifie sans peine que l'automorphisme τ peut s'étendre à K en posant, pour $z = x + \varrho y$, $z^\tau = x^\tau + \varrho a y^\tau$.

Si l'automorphisme τ et l'antiautomorphisme $x \to \bar{x}$ sur L sont permutables à un automorphisme intérieur près, c'est-à-dire si on a

$$\overline{x^\tau} = e\, \bar{x}^\tau e^{-1} \qquad (e \in L) \tag{37}$$

on constate de même que cette relation s'étend à K moyennant la condition

$$\bar{a}^\sigma b e = e^\sigma a b^\tau. \tag{38}$$

Enfin, si on a un second automorphisme τ' sur L du même type que τ (donc prolongeable à K) et tel que l'on ait

$$x^{\tau\tau'} = l\, x^{\tau'\tau} l^{-1} \tag{39}$$

cette relation s'étend encore à K moyennant la condition

$$a' a^{\tau'} l = l^\sigma a a'^\tau. \tag{40}$$

II. Corrélations involutives et extensions quadratiques.

16. Soit K un corps (de caractéristique $\neq 2$) admettant un antiautomorphisme ϖ (qui peut être l'identité si K est commutatif), et soit E un espace vectoriel à droite de dimension n sur K. Une *forme bilinéaire hermitienne* $f(x, y)$ est une application de $E \times E$ dans K, additive en x et y et linéaire en y (c'est-à-dire telle que $f(x, y\alpha) = f(x, y)\alpha$), et telle que l'on ait

$$f(y, x) = r^{-1} (f(x, y))^\varpi \tag{41}$$

identiquement. Ceci entraîne aussitôt $f(x, y) = r^{-1}(f(x, y))^{\varpi^2} r^{-\varpi}$, et si $f(x, y)$ n'est pas identiquement nulle, elle prend des valeurs arbitraires dans K, comme on le voit en remplaçant y par $y\alpha$. L'antiautomorphisme ϖ doit donc satisfaire à l'identité

$$\xi^{\varpi^2} = r\,\xi\,r^{\varpi} \tag{42}$$

Pour un ξ quelconque dans K, considérons alors l'élément $\xi + r^{\varpi}\xi^{\varpi}$; si cet élément est nul pour tout $\xi \in K$, on a nécessairement, en faisant $\xi = 1$, $r^{\varpi} = -1$, d'où $r = -1$, et par suite $\xi^{\varpi} = \xi$; ce cas ne peut donc se produire que si K est commutatif, ϖ l'identité, et f une forme bilinéaire *alternée*. Nous écarterons ce cas dans tout ce qui suit (cf. n° 22, note 1). Il existe alors un $\zeta \in K$ tel que $q = \zeta + r^{\varpi}\zeta^{\varpi} \neq 0$; or, on a $q^{\varpi} = \zeta^{\varpi} + r\,\zeta\,r\,r^{\varpi} = r\,q$, puisque d'après (42) on a $r\,r^{\varpi} = 1$; on peut donc écrire $r = q^{\varpi} q^{-1}$. Si alors on désigne par $\xi \to \bar{\xi}$ l'antiautomorphisme $\xi \to (q\,\xi\,q^{-1})^{\varpi}$, et par $g(x, y)$ la forme $q^{-1} f(x, y)$, on constate aisément que $\bar{\bar{\xi}} = \xi$ et $g(y, x) = \overline{g(x, y)}$. Nous pouvons donc toujours nous ramener à l'étude des formes hermitiennes correspondant à un antiautomorphisme *involutif* $\xi \to \bar{\xi}$ et pour lesquelles on a $r = 1$. Nous ne considérerons en outre que de telles formes de rang maximum n (formes non dégénérées).

Désignons par E^* le dual de E (espace vectoriel à gauche sur K), par $\langle x', x\rangle$ la forme bilinéaire canonique sur $E^* \times E$. Pour toute forme bilinéaire f sur $E \times E$ (telle que $f(x, y\alpha) = f(x, y)\alpha$ et $f(x\alpha, y) = \bar{\alpha} f(x, y)$), l'application $y \to f(x, y)$ est une forme linéaire $\psi(x) \in E^*$ et on a $f(x, y) = \langle \psi(x), y\rangle$; en outre $\psi(x\alpha) = \bar{\alpha}\,\psi(x)$, autrement dit, ψ est une application semi-linéaire (relative à $\xi \to \bar{\xi}$) de E dans E^*. Par définition, la transposée ${}^t\psi$ de ψ est l'application semi-linéaire de E dans E^* (relative au même antiautomorphisme) telle que

$$\langle \psi(x), y\rangle = \overline{\langle {}^t\psi(y), x\rangle};$$

en d'autres termes, ${}^t\psi(y)$ est la forme linéaire $x \to \overline{f(x, y)}$ sur E.

Cela étant, si $f(y, x) = \overline{f(x, y)}$, on a ${}^t\psi = \psi$, et si f est de rang n, ψ est aussi de rang n; il y a donc correspondance biunivoque entre corrélations ψ telles que ${}^t\psi = \psi$ et formes hermitiennes de rang n.

17. Supposons maintenant que L soit un sous-corps galoisien de K tel que K soit de rang 2 sur L, les notations ϱ, c et σ ayant même sens qu'au n° 14; supposons comme au n° 14 que l'antiautomorphisme $\xi \to \bar{\xi}$ laisse invariant L; on a alors $\bar{\varrho} = \varrho\,b$, et les relations (32), (33) et (34). On peut écrire $f(x, y) = f_1(x, y) + \varrho\,f_2(x, y)$, où f_1 et f_2 sont des applications de $E \times E$ dans L. Remarquons d'abord que E peut être considéré comme espace vectoriel à droite de dimension $2n$ sur L,

espace que nous noterons E_0; f_1 est alors une forme bilinéaire sur $E_0 \times E_0$. La relation $f(y, x) = \overline{f(x, y)}$ donne d'abord $f_1(y, x) = \overline{f_1(x, y)}$, donc f_1 est *hermitienne*; d'autre part, on a $\varrho f_2(y, x) = \overline{f_2(x, y)}\,\bar{\varrho}\, b$, ce qui donne $f_2(y, x) = \overline{f_2(x, y)}^{\sigma} b$. Considérons d'autre part l'application $x \to x\varrho$ de E_0 sur lui-même, que nous désignerons par u_0; pour tout $\lambda \in L$, on a $u_0(x\lambda) = x\lambda\varrho = x\varrho\lambda^{\sigma} = u_0(x)\lambda^{\sigma}$, autrement dit, u_0 est une collinéation de E_0 relative à l'automorphisme σ de L; en outre, comme $u_0^2(x) = x\varrho^2 = xc$, u_0 est une collinéation involutive de E_0. Cela étant, on a par hypothèse $f(x\varrho, y) = \bar{\varrho} f(x, y)$, ce qui s'écrit $f_1(x\varrho, y) + \varrho f_2(x\varrho, y) = c b^{\sigma} f_2(x, y) + \varrho b f_1(x, y)$; par suite $f_2(x, y) = b^{-\sigma} c^{-1} f_1(u_0(x), y)$ et $f_2(u_0(x), y) = b f_1(x, y)$, ces deux relations étant d'ailleurs équivalentes en raison de (33) et (34). Enfin, on a, d'après ce qui précède, $f_1(u_0(x), u_0(y)) = c b^{\sigma} f_2(x, u_0(y)) = c b^{\sigma} \overline{f_2(u_0(y), x)}^{\sigma} b = c b^{\sigma} \overline{f_1(y, x)}^{\sigma} \bar{b}^{\sigma} b = h(f_1(x, y))^{\sigma}$ en raison de (33) et (34).

18. Réciproquement, soit L un corps admettant un antiautomorphisme involutif $\xi \to \bar{\xi}$ et un automorphisme σ tel que $\xi^{\sigma^2} = c^{-1}\xi c$; nous supposons en outre que ces deux transformations vérifient (32) et (33), et que c n'est pas de la forme $\lambda\lambda^{\sigma}$ (pour $\lambda \in L$). Soit E_0 un espace vectoriel à droite sur L, de dimension *paire* $2n$ et soit u_0 une collinéation de E_0 relative à l'automorphisme σ, et telle que $u_0^2(x) = xc$. Nous avons vu qu'on peut alors former une extension quadratique K de L, ayant pour base 1 et ϱ sur L, avec $\varrho^2 = c$ et $\xi^{\sigma} = \varrho^{-1}\xi\varrho$ pour $\xi \in L$; en outre, on peut prolonger à K l'antiautomorphisme $\xi \to \bar{\xi}$ de L, en posant $\bar{\varrho} = \varrho b$. On en déduit tout d'abord qu'on peut définir sur E_0 une structure d'espace vectoriel à droite *par rapport à K*, en posant $x(\xi + \varrho\eta) = x\xi + u_0(x)\eta$ $(\xi \in L, \eta \in L)$; la vérification des axiomes des espaces vectoriels résulte des relations $u_0(x\lambda) = u_0(x)\lambda^{\sigma}$ et $u_0^2(x) = xc$.

Supposons en second lieu donnée sur E_0 une forme bilinéaire hermitienne f_1 (pour l'antiautomorphisme $\xi \to \bar{\xi}$), telle que l'on ait

$$f_1(u_0(x), u_0(y)) = h(f_1(x, y))^{\sigma}. \tag{43}$$

Posons $f_2(x, y) = b^{-\sigma} c^{-1} f_1(u_0(x), y)$ et $f(x, y) = f_1(x, y) + \varrho f_2(x, y)$. On vérifie alors aisément que $f(x\varrho, y) = \bar{\varrho} f(x, y)$ et $f(y, x) = \overline{f(x, y)}$, en tenant compte de (43), (32), (33) et (34). On voit donc que f est une forme bilinéaire hermitienne sur l'espace E obtenu en munissant E_0 de la structure d'espace vectoriel à droite par rapport à K (de dimension n) définie ci-dessus.

Soit maintenant τ un second automorphisme de L, que l'on puisse prolonger à K, satisfaisant aux relations (35), (36), (37) et (38) du n° 15. Soit u une application semi-linéaire de E_0 dans lui-même, relative à l'automorphisme τ, telle que $u \cdot u_0 = (u_0 \cdot u)\, a$ et

(44) $$f_1(u(x), u(y)) = e(f_1(x, y))^{\tau}.$$

On a alors $u(x\varrho) = u(u_0(x)) = u_0(u(x))a = u(x)\varrho a = u(x)\varrho^{\tau}$, et par suite u peut être considérée comme une application semi-linéaire de E dans lui-même, relative à τ; on tire en outre de (44) que

$$\begin{aligned} f_2(u(x), u(y)) &= b^{-\sigma}c^{-1}f_1(u_0(u(x)), u(y)) = b^{-\sigma}c^{-1}f_1(u(u_0(x))a^{-1}, u(y)) = \\ &= b^{-\sigma}c^{-1}\bar{a}^{-1}f_1(u(u_0(x)), u(y)) = b^{-\sigma}c^{-1}\bar{a}^{-1}e(f_1(u_0(x), y))^{\tau} = \\ &= b^{-\sigma}c^{-1}\bar{a}^{-1}e\,c^{\tau}b^{\sigma\tau}(f_2(x, y))^{\tau}. \end{aligned}$$

Mais on a $b^{\sigma\tau} = a^{-1}b^{\tau\sigma}a$, $c^{\tau}a^{-1} = c\,a^{\sigma}$, et enfin, en appliquant à (38) l'automorphisme σ, $\bar{a}\,c\,b^{\sigma}e^{\sigma} = e\,c\,a^{\sigma}b^{\tau\sigma}$, d'où finalement $f_2(u(x), u(y)) = e^{\sigma}a(f_2(x, y))^{\tau}$, et par suite, puisque $\varrho^{\tau} = \varrho a$, $f(u(x), u(y)) = e(f(x, y))^{\tau}$.

Soit ψ_0 la corrélation involutive de E_0 sur E_0^* correspondant à la forme f_1 (et relative à l'antiautomorphisme $\xi \to \bar{\xi}$). La formule (43) peut s'exprimer d'une autre manière: on remarque en effet que pour tout $x' \in E_0^*$, $x \to \langle x', u_0(x)\rangle^{\sigma^{-1}}$ est une forme linéaire sur E_0; on définit alors la *transposée* ${}^t u_0$ de u_0 en lui donnant cette forme linéaire pour valeur au point x'; en d'autres termes, on a $\langle x', u_0(x)\rangle = \langle {}^t u_0(x'), x\rangle^{\sigma}$. La relation (43) s'écrit alors

$$\langle \psi_0(u_0(x)), u_0(y)\rangle = h\langle \psi_0(x), y\rangle^{\sigma}$$

ou

$$\langle {}^t u_0(\psi_0(u_0(x))), y\rangle^{\sigma} = h\langle \psi_0(x), y\rangle^{\sigma}$$

ce qui s'écrit, en appliquant σ aux deux membres

(45) $${}^t u_0 \cdot \psi_0 \cdot u_0 = c\,h^{\sigma}c^{-1} \cdot \psi_0$$

ou, en remarquant que u_0 (et par suite ${}^t u_0$) est biunivoque,

(46) $$\psi_0 \cdot u_0 = h \cdot \check{u}_0 \cdot \psi_0.$$

19. Nous pouvons maintenant aborder le problème décrit dans l'Introduction. Soit E_0 un espace vectoriel à droite de dimension finie sur un corps L. Supposons donnés sur L un antiautomorphisme involutif $\xi \to \bar{\xi}$ et m automorphismes σ_i ($0 \le i \le m-1$) dont le carré est un automorphisme intérieur et qui sont deux à deux permutables à un automorphisme intérieur près, et permutables avec $\xi \to \bar{\xi}$ à un automorphisme intérieur près. Supposons donnés une corrélation ψ_0 de E_0 sur E_0^* relative à $\xi \to \bar{\xi}$ et telle que ${}^t\psi_0 = \psi_0$, et m collinéations involutives u_i ($0 \le i \le m-1$) relatives respectivement aux automorphismes σ_i; nous supposons enfin que toutes ces collinéations et la corrélation ψ_0 sont deux à deux «projectivement permutables»

au sens de l'Introduction; il existe donc dans L des constantes c_i, h_i et a_{ij} $(0 \leq i, j \leq m-1)$ telles que l'on ait

$$u_i^2(x) = x\, c_i \tag{47}$$

$$\psi_0 \cdot u_i = h_i \cdot \check{u}_i \cdot \psi_0 \tag{48}$$

$$u_i \cdot u_j = (u_j \cdot u_i) \cdot a_{ij}. \tag{49}$$

Le problème consiste à étudier le *groupe* Γ_0 des *collinéations* u de E_0 qui permutent projectivement avec ψ_0 et toutes les collinéations u_i.

Posons $\sigma_0 = \sigma$, $c_0 = c$, $h_0 = h$, $a_{i0} = a_i$ pour $1 \leq i \leq m-1$. Si, dans la relation $u_0^2(x) = x\,c$ on remplace x par $x\,\xi$ (ξ arbitraire dans L) on voit que l'on a $\xi^{\sigma^2} = c^{-1}\xi\, c$; en outre, comme $u_0^3(x) = u_0(x\,c) = u_0^2(u_0(x)) = u_0(x)\,c$, on a nécessairement $c^\sigma = c$. Soit d'autre part $f_1(x, y)$ la forme hermitienne $\langle\psi_0(x), y\rangle$; on a par hypothèse la relation (43); échangeant x et y dans cette relation, et remarquant que $f_1(x, y)$ peut prendre des valeurs arbitraires dans L, il vient $\overline{\xi^\sigma} = h\,\bar{\xi}^\sigma\,\bar{h}^{-1}$, d'où en particulier $\bar{h} = h$ en faisant $\xi = 1$. Enfin, en remplaçant x et y par $u_0(x)$ et $u_0(y)$ dans (43), il vient

$$\bar{c}\, f_1(x, y)\, c = h\, h^\sigma (f_1(x, y))^{\sigma^2} = h\, h^\sigma c^{-1} f_1(x, y)\, c$$

d'où $\bar{c}\, c = h\, h^\sigma$.

Supposons alors que c *ne soit pas de la forme* $\lambda\,\lambda^\sigma$ (avec $\lambda \in L$); nous nous trouvons dans la situation étudiée aux n^{os} 15 et 18; soit K l'extension quadratique de L définie au n° 18; on peut prolonger à K l'antiautomorphisme $\xi \to \bar{\xi}$ (n° 15), et définir sur E_0 une structure d'espace vectoriel à droite sur K (n° 18), ce qui montre d'ailleurs que nos hypothèses ne sont compatibles que si la dimension de E_0 sur L est paire. Enfin, en désignant par E l'espace vectoriel à droite sur K ainsi défini, on a vu (n° 18) que $f(x, y) = f_1(x, y) + \varrho\, b^{-\sigma} c^{-1} f_1(u_0(x), y)$ est une forme hermitienne sur E pour l'antiautomorphisme $\xi \to \bar{\xi}$ de K.

Cherchons maintenant à prolonger les σ_i $(1 \leq i \leq m-1)$ à K. On voit (comme ci-dessus pour u_0) que l'on a nécessairement $\xi^{\sigma_i^2} = c_i^{-1}\,\xi\, c_i$ pour $\xi \in L$, et $c_i^{\sigma_i} = c_i$; si, dans la relation $u_i(u_0(x)) = u_0(u_i(x))\, a_i$ on remplace x par $x\,\xi$, il vient $\xi^{\sigma\sigma_i} = a_i^{-1}\,\xi^{\sigma_i\sigma}\, a_i$. D'autre part, on a $u_0(u_0(u_i(x))\, a_i) = u_0^2(u_i(x))\, a_i^\sigma = u_i(x)\, c\, a_i^\sigma$, et $u_0(u_0(u_i(x))\, a_i) = u_0(u_i(u_0(x))) = u_i(u_0^2(x))\, a_i^{-1} = u_i(x\,c)\, a_i^{-1} = u_i(x)\, c^{\sigma_i} a_i^{-1}$, d'où par comparaison, $a_i^\sigma\, a_i = c^{-1} c^{\sigma_i}$. Enfin, l'identité $f_1(u_i(x), u_i(y)) = h_i (f_1(x, y))^{\sigma_i}$ donne d'abord, comme ci-dessus $\overline{\xi^{\sigma_i}} = h_i\,\bar{\xi}^{\sigma_i} h_i^{-1}$; puis, en y remplaçant x et y par $u_0(x)$ et $u_0(y)$ on obtient aisément, compte tenu de (49), les relations $h_i\, h^{\sigma_i} a_i^{-1} = \bar{a}_i\, h\, h_i^\sigma$. Or, on a $\bar{a}_i\, \overline{a_i^\sigma} = \overline{c^{\sigma_i}}\, \bar{c}^{-1}$, ce qui, compte tenu de (34), montre qu'on a $\overline{a_i^\sigma}\, b\, h_i = h_i^\sigma\, a_i\, b^{\sigma_i}$. On a donc bien les relations (35), (36), (37) et (38) qui permettent de prolonger σ_i en un automorphisme de K permutable avec $\xi \to \bar{\xi}$. Comme on l'a vu au n° 18, la collinéation u_i devient une collinéation de l'espace E pour l'automorphisme σ_i de K, et le calcul du n° 18 montre que $f(u_i(x), u_i(y)) = h_i(f(x, y))^{\sigma_i}$ dans E. Il est clair d'ailleurs que les relations (47) et (49) continuent d'être satisfaites pour ces collinéations de E.

Le raisonnement qui vient d'être fait pour les u_i peut aussi s'appliquer à une collinéation quelconque u de groupe Γ_0; l'automorphisme de L qui lui correspond se prolonge en un automorphisme de K, la collinéation u dans E_0 devient une collinéation (relative à cet automorphisme de K) dans E, qui permute projectivement à la corrélation involutive ψ de E (correspondant à la forme f) et aux $m-1$ collinéations involutives u_i $(1 \leq i \leq m-1)$. En d'autres termes, on est ramené au problème initial, *mais pour* $m-1$ *collinéations involutives* (dans E) *au lieu de* m (dans E_0).

On remarquera que si u est une transformation *linéaire* de E_0 qui permute *strictement* avec ψ_0 et les u_i $(0 \leq i \leq m-1)$, elle devient une transformation *linéaire* de E qui permute *strictement* avec ψ et les u_i $(1 \leq i \leq m-1)$; ces transformations forment évidemment un *sous-groupe distingué* Γ de Γ_0.

20. Avant de pouvoir déduire de ce qui précède un *procédé de récurrence sur* m pour l'étude du groupe Γ_0 (ou du groupe Γ), il faut d'abord examiner ce qui se passe lorsque (avec les notations du n° 19) l'élément $c \in L$ *est de la forme* $\lambda \lambda^{\sigma}$ (avec $\lambda \in L$). On a donc alors $u_0^2(x) = x \lambda \lambda^{\sigma}$; si on pose $v_0(x) = u_0(x) \lambda^{-1}$, v_0 est une application semi-linéaire de E_0 relative à l'automorphisme $\xi \to \xi^{\tau} = \lambda \xi^{\sigma} \lambda^{-1}$ de L, et on a identiquement $v_0^2(x) = x$, ce qui entraîne que l'automorphisme τ est *involutif*. Le sous-corps M des invariants de τ est alors, soit identique à L si τ est l'identité, soit un sous-corps *galoisien* de L tel que $[L:M] = 2$.

Considérons d'abord le cas où $M = L$, τ étant donc l'identité. En général la relation (43) donne

$$f_1(v_0(x), v_0(y)) = s\,(f_1(x, y))^{\tau} \tag{50}$$

avec $s = \bar{\lambda}^{-1} h \lambda^{-1}$. Dans le cas actuel, on a donc

$$f_1(v_0(x), v_0(y)) = s\, f_1(x, y). \tag{51}$$

Comme $v_0^2(x) = x$, l'espace E_0 est somme directe de deux sous-espaces U, V tels que $v_0(x) = x$ dans U et $v_0(x) = -x$ dans V. D'autre part, on a $s^2 = 1$ d'après (33), d'où $s = 1$ ou $s = -1$. Si tout d'abord $s = 1$, U et V sont orthogonaux pour la forme f_1, et par suite non isotropes. Remarquons qu'on ne modifie pas l'étude du groupe Γ_0 en multipliant les collinéations involutives u_i par des facteurs arbitraires de L; on peut donc en premier lieu remplacer u_0 par v_0. La formule (36) prouve alors que si $u_i \cdot v_0 = (v_0 \cdot u_i)\, a_i$, on a $a_i^2 = 1$; en d'autres termes, on a, soit $u_i(U) = U$ (et alors $u_i(V) = V$), soit $u_i(U) = V$ (et alors $u_i(V) = U$, ce second cas n'étant possible que si U et V ont même dimension, moitié de celle de E_0). D'ailleurs, si on a par exemple $v_0 \cdot u_i = -u_i \cdot v_0$ pour $1 \leq i \leq p$, et $v_0 \cdot u_i = u_i \cdot v_0$ pour les autres indices, en considérant les collinéations involutives $u_1 \cdot u_i$ au lieu de u_i pour $2 \leq i \leq p$, on peut toujours se ramener au cas où $p = 1$; les seuls cas à envisager sont donc $p = 0$ et $p = 1$.

Le même raisonnement, appliqué à une collinéation u du groupe Γ_0 montre qu'on a, soit $u(U) = U$ et $u(V) = V$, soit $u(U) = V$ et $u(V) = U$, et il est clair que les transformations du premier type forment un sous-groupe distingué Γ_1 de Γ_0, égal à Γ_0 ou d'indice 2 dans ce dernier. On peut se limiter à la considération du groupe Γ_1. Si alors $p = 0$, les conditions pour les collinéations $u \in \Gamma_1$ se réduisent aux suivantes: les restrictions de u à U et à V doivent permuter projectivement avec les restrictions respectives de ψ_0 et des $m-1$ collinéations involutives $u_i\,(i \geq 1)$; Γ_1 apparaît donc comme le *produit direct* de deux groupes analogues, mais relatifs aux espaces U et V (au lieu de E_0), *et à $m-1$ collinéations involutives au lieu de m*. Si au contraire $p = 1$, la connaissance de $u \in \Gamma_1$ et des u_i $(i \geq 2)$ dans U les détermine complètement dans E, puisque l'on a par exemple pour u, $u(u_1(x)) = u_1(u(x))\,\mu$ (μ constante convenable) et que u_1 échange U et V (et de même pour les u_i d'indice ≥ 2); pour la même raison, la forme f est connue dans V lorsqu'elle est connue dans U. Le groupe Γ_1 est dans ce cas isomorphe au groupe des restrictions à U des $u \in \Gamma_1$, et ces dernières doivent permuter projectivement aux restrictions de ψ_0 et des u_i $(i \geq 1)$ à U. Le groupe ainsi obtenu est donc encore de même type, mais relatif à l'espace U au lieu de E_0, *et à $m-2$ collinéations involutives au lieu de m*.

Supposons maintenant que $s = -1$. Alors U et V sont totalement isotropes pour la forme f (qui est donc d'indice maximum). Comme f est alors entièrement déterminée par ses valeurs $f(x, y)$ pour $x \in U$ et $y \in V$, on peut identifier V au *dual* U^* de U, en posant, pour $y \in V$ et $\alpha \in L$, $\alpha y = y\bar{\alpha}$ (ce qui définit V comme espace vectoriel à gauche sur L), et $\langle y, x\rangle = f(y, x)$ pour $x \in U$ et $y \in V$. On voit comme ci-dessus que les u_i $(i \geq 1)$ laissent invariants chacun des sous-espaces U et V, ou les échangent, et qu'on peut toujours supposer que le nombre p des collinéations u_i qui appartiennent à la seconde catégorie est 0 ou 1; de même, le sous-groupe distingué Γ_1 de Γ_0 formé des collinéations $u \in \Gamma_0$ laissant invariants U et V est d'indice 1 ou 2 dans Γ_0. Remarquons maintenant que dire qu'une collinéation w laisse invariants U et V et permute projectivement avec ψ_0 signifie (avec l'identification faite ci-dessus) que la restriction de w à V est égale au produit d'un facteur constant par la contragrédiente de la restriction de w à U, cette dernière n'étant plus soumise de ce fait à *aucune* condition. Au contraire, une collinéation qui permute projectivement avec ψ_0 et échange U et V doit être considérée comme une *corrélation* dans U. Cela étant, le groupe Γ_1 est toujours isomorphe au groupe de ses restrictions à U; si $p = 0$, les conditions sur la restriction de $u \in \Gamma_1$ à U se réduisent à ce qu'elle doit permuter projectivement avec les restrictions à U des $m - 1$ collinéations u_i; on a un problème analogue à celui du début, mais où ne figure plus *aucune corrélation*, et seulement $m - 1$ *collinéations involutives au lieu de* m.[1] Si au contraire $p = 1$, la restriction de $u \in \Gamma_1$ à U est soumise à la restriction de permuter projectivement avec la corrélation involutive u_1 et les $m - 2$ collinéations involutives u_i $(i \geq 2)$; c'est le problème du début, mais avec $m - 2$ *collinéations involutives au lieu de* m.[2]

21. Il nous faut maintenant examiner le cas où τ n'est pas l'identité. On notera alors que tout élément $\xi \in L$ peut s'écrire $\xi = \frac{1}{2}(\xi + \xi^\tau) + \frac{1}{2}(\xi - \xi^\tau)$, et comme τ est involutif, cela montre que L est somme directe de M et du sous-espace vectoriel (à droite et à gauche) M_1 sur M formé des éléments ξ tels que $\xi^\tau = -\xi$; si θ est un de ces éléments, on peut écrire $M_1 = \theta M$. Désignons par E_1 l'espace vectoriel *sur* M obtenu en restreignant à M le corps des scalaires de E_0; v_0 est alors une application *linéaire* de E_1 sur lui-même, et E_1 est somme directe des deux sous-espaces U, V tels que $v_0(x) = x$ dans U et $v_0(x) = -x$ dans V; en outre, on a $v_0(x\theta) = v_0(x)\theta^\tau = -v_0(x)\theta$, et par suite l'application $x \to x\theta$ est une application semi-linéaire biunivoque de U sur V, ce qui prouve que U et V ont même dimension et qu'une base de U sur M est aussi une base de E_0 sur L; il en résulte en particulier que la restriction de $f_1(x, y)$ à $U \times U$ est non singulière. Cela étant, supposons d'abord que $s = 1$; la formule (50) prouve que, pour $x \in U$ et $y \in U$, on a $f_1(x, y) = (f_1(x, y))^\tau$, c'est-à-dire que, *dans* U, f_1 *prend ses valeurs dans le corps* M. D'ailleurs, l'hypothèse $s = 1$ entraîne que τ et l'antiautomorphisme $\xi \to \bar{\xi}$ sont *per-*

---

[1] Pour traiter ce problème, il suffit évidemment, dans les raisonnements des nos précédents, de supprimer tout ce qui a trait à la corrélation ψ_0; en particulier, il n'y a pas lieu de faire de distinctions suivant la valeur de s. La récurrence peut donc se poursuivre ici beaucoup plus simplement, car il ne s'introduit jamais de corrélation.

[2] Il peut se faire ici que la corrélation involutive u_1 corresponde à une forme bilinéaire alternée, cas que nous avons écarté au début; pour la façon de traiter ce cas, voir note 1 du n° 22.

mutables, et par suite que $\xi \to \bar{\xi}$ laisse invariant M; pour la restriction à M de cet automorphisme, on voit donc que f_1, restreinte à U, est une *forme hermitienne.*

Soit maintenant u une collinéation du groupe Γ_0, telle que $u \cdot v_0 = v_0 \cdot u \cdot a$; on a $a^\tau a = 1$ (n° 19); l'automorphisme involutif τ laisse donc invariant le corps commutatif $Z(a)$; si sa restriction à $Z(a)$ est l'identité, on a $a^2 = 1$; dans le cas contraire, il existe un élément $c \in Z(a)$ tel que $a = c^\tau c^{-1}$, et en remplaçant u par $u c$, on se ramène au cas où $a = 1$. On peut donc toujours, en multipLant chaque élément de Γ_0 par une constante convenable, supposer que $a = 1$ ou $a = -1$; et dans ce dernier cas, si on multiplie u par θ, on se ramène encore au cas où $a = 1$. On peut donc, à des facteurs scalaires près, se ramener à des collinéations qui permutent strictement avec v_0, et par suite laissent *invariant* U; la méthode s'applique en particulier aux u_i, et on voit finalement que dans ce cas on est ramené encore au problème initial, mais relatif à l'espace U sur le corps M (au lieu de l'espace E_0 sur le corps L), et *à* $m-1$ *collinéations involutives au lieu de* m.

22. Cherchons maintenant à ramener le cas général où $s \neq 1$ au cas où $s = 1$. Supposons d'abord que $s \neq -1$, et posons $r = 1 + s \neq 0$; on a $\bar{s} = s$, d'où $\bar{r} = r$, et comme $s^\tau s = 1$, $r^\tau = 1 + s^{-1} = r s^{-1} = s^{-1} r$. D'autre part (n° 19), on a $\bar{\xi}^\tau = s^{-1} \bar{\xi^\tau} s$; si on pose $\xi^\varpi = r^{-1} \bar{\xi^\tau} r$, on vérifie que ϖ est un antiautomorphisme involutif de L, permutable avec τ; si alors on remplace f_1 par la forme $g_1(x, y) = r^{-1} f_1(x, y)$, on a identiquement $g_1(v_0(x), v_0(y)) = (g_1(x, y))^\tau$, donc, *dans* U, la forme g_1 prend ses valeurs dans le corps M; en outre, *dans* U, on a $g_1(y, x) = r^{-1} \overline{g_1(x, y)}\, r$ et comme $(g_1(x, y))^\tau = g_1(x, y)$, on voit que $g_1(y, x) = (g_1(x, y))^\varpi$. L'antiautomorphisme involutif ϖ laissant invariant le corps M, on est ramené au cas traité au n° 21.

Supposons ensuite que $s = -1$, ce qui entraîne que τ est permutable avec $\xi \to \bar{\xi}$, donc laisse M invariant. Prenons $r = \bar{\theta} \bar{\beta} + \theta \beta$, où $\theta^\tau = -\theta$ et $\beta \in M$; on aura encore $\bar{r} = r$ et $r^\tau = -r$; la méthode précédente s'applique donc pourvu que $r \neq 0$. Or, on ne peut avoir $r = 0$ pour tout $\beta \in M$ que si $\bar{\theta} = -\theta$ et $\bar{\beta} = \theta \beta \theta^{-1}$ identiquement dans M; cela entraîne en premier lieu que M est *commutatif.* En outre, si on pose $g_1(x, y) = f_1(x, y)\, \theta$, on a $g_1(v_0(x), v_0(y)) = (g_1(x, y))^\tau$, et par suite g_1 prend ses valeurs dans M pour $x \in U$ et $y \in U$; d'autre part on a $g_1(y, x) = $ $= f_1(y, x)\, \theta = \overline{f_1(x, y)}\, \theta = -\theta^{-1} \overline{g_1(x, y)}\, \theta = -g_1(x, y)$ dans U, ce qui signifie que dans U, g_1 est une forme bilinéaire *alternée*; quant aux collinéations u_i $(1 \leq i \leq m-1)$ et aux éléments u de Γ_0, on peut encore, en les multipliant par des constantes convenables, supposer qu'elles laissent invariant U, comme au n° 21. On est donc encore ramené au même type de problème pour $m-1$ collinéations involutives au lieu de m, mais pour une corrélation involutive qui correspond à une *forme alternée*, cas que nous avions jusqu'ici laissé de coté (cf. n° 16), mais qu'il est aisé de traiter suivant les mêmes méthodes.[1]

En résumé, le procédé décrit dans cette partie fournit une *méthode de récurrence*, qui, dans *tous* les cas, permet de ramener l'étude du groupe Γ_0 (ou tout au moins d'un sous-groupe distingué d'indice fini de Γ_0) au cas particulier où Γ_0 est défini comme le groupe des collinéations permutant avec *une seule collinéation involutive* ou *une seule corrélation involutive;* mais le corps initial L aura été remplacé par un autre corps (qui, même si L était commutatif, ne le sera plus nécessairement), obtenu à partir de L par une suite d'extensions quadratiques ou au contraire de restrictions à des sous-corps par rapport auquel le corps considéré est une extension quadratique.

III. Les groupes orthogonaux à 3, 4, 5 et 6 variables.

23. Soit K un corps commutatif de caractéristique $\neq 2$, E un espace vectoriel de dimension n sur K, f une forme quadratique non dégénérée définie sur E, et

---

[1] Partons des relations (47), (48) et (49), le corps L étant supposé commutatif, l'antiautomorphisme $\xi \to \bar{\xi}$ réduit à l'identité, et la forme $f_2(x, y) = \langle \psi_0(x), y \rangle$ *alternée.* Supposons d'abord que σ ne soit pas l'identité. On voit comme au n° 19 qu'on a $c^2 = h h^\sigma$, ce qui s'écrit encore $(-h c^{-1})(-h c^{-1})^\sigma = 1$; il existe donc $d \in L$ tel que $-h c^{-1} = d^{\sigma - 1}$. La relation

$$f_2(u_0(x), u_0(y)) = h(f_2(x, y))^\sigma$$

s'écrit donc aussi

$$d f_2(u_0(x), u_0(y)) = -c(d f_2(x, y))^\sigma$$

et en remplaçant f_2 par $d f_2$, on peut donc supposer que $h = -c$. *Si c n'est pas de la forme $\lambda \lambda^\sigma$,* on forme l'extension quadratique K de L comme au n° 18, et on prolonge l'application σ en un antiautomorphisme $\xi \to \bar{\xi}$ de K en posant $\overline{x + \varrho y} = x^\sigma - \varrho y$. On vérifie alors aussitôt que $f(x, y) = f_2(u_0(x), y) + \varrho f_2(x, y)$ est une forme hermitienne sur E (considéré comme espace vectoriel à droite sur K). On constate ensuite qu'on a $\sigma_i \sigma = \sigma \sigma_i$, et qu'on peut prolonger σ_i en un automorphisme de K (noté de la même façon) en vertu de la relation $a_i^\sigma a_i = c^{-1} c^{\sigma_i}$; on pose encore $\varrho^{\sigma_i} = \varrho a_i$; on constate alors que dans K, σ_i et l'antiautomorphisme $\xi \to \bar{\xi}$ sont permutables. En outre, on vérifie que l'on a $f(u_i(x), u_i(y)) = a_i^{-1} h_i (f(x, y))^{\sigma_i}$, et on a une relation analogue pour toute collinéation permutable projectivement avec ψ_0 et les u_i.

Si au contraire $c = \lambda \lambda^\sigma$, on a alors, en posant $u_0 = v_0 \lambda$, $v_0^2(x) = x$ et $\lambda f_2(v_0(x), v_0(x)) = -(\lambda f_2(x, y))^\sigma$; remplaçant f_2 par λf_2, on peut toujours supposer que $\lambda = 1$. Comme σ^2 est l'identité, et que L n'est pas de caractéristique 2, il existe dans L un élément r tel que $r^\sigma = -r$; en multipliant f_2 par r, on peut donc se ramener au cas où on a $f_2(v_0(x), v_0(y)) = (f_2(x, y))^\sigma$. Cela fait, la méthode du n° 21 s'applique, à cela près que la restriction de f_2 au sous-espace U est encore une forme alternée au lieu d'une forme hermitienne.

On procède de façon analogue si σ est l'identité. On a alors $h = c$ ou $h = -c$; considérons d'abord le cas où c *n'est pas un carré.* Si $h = -c$, il n'y a rien à changer à la méthode suivie plus haut; K est alors une extension quadratique commutative de L. Si $h = c$, on procède de même, mais cette fois $f(x, y)$ est encore une *forme alternée* sur E (considéré comme espace vectoriel sur K). Enfin, si c est un carré, la méthode du n° 20 est applicable.

d'indice ν ([8], p. 17). Soit $GO_n(K,f)$ le groupe des transformations linéaires inversibles u de E sur lui-même, telles que $f(u(x), u(y)) = \lambda_u \cdot f(x,y)$, où $\lambda_u \in K$ (*multiplicateur* de u); en prenant les discriminants des formes bilinéaires des deux membres, il vient $(\det u)^2 = \lambda_u^n$; si n est *impair*, λ_u est donc un *carré*, et on peut donc écrire $u = \mu v$, où v est une transformation orthogonale; en d'autres termes, $GO_n(K,f)$ est alors *produit direct* du groupe orthogonal $O_n(K,f)$ et du groupe des homothéties (isomorphe au groupe multiplicatif K^* des éléments $\neq 0$ de K). Au contraire, si $n = 2m$ est pair, on a $\det u = \pm \lambda_u^m$; les transformations de $GO_n(K,f)$ pour lesquelles $\det u = \lambda_u^m$ sont appelées *similitudes directes;* elles forment un sous-groupe distingué $GO_n^+(K,f)$ d'indice 2 du groupe $GO_n(K,f)$, qui contient le groupe des homothéties et le groupe des rotations $O_n^+(K,f)$, mais n'est pas en général produit direct de ces deux groupes.

De même, si g est une forme hermitienne non dégénérée sur E (relative à un automorphisme $\xi \to \bar{\xi}$ de K), on désigne par $GU_n(K,g)$ le groupe des transformations linéaires inversibles u de E sur lui-même telles que $g(u(x), u(y)) = \lambda_u \cdot g(x,y)$; ici le multiplicateur λ_u doit nécessairement appartenir au corps des invariants L de l'automorphisme $\xi \to \bar{\xi}$. En posant $\Delta = \det u$, il vient ici $\Delta\bar{\Delta} = \lambda_u^n$; si n est *impair*, λ_u est une *norme* d'un élément de K, d'où résulte aussitôt que $GU_n(K,f)$ est produit direct du groupe des homothéties et du groupe unitaire $U_n(K,f)$. Si $n = 2m$ est pair, on appelle encore *similitudes directes* les transformations de $GU_n(K,f)$ pour lesquelles $\det u = \lambda_u^m$; elles forment un sous-groupe distingué $GU_n^+(K,f)$ de $GU_n(K,f)$, le groupe quotient étant isomorphe au groupe N des éléments de norme 1 dans K.

On définit de même $GU_n(K,f)$ lorsque K est un corps non commutatif et $\xi \to \bar{\xi}$ un antiautomorphisme de K; on impose alors à λ_u la condition d'appartenir au *centre* de K.

24. Nous nous proposons dans cette partie d'étudier la structure des groupes $GO_n^+(K,f)$ pour $n = 4$ et $n = 6$ et les groupes $O_n^+(K,f)$ pour $n = 3$ et $n = 5$, en suivant la méthode développée par B. L. van der Waerden [14], mais en complétant ses résultats dans les cas qu'il n'a pas examinés; ceci sera possible principalement grâce au procédé décrit ci-dessus dans la II^e partie.

Cas I a: $n = 4$, $\nu = 2$. On peut supposer la forme f rapportée à une base telle que $f(x,x) = \xi_1\xi_4 - \xi_2\xi_3$. Si alors on identifie tout point $x = (\xi_1, \xi_2, \xi_3, \xi_4)$ de E à la matrice $X = \begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix}$, toute similitude directe u peut s'écrire sous la forme

$$X \to U_1 X U_2 \tag{52}$$

U_1 et U_2 étant deux matrices inversibles d'ordre 2; elles ne sont pas entièrement déterminées par u, car on peut multiplier U_1 par un facteur arbitraire μ et U_2 par μ^{-1}; enfin le multiplicateur de u est det $(U_1 U_2)$ ([14], p. 20–21). *Le groupe* $G O_4^+(K, f)$ *est donc isomorphe au quotient du groupe produit* $G L_2(K) \times G L_2(K)$ *par le sous-groupe formé des couples de matrices* $(\mu I, \mu^{-1} I)$ (I *matrice unité*).

Cas I b: $n = 4$, $\nu = 1$. On peut supposer f rapportée à une base de E telle que $f(x, x) = \xi_1 \xi_4 - (a_2 \xi_2^2 + a_3 \xi_3^2)$, l'élément $-a_3/a_2$ n'étant pas un carré dans K [15]; cela signifie que le *discriminant* $d = -a_2 a_3$ *de* f *n'est pas un carré.* Soit $K_1 = K(\sqrt{d})$ l'extension quadratique de K obtenue par adjonction d'une racine ω du polynôme $a_2 X^2 + a_3$, et soit E_1 l'espace vectoriel obtenu par extension à K_1 du corps des scalaires de E. La forme f est la restriction à E de la forme f_1 d'indice 2 sur E_1, telle que $f_1(x, x) = \xi_1 \xi_4 - a_2(\xi_2 + \omega \xi_3)(\xi_2 - \omega \xi_3)$, et les transformations de $G O_4^+(K, f)$ sont les restrictions à E des transformations de $G O_4^+(K_1, f_1)$ permutables avec la transformation semi-linéaire involutive $(\xi_k) \to (\xi_k^\sigma)$ de E_1, où σ est l'unique K-automorphisme de K_1 distinct de l'identité. En faisant dans E_1 le changement de coordonnées

$$\eta_1 = \xi_1, \; \eta_4 = \xi_4, \; \eta_2 = a_2(\xi_2 + \omega \xi_3), \; \eta_3 = \xi_2 - \omega \xi_3$$

la forme f_1 est ramenée à l'écriture du cas I a, et la transformation semi-linéaire de E_1 s'écrit

$$(\eta_1, \eta_2, \eta_3, \eta_4) \to (\eta_1^\sigma, a_2 \eta_3^\sigma, a_2^{-1} \eta_2^\sigma, \eta_4^\sigma).$$

En écrivant que (52) permute avec cette transformation, il vient aisément $U_2 = \mu P \cdot {}^t U_1^\sigma \cdot P^{-1}$, où μ est une constante arbitraire dans K, $P = \begin{pmatrix} 1 & 0 \\ 0 & a_2^{-1} \end{pmatrix}$, ${}^t V$ désignant la transposée d'une matrice V; U_1 n'est pas complètement déterminée par u, car on peut encore la multiplier par un élément de K_1 de *norme* 1 sans changer u; enfin, le multiplicateur de u est ici $\mu^2 \Delta \Delta^\sigma$, où $\Delta = \det(U_1)$ ([14], p. 25–26). *Le groupe* $G O_4^+(K, f)$ *est donc isomorphe au produit de* K^* *par le groupe quotient* $G L_2(K_1)/N$, *où* N *est le groupe des éléments de* K_1 *de norme* 1 (identifié au groupe des homothéties correspondantes).

25. Dans le cas où $n = 4$ et $\nu = 0$, supposons la forme f rapportée à une base telle que $f(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_3 \xi_3^2$, les éléments $-a_4/a_1$ et $-a_3/a_2$ n'étant pas des carrés dans K. Soit K_1 l'extension quadratique de K obtenue par adjonction d'une racine ω de $a_1 X^2 + a_4$; $-a_3/a_2$ peut ou non être un carré dans K_1; dans le premier cas, on a nécessairement $-a_3/a_2 = \lambda^2 \omega^2 = -\lambda^2 a_4/a_1$, avec $\lambda \in K$,

donc $d = a_1 a_2 a_3 a_4$ est un *carré* dans K, et réciproquement. Nous sommes donc amenés à distinguer deux cas.

Cas I c: $n = 4$, $\nu = 0$, le discriminant de f est un carré. On peut évidemment supposer alors que $a_1 a_3 = a_2 a_4$, et par suite, f est la restriction à E de la forme définie sur E_1

$$f_1(x, x) = a_1(\xi_1 + \omega \xi_4)(\xi_1 - \omega \xi_4) - a_2(\xi_2 + \omega \xi_3)(\xi_2 - \omega \xi_3).$$

$G O_4^+(K, f)$ est le groupe des restrictions à E des transformations de $G O_4^+(K_1, f_1)$ permutables à $(\xi_k) \to (\xi_k^\sigma)$. Ici, on fait le changement de coordonnées

$$\eta_1 = a_1(\xi_1 + \omega \xi_4), \quad \eta_4 = \xi_1 - \omega \xi_4, \quad \eta_2 = a_2(\xi_2 + \omega \xi_3), \quad \eta_3 = \xi_2 - \omega \xi_3$$

de façon que la forme soit ramenée à l'écriture du cas I a; la transformation semilinéaire de E_1 s'écrit alors

$$(\eta_1, \eta_2, \eta_3, \eta_4) \to (a_1 \eta_4^\sigma, a_2 \eta_3^\sigma, a_2^{-1} \eta_2^\sigma, a_1^{-1} \eta_1^\sigma).$$

En écrivant que (52) permute avec cette transformation, on trouve cette fois qu'en posant $Q = \begin{pmatrix} 1 & 0 \\ 0 & a_1 \end{pmatrix}$, les transformations (52) qui appartiennent au groupe $G O_4^+(K, f)$ sont de la forme

$$X \to M V_1 X (Q V_2 Q^{-1}) M^{-1}$$

où $M = \begin{pmatrix} 1 & 0 \\ 0 & \mu \end{pmatrix}$, avec $\mu \in K_1$ de norme 1 (c'est-à-dire tel que $\mu \mu^\sigma = 1$), V_1 et V_2 étant deux matrices arbitraires de la forme $\begin{pmatrix} \alpha & a_1 a_2 \beta \\ \beta^\sigma & \alpha^\sigma \end{pmatrix}$. Or, on constate aisément que ces matrices ne sont autres que les matrices du groupe des *similitudes hermitiennes directes* $G U_2^+(K_1, g)$ où g est la forme hermitienne définie dans $F = K_1^2$ par la relation $g(z, z) = \zeta_1 \zeta_1^\sigma - a_1 a_2 \zeta_2 \zeta_2^\sigma$. Mais d'autre part, les matrices du groupe $G U_2^+(K_1, g)$ sont aussi les matrices qui permutent avec la collinéation involutive u_0 (relative à σ) de F, définie par

$$(\zeta_1, \zeta_2) \to (a_1 a_2 \zeta_2^\sigma, \zeta_1^\sigma).$$

On a d'ailleurs de façon précise $u_0^2(z) = a_1 a_2 z$, et

$$g(u_0(z), u_0(t)) = -a_1 a_2 (g(z, t))^\sigma.$$

D'autre part, $a_1 a_2$ n'est pas de la forme $\lambda \lambda^\sigma$, car cela entraînerait que $a_2/a_1 = (a_1 a_2)/a_1^2$ serait de la même forme, c'est-à-dire une norme d'un élément de K_1, et par suite on pourrait avoir $f(x, x) = 0$ pour un vecteur $x \neq 0$ de E, contrairement à l'hypothèse $\nu = 0$. On peut donc appliquer aux éléments de $G\,U_2^+(K_1, g)$ la méthode du n° 18; ici K_1 est commutatif, et l'antiautomorphisme $\zeta \to \bar{\zeta}$ est identique à l'automorphisme σ; on formera donc l'extension quadratique K_2 de K_1, ayant pour base 1 et ϱ, avec $\varrho^2 = a_1 a_2$, $\zeta^\sigma = \varrho^{-1}\zeta\varrho$ pour $\zeta \in K_1$, et $\bar{\varrho} = -\varrho$; les éléments de K_2 peuvent donc s'écrire $\boldsymbol{z} = a_1(\xi_1 + \omega\xi_4) + \varrho(\xi_2 + \omega\xi_3)$, avec $\omega^2 = -a_4/a_1$, $\varrho^2 = a_1 a_2$, $\varrho\omega = -\omega\varrho$, ce qui signifie que K_2 n'est autre que le *corps des quaternions* (généralisés) sur K, correspondant au couple $(-a_4/a_1, a_1 a_2)$ d'éléments de K. D'après la méthode du n° 18, les éléments de $G\,U_2^+(K_1, g)$ sont identifiés avec les transformations linéaires de K_2 (considéré comme espace vectoriel à droite sur lui-même) qui permutent avec la corrélation involutive correspondant à la forme g; mais toute transformation linéaire de K_2 est de la forme $\boldsymbol{z} \to \boldsymbol{q}\boldsymbol{z}$, où $\boldsymbol{q}$ est un quaternion fixe, et on a $g(\boldsymbol{z}, \boldsymbol{t}) = \bar{\boldsymbol{z}}\boldsymbol{t}$ (avec $\bar{\boldsymbol{z}} = a_1(\xi_1 - \omega\xi_4) - \varrho(\xi_2 + \omega\xi_3)$); comme $g(\boldsymbol{q}\boldsymbol{z}, \boldsymbol{q}\boldsymbol{t}) = \bar{\boldsymbol{q}}\boldsymbol{q}\,g(\boldsymbol{z}, \boldsymbol{t})$ (puisque $\bar{\boldsymbol{q}}\boldsymbol{q}$ appartient au centre K de K_2), la condition de permutabilité est vérifiée ipso facto, et par suite les transformations de $G\,U_2^+(K_1, g)$ sont simplement identifiées aux homothéties à gauche $\boldsymbol{z} \to \boldsymbol{q}\boldsymbol{z}$ du corps K_2. Finalement, si le point $(\xi_1, \xi_2, \xi_3, \xi_4)$ de E est identifié au quaternion $\boldsymbol{z} = a_1(\xi_1 + \omega\xi_4) + \varrho(\xi_2 + \omega\xi_3)$, on vérifie aisément que l'on a $g(\boldsymbol{z}, \boldsymbol{z}) = a_1 f(x, x)$, et que les transformations $X \to V_1 X Q V_2 Q^{-1}$ (avec les notations précédentes) s'identifient aux transformations $\boldsymbol{z} \to \boldsymbol{q}_1\boldsymbol{z}\boldsymbol{q}_2$, où $\boldsymbol{q}_1$ et $\boldsymbol{q}_2$ sont des quaternions arbitraires; d'ailleurs, une telle transformation ne détermine $\boldsymbol{q}_1$ qu'à un facteur scalaire $\beta \in K^*$ près, $\boldsymbol{q}_2$ devant alors être multiplié par β^{-1}. D'autre part, pour tout élément $\mu \in K_1$ tel que $\mu\mu^\sigma = 1$, il existe $\lambda \in K_1$ tel que $\mu = \lambda^\sigma\lambda^{-1}$; on en déduit aisément que l'application $X \to M X M^{-1}$ s'identifie à $\boldsymbol{z} \to \lambda\boldsymbol{z}\lambda^{-1}$; donc toutes les transformations de $G\,O_4^+(K, f)$ sont ainsi identifiées aux transformations $\boldsymbol{z} \to \boldsymbol{q}_1\boldsymbol{z}\boldsymbol{q}_2$. le multiplicateur correspondant étant le produit $N(\boldsymbol{q}_1)N(\boldsymbol{q}_2)$ des *normes* de $\boldsymbol{q}_1$ et $\boldsymbol{q}_2$; on voit que *$G\,O_4^+(K, f)$ est isomorphe au quotient du groupe produit $K_2^* \times K_2^*$ par le sous-groupe des éléments (β, β^{-1}), où β parcourt K^** (K centre de K_2) ([14], p. 26–27).

26. *Cas I d: $n = 4$, $\nu = 0$, le discriminant de f n'est pas un carré* (ce cas, non traité dans [14], ne peut évidemment se présenter lorsque K est le corps des nombres réels). Avec les mêmes notations que dans le n° 25, $-a_3/a_2$ n'est pas alors un carré dans K_1; soit K_2 le corps obtenu par adjonction à K d'une racine ω' de $a_2 X^2 + a_3$; K_1 et K_2 sont linéairement disjoints sur K, et leur corps composé K_3 est une extension galoisienne de degré 4 sur K. La forme f est la restriction à E de la forme définie sur l'espace E_3 (obtenu par extension à K_3 du corps des scalaires de E) par la condition

$$f_1(x, x) = a_1(\xi_1 + \omega\xi_4)(\xi_1 - \omega\xi_4) - a_2(\xi_2 + \omega'\xi_3)(\xi_2 - \omega'\xi_3).$$

Si on désigne par σ et τ les automorphismes de K_3 définis par $\omega^\sigma = -\omega$, $\omega'^\sigma = \omega'$, et $\omega^\tau = \omega$, $\omega'^\tau = -\omega'$, $G O_4^+(K, f)$ est le sous-groupe de $G O_4^+(K_3, f_1)$ formé des transformations permutables aux deux transformations semi-linéaires $(\xi_k) \to (\xi_k^\sigma)$ et $(\xi_k) \to (\xi_k^\tau)$. On fait ici le changement de coordonnées

$$\eta_1 = a_1(\xi_1 + \omega\,\xi_4), \quad \eta_4 = \xi_1 - \omega\,\xi_4, \quad \eta_2 = a_2(\xi_2 + \omega'\,\xi_3), \quad \eta_3 = \xi_2 - \omega'\,\xi_3$$

pour ramener la forme f_1 à l'écriture du cas I a; les deux transformations semi-linéaires de E_3 s'écrivent alors

$$(\eta_1, \eta_2, \eta_3, \eta_4) \to (a_1\,\eta_4^\sigma, \eta_2^\sigma, \eta_3^\sigma, a_1^{-1}\,\eta_1^\sigma)$$
$$(\eta_1, \eta_2, \eta_3, \eta_4) \to (\eta_1^\tau, a_2\,\eta_3^\tau, a_2^{-1}\,\eta_2^\tau, \eta_4^\tau).$$

En écrivant que (52) permute avec ces deux transformations, on obtient les conditions suivantes: si on désigne par ϖ l'automorphisme $\sigma\tau$ du corps K_3, U_1 est de la forme λV_1 où $\lambda \in K$ et V_1 est une matrice arbitraire du groupe $G U_2^+(K_3, g)$, g étant la forme hermitienne définie sur $F = K_3^2$ par $g(z, z) = \zeta_1 \zeta_1^\varpi - a_1 a_2 \zeta_2 \zeta_2^\varpi$; enfin, $U_2 = P \cdot {}^t V_1^\tau \cdot P^{-1}$. La matrice U_1 n'est d'ailleurs déterminée qu'à un facteur près $\alpha \in K_3$ tel que αV_1 appartienne encore à $G U_2^+(K_3, g)$ et que $\alpha \alpha^\tau = 1$, et la première de ces deux conditions signifie que $\alpha = \alpha^\varpi$. Si K_0 est le sous-corps de K_3 formé des invariants de ϖ, on a $K_0 = K(\omega\omega') = K(\sqrt{d})$, d désignant le discriminant de la forme f; les automorphismes σ et τ coincident sur K_0 avec l'unique K-automorphisme de ce corps distinct de l'identité; on peut donc dire que le facteur α par lequel on peut multiplier U_1 sans changer la transformation, doit être un élément de norme 1 dans le corps K_0. *Le groupe $G O_4^+(K, f)$ est finalement isomorphe au produit du groupe K^* par le quotient $G U_2^+(K_3, g)/N_0$, où $N_0 \subset K_0^*$ est le groupe des éléments de K_0 de norme* 1 (*par rapport à* K). D'ailleurs, si on avait $a_1 a_2 = \xi \xi^\varpi$, f ne serait pas d'indice 0; on peut donc appliquer au groupe $G U_2^+(K_3, g)$ la méthode du n° 18, l'automorphisme et l'antiautomorphisme qui interviennent au n° 18 étant tous deux égaux à ϖ. On forme donc l'extension quadratique L de K_3, ayant pour base 1 et ϱ, avec $\varrho^2 = a_1 a_2$, $\zeta^\varpi = \varrho^{-1} \zeta \varrho$ pour $\zeta \in K_3$, et $\bar{\varrho} = -\varrho$; les éléments de L peuvent ici s'écrire $\boldsymbol{z} = a_1(\xi_1' + \omega\,\xi_4') + \varrho(\xi_2' + \omega\,\xi_3')$, les ξ_i' étant *dans* K_0, avec $\omega^2 = -a_4/a_1$, $\varrho^2 = a_1 a_2$, $\omega\varrho = -\varrho\omega$; ce qui montre que L est encore un *corps de quaternions* (généralisés) *sur l'extension quadratique* $K_0 = K(\sqrt{d})$ de K, correspondant au couple $(-a_4/a_1, a_1 a_2)$. Les transformations de $G U_2^+(K_3, g)$ sont alors identifiées aux homothéties à gauche $\boldsymbol{z} \to \boldsymbol{q}\boldsymbol{z}$ de L; le déterminant Δ de la matrice V_1 correspondant à $\boldsymbol{q}$ est alors $N(\boldsymbol{q})$, norme du quaternion $\boldsymbol{q}$ (qui est par suite un élément de K_0); le multiplicateur de la transformation correspondante de $GO_4^+(K, f)$ est alors $\lambda^2 \Delta\Delta^\tau$, et $\Delta\Delta^\tau$ n'est autre que la *norme* (dans K) de $N(\boldsymbol{q})$.

27. *Cas II a:* $n = 3$, $\nu = 1$. Comme on peut évidemment multiplier la forme quadratique f par un facteur constant de K sans changer le groupe $O_3^+(K, f)$, on peut supposer la forme f rapportée à une base de E telle que $f(x, x) = \xi_1^2 - \xi_2\xi_3$. Suivant la méthode de van der Waerden ([14], p. 27), on considère E comme le sous-espace $\xi_4 = 0$ d'un espace F de dimension 4 sur K, f étant la restriction à E de la forme g telle que $g(x, x) = \xi_1^2 - \xi_4^2 - \xi_2\xi_3$: le groupe $O_3^+(K, f)$ est par suite le sous-groupe de $O_4^+(K, g)$ formé des rotations laissant invariant ξ_4. On ramène la forme g à l'écriture du cas I a, par le changement de variables

$$\eta_1 = \xi_1 + \xi_4, \quad \eta_4 = \xi_1 - \xi_4, \quad \eta_2 = \xi_2, \quad \eta_3 = \xi_3$$

et $O_3^+(K, f)$ peut être identifié aux transformations (52) qui laissent invariant $\eta_1 - \eta_4$ et appartiennent à $O_4^+(K, g)$; on trouve la condition $U_2 = (\det U_1)^{-1} R \cdot {}^tU_1 \cdot R^{-1}$, avec $R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. D'ailleurs, si on multiplie U_1 par λ, U_2 est multiplié par λ^{-1}, donc la transformation (52) n'est pas modifiée. On en conclut que *$O_3^+(K, f)$ est isomorphe au groupe projectif $PGL_2(K) = GL_2(K)/K^*$* ([14], p. 27–28).

Cas II b: $n = 3$, $\nu = 0$. On peut ici multiplier la forme f par un facteur constant de sorte qu'elle s'écrive $f(x, x) = a_2 a_3 \xi_4^2 - (a_2\xi_2^2 + a_3\xi_3^2)$ par rapport à une base convenable de E, l'élément $-a_3/a_2$ n'étant pas un carré dans K. Considérons E comme le sous-espace $\xi_1 = 0$ d'un espace F de dimension 4 sur K, f étant la restriction à E de la forme g telle que $g(x, x) = \xi_1^2 + a_2 a_3 \xi_4^2 - (a_2\xi_2^2 + a_3\xi_3^2)$. Montrons que la forme g est *d'indice* 0 dans F; en effet, la relation $g(x, x) = 0$ est par hypothèse impossible si $\xi_1 = \xi_4 = 0$; si ξ_1 et ξ_4 ne sont pas nuls tous deux, $g(x, x) = 0$ s'écrit

$$a_2 = (\xi_2^2 + a_3 a_2^{-1} \xi_3^2) / ((a_2^{-1}\xi_1)^2 + a_3 a_2^{-1} \xi_4^2)$$

ce qui signifie que a_2 serait la *norme* (sur K) d'un élément $\lambda + \omega\mu$ du surcorps obtenu en adjoignant à K une racine ω du polynôme $a_2 X^2 + a_3$; mais alors la relation $a_2 = \lambda^2 + a_3 a_2^{-1} \mu^2$ entraîne que f n'est pas d'indice 0, car on aurait $f(x, x) = 0$ pour $\xi_2 = a_2^{-1}\mu$, $\xi_3 = a_3^{-1}\lambda$ et $\xi_4 = a_3^{-1}$.

Cela étant, la forme g a un discriminant *carré*. L'étude du cas I c (n° 25) montre que si on fait correspondre au point $(\xi_1, \xi_2, \xi_3, \xi_4)$ le *quaternion* $\boldsymbol{z} = \xi_1 + \omega\xi_4 + \varrho(\xi_2 + \omega\xi_3)$, relatif au couple $(-a_2 a_3, a_2)$, toute rotation du groupe $O_4^+(K, g)$ peut s'écrire $\boldsymbol{z} \to \boldsymbol{q}_1 \boldsymbol{z} \boldsymbol{q}_2$, où $\boldsymbol{q}_1$ et $\boldsymbol{q}_2$ sont des quaternions tels que $N(\boldsymbol{q}_1 \boldsymbol{q}_2) = 1$. Pour qu'une telle rotation appartienne à $O_3^+(K, f)$, il faut et il suffit qu'elle laisse invariant ξ_1, ce qui donne la condition $\boldsymbol{q}_1 \boldsymbol{q}_2 = 1$; toute rotation du groupe $O_3^+(K, f)$ peut donc s'écrire $\boldsymbol{z} \to \boldsymbol{q}\,\boldsymbol{z}\,\boldsymbol{q}^{-1}$, $\boldsymbol{q}$ étant un quaternion arbitraire $\neq 0$ dans le corps K_2 des quaternions sur K relatifs au couple $(-a_2 a_3, a_2)$, et l'espace E étant identifié à l'ensemble des quaternions de partie scalaire nulle. D'ailleurs le quaternion $\boldsymbol{q}$ n'est déterminé qu'à un facteur près de K^*, ce qui montre que *$O_3^+(K, f)$ est isomorphe à K_2^*/K^*.*

28. *Cas III a:* $n = 6$, $\nu = 3$. On peut supposer la forme f rapportée à une base telle que $f(x, x) = \xi_1 \xi_4 - \xi_2 \xi_5 + \xi_3 \xi_6$. Désignons par F l'espace K^4, par $(e_i)_{1 \leq i \leq 4}$ la base canonique de F; on peut alors identifier E à l'espace $F^{(2)}$ des *bivecteurs* sur F, le point (ξ_k) étant identifié au bivecteur

$$x = \xi_1 e_1 \wedge e_2 + \xi_2 e_1 \wedge e_3 + \xi_3 e_1 \wedge e_4 + \xi_4 e_3 \wedge e_4 + \xi_5 e_2 \wedge e_4 + \xi_6 e_2 \wedge e_3$$

de sorte qu'on a alors $x \wedge y = f(x, y)\, e_1 \wedge e_2 \wedge e_3 \wedge e_4$ pour le produit extérieur de deux bivecteurs x, y. Pour toute application semi-linéaire v de F sur lui-même on désigne par $v^{(2)}$ la puissance extérieure seconde de v, c'est-à-dire l'application semi-linéaire de $F^{(2)} = E$ sur lui-même définie en posant, pour deux vecteurs quelconques z_1, z_2 de F, $v^{(2)}(z_1 \wedge z_2) = v(z_1) \wedge v(z_2)$; si on pose $u = v^{(2)}$, on a donc, pour deux bivecteurs quelconques x, y, $u(x \wedge y) = (f(x, y))^\sigma v(e_1) \wedge v(e_2) \wedge v(e_3) \wedge v(e_4)$ (σ désignant l'automorphisme de K auquel correspond v), ou encore, par définition du déterminant,

$$f(u(x), u(y)) = (\det v)\,(f(x, y))^\sigma.$$

En particulier, si v est une application linéaire de F sur lui-même, $u = v^{(2)}$ est une *similitude directe* pour la forme f, le déterminant de u étant $(\det v)^3$. Inversement, on montre que si u est une similitude directe pour f, il existe une application semi-linéaire v de F sur lui-même telle que $v^{(2)} u^{-1}$ transforme toute droite de E passant par l'origine en elle-même ([14], p. 21–22, et [6], p. 36–38); ceci n'est possible que si cette transformation est une homothétie, ce qui entraîne que v est linéaire, et $u = \mu \cdot v^{(2)}$, où $\mu \in K^*$. En outre, si on a $\mu \cdot v^{(2)} = \mu_1 \cdot v_1^{(2)}$ pour deux scalaires μ, μ_1 et deux applications linéaires v, v_1 de F sur lui-même, $(v v_1^{-1})^{(2)}$ est une homothétie dans E, donc $v v_1^{-1}$ laisse invariant dans F tout plan passant par l'origine (puisque le bivecteur décomposable correspondant à ce plan est multiplié par un scalaire); cela n'est possible que si $v v_1^{-1}$ laisse invariante toute droite passant par l'origine, c'est-à-dire est une *homothétie*; autrement dit, on doit avoir $v_1 = \lambda v$ avec $\lambda \in K^*$, ce qui entraîne $\mu_1 = \mu \lambda^{-2}$. On en conclut aussitôt que *le groupe $G O_6^+(K, f)$ est alors isomorphe au quotient du groupe $K^* \times G L_4(K)$ par le sous-groupe formé des couples de* *la forme* $(\lambda^2, \lambda^{-1})$, *où* λ *parcourt* K^*. Enfin, le multiplicateur de $u = \mu \cdot v^{(2)}$ est égal à $\mu^2 \cdot \det v$ ([14], p. 21–22).

29. *Cas III b:* $n = 6$, $\nu = 2$. On peut supposer f rapportée à une base de E telle que $f(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - \xi_2 \xi_5 + \xi_3 \xi_6$, l'élément $-a_4/a_1$ n'étant pas un carré dans K, ce qui signifie que le *discriminant* $d = a_1 a_4$ de f est tel que $-d$ *ne soit pas un carré* [15]. Soit $K_1 = K(\sqrt{-d})$ l'extension quadratique de K obtenue par adjonction d'une racine ω du polynôme $a_1 X^2 + a_4$, et soit E_1 l'espace vectoriel obtenu par extension à K_1 du corps des scalaires de E. La forme f est la restriction à E de la forme f_1 d'indice 3 sur E_1, telle que $f_1(x, x) = a_1(\xi_1 + \omega \xi_4)(\xi_1 - \omega \xi_4) - \xi_2 \xi_5 + \xi_3 \xi_6$, et les transformations de $GO_6^+(K, f)$ sont les restrictions à E des transformations de $GO_6^+(K_1, f_1)$ permutables avec la transformation semi-linéaire involutive $(\xi_k) \to (\xi_k^\sigma)$ (σ unique K-automorphisme de K_1 distinct de l'identité). Par le changement de coordonnées

$$\eta_1 = a_1(\xi_1 + \omega \xi_4),\ \eta_4 = \xi_1 - \omega \xi_4,\ \eta_k = \xi_k \text{ pour } k = 2, 3, 5, 6$$

la forme f_1 est ramenée à l'écriture du cas III a, et la transformation semi-linéaire involutive de E_1 s'écrit

$$(53) \qquad (\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6) \to (a_1 \eta_4^\sigma, \eta_2^\sigma, \eta_3^\sigma, a_1^{-1} \eta_1^\sigma, \eta_5^\sigma, \eta_6^\sigma).$$

Soit F_1 l'espace K_1^4, et identifions comme au n° 28 l'espace E_1 à l'espace des bivecteurs sur F_1, le point (η_k) étant identique au bivecteur dont les coordonnées sont η_k par rapport à la base formée des $e_i \wedge e_j$ $(i<j)$ ordonnée comme au n° 28. Soit F_1^* le dual de F_1, $(e'_i)_{1 \le i \le 4}$ la base duale de (e_i) dans F_1^*; désignons par φ l'application canonique de $F_1^{(2)}$ sur $F_1^{*(2)}$, définie par

$$\varphi(e_1 \wedge e_2) = e'_3 \wedge e'_4, \quad \varphi(e_1 \wedge e_3) = -e'_2 \wedge e'_4, \quad \varphi(e_1 \wedge e_4) = e'_2 \wedge e'_3$$
$$\varphi(e_3 \wedge e_4) = e'_1 \wedge e'_2, \quad \varphi(e_2 \wedge e_4) = -e'_1 \wedge e'_3, \quad \varphi(e_2 \wedge e_3) = e'_1 \wedge e'_4$$

([2], p. 108). Soit d'autre part ψ la corrélation involutive (relative à l'automorphisme σ de K_1) de F_1 sur F_1^*, telle que

$$\psi(e_1) = a_1^{-1} e'_2, \quad \psi(e_2) = -a_1^{-1} e'_1, \quad \psi(e_3) = -e'_4, \quad \psi(e_4) = e'_3.$$

On constate alors aisément que la transformation (53), composée avec l'homothétie de rapport a_1, n'est autre que l'application $\varphi^{-1} \cdot \psi^{(2)}$, où $\psi^{(2)}$ désigne l'application semi-linéaire de $F_1^{(2)}$ sur $F_1^{*(2)}$ déduite de ψ par extension aux produits extérieurs. Les transformations de $GO_6^+(K, f)$ sont donc les transformations $\mu \cdot v^{(2)}$, où $\mu \in K_1^*$ et $v \in GL_4(K_1)$, telles que

(54) $$\mu \cdot v^{(2)} \cdot \varphi^{-1} \cdot \psi^{(2)} = \mu^{\sigma} \cdot \varphi^{-1} \cdot \psi^{(2)} \cdot v^{(2)}.$$

Or, on a $v^{(2)} \cdot \varphi^{-1} = (\det v) \cdot \varphi^{-1} \cdot \check{v}^{(2)}$, $\check{v}$ désignant la contragrédiente de v ([2], p. 110, formule (30)); la formule (54) s'écrit donc encore

(55) $$\mu (\det v) \cdot (\check{v} \cdot \psi)^{(2)} = \mu^{\sigma} \cdot (\psi \cdot v)^{(2)}.$$

Si on pose $w = \psi \cdot v$, $w_1 = \check{v} \cdot \psi$, $w^{-1} w_1$ est une application linéaire de F_1 sur lui-même, et la formule (55) montre que $(w^{-1} w_1)^{(2)}$ est une homothétie dans $F_1^{(2)}$, donc que $w^{-1} w_1$ laisse invariant tout plan dans F_1. On en conclut comme ci-dessus que $w^{-1} w_1$ est une homothétie dans F_1, autrement dit que l'on a

(56) $$\psi \cdot v = \lambda \cdot \check{v} \cdot \psi$$

avec $\lambda \in K_1$; cela signifie que v permute projectivement avec la corrélation involutive ψ, ou encore, en posant $g(x, y) = \langle \psi(x), y \rangle$, que l'on a $g(v(x), v(y)) = \lambda g(x, y)$; en outre, si $\Delta = \det v$, la relation (55) montre que l'on doit avoir $\Delta = \mu^{\sigma - 1} \lambda$. La transformation v peut être quelconque dans $G U_4(K_1, g)$, car on a alors $\Delta \Delta^{\sigma} = \lambda^4$, et il est toujours possible de déterminer μ de façon à satisfaire à la relation ci-dessus (en notant que $\lambda^{\sigma} = \lambda \in K$); d'ailleurs, μ n'est ainsi déterminé qu'à un facteur près $\gamma \in K^*$. On conclut finalement que le groupe $G O_6^+(K, f)$ peut être décrit de la façon suivante: pour toute transformation v de $G U_4(K_1, g)$, soit $\chi(v)$ le quotient $\Delta \lambda^{-2}$ du déterminant de v par le carré de son multiplicateur. L'application $v \to \chi(v)$ est évidemment une représentation de $G U_4(K_1, g)$ dans le groupe N_1 des éléments de K_1 de *norme* 1; alors, *$G O_6^+(K, f)$ est isomorphe au quotient du sous-groupe Γ de $K_1^* \times G U_4(K_1, g)$ formé des couples (μ, v) tels que $\mu^{\sigma - 1} = \chi(v)$, par le sous-groupe des couples (γ^2, γ^{-1}), où γ parcourt K^** [14, p. 24]. On a d'ailleurs $g(x, x) = a_1^{-1} (\xi_1^{\sigma} \xi_2 - - \xi_2^{\sigma} \xi_1) - \xi_3^{\sigma} \xi_4 + \xi_4^{\sigma} \xi_3$, ce qui montre que ωg est une forme hermitienne d'indice 2 sur F_1.

30. Lorsque $n = 6$ et $\nu = 1$, supposons la forme f rapportée à une base telle que $f(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2 + \xi_3 \xi_6$, les éléments $-a_4/a_1$ et $-a_5/a_2$ n'étant pas des carrés dans K. Soit K_1 l'extension quadratique de K obtenue par adjonction d'une racine ω de $a_1 X^2 + a_4$; nous sommes amenés à distinguer deux cas, suivant que sur K_1, la forme à quatre variables $a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2$ est d'indice 2 ou d'indice 1; d'après le n° 25, cela revient à savoir si, en désignant par d le discriminant de f, $-d$ est ou non un *carré* dans K.

Cas III c: $n = 6$, $\nu = 1$, $-d$ est un carré. On peut supposer que $a_1 a_5 = a_2 a_4$, et par suite f est la restriction à E de la forme définie sur E_1

$$f_1(x, x) = a_1 (\xi_1 + \omega \xi_4)(\xi_1 - \omega \xi_4) - a_2 (\xi_2 + \omega \xi_5)(\xi_2 - \omega \xi_5) + \xi_3 \xi_6.$$

$G O_6^+(K, f)$ est le groupe des restrictions à E des transformations de $G O_6^+(K_1, f_1)$ permutables à $(\xi_k) \to (\xi_k^\sigma)$. On fait le changement de coordonnées

$$\eta_1 = a_1(\xi_1 + \omega \xi_4),\ \eta_4 = \xi_1 - \omega \xi_4,\ \eta_2 = a_2(\xi_2 + \omega \xi_5),\ \eta_5 = \xi_2 - \omega \xi_5,\ \eta_3 = \xi_3,\ \eta_6 = \xi_6$$

de sorte que la forme f_1 soit ramenée à l'écriture du cas III a; la transformation semi-linéaire sur E_1 est alors

$$(\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6) \to (a_1 \eta_4^\sigma, a_2 \eta_5^\sigma, \eta_3^\sigma, a_1^{-1} \eta_1^\sigma, a_2^{-1} \eta_2^\sigma, \eta_6^\sigma). \tag{57}$$

On constate alors aisément que cette transformation n'est autre que l'homothétie de rapport $-(a_1 a_2)^{-1}$ composée avec la puissance extérieure $\theta^{(2)}$, où θ désigne la collinéation involutive de F_1 (relative à σ) telle que

$$\theta(e_1) = e_4, \quad \theta(e_2) = a_2 e_3, \quad \theta(e_3) = a_1 e_2, \quad \theta(e_4) = a_1 a_2 e_1.$$

En écrivant que $\mu v^{(2)}$ permute avec $\theta^{(2)}$, il vient

$$\mu(v \cdot \theta)^{(2)} = \mu^\sigma (\theta \cdot v)^{(2)}$$

d'où on déduit, comme aux n^{os} précédents, que v doit permuter projectivement avec θ; d'ailleurs, on a $\theta^2(x) = a_1 a_2 x$, d'où si $\theta \cdot v = \lambda(v \cdot \theta)$, $\lambda \lambda^\sigma = 1$ (n° 19); en outre, on doit avoir $\mu^{1-\sigma} = \lambda^2$, ce qui est toujours possible et détermine μ à un facteur près γ arbitraire dans K^*. Notons maintenant que $a_1 a_2$ n'est pas de la forme $\zeta \zeta^\sigma$ dans K_1 (n° 25); suivant la méthode du n° 20 (note 1) formons l'extension quadratique K_2 de K_1, ayant pour base 1 et ϱ, avec $\varrho^2 = a_1 a_2$, $\zeta^\sigma = \varrho^{-1} \zeta \varrho$ et $\bar{\varrho} = -\varrho$; K_2 est le *corps des quaternions* (généralisés) sur K, correspondant au couple $(-a_4/a_1, a_1 a_2)$. L'espace E_1 est alors considéré commo espace vectoriel de dimension 2 sur K_2, et si on détermine $\beta \in K_1$ tel que $\lambda = \beta^{1-\sigma}$, βv est une application linéaire *arbitraire* w de cet espace sur lui-même; comme alors $\mu = \gamma \beta^2$, on a finalement $u = \gamma \cdot w^{(2)}$, et par suite $G O_6^+(K, f)$ *est isomorphe au quotient du groupe* $K^* \times G L_2(K_2)$ *par le sous-groupe formé des couples* (γ^2, γ^{-1}), *où* γ *parcourt* K^* [14].

31. *Cas III d:* $n = 6$, $\nu = 1$, $-d$ *n'est pas un carré* (ici encore, ce cas ne peut se présenter lorsque K est le corps des nombres réels). Avec les notations du n° 30, $-a_5/a_2$ n'est pas un carré dans K_1; soit K_2 le corps obtenu par adjonction à K d'une racine ω' de $a_2 X^2 + a_5$; K_1 et K_2 sont linéairement disjoints sur K, leur composé K_3 est une extension galoisienne de degré 4 sur K. La forme f est ici restriction à E de la forme

$$f_1(x, x) = a_1(\xi_1 + \omega \xi_4)(\xi_1 - \omega \xi_4) - a_2(\xi_2 + \omega' \xi_5)(\xi_2 - \omega' \xi_5) + \xi_3 \xi_6.$$

On fait ici le changement de coordonnées

$\eta_1 = a_1(\xi_1 + \omega\,\xi_4),\ \eta_4 = \xi_1 - \omega\,\xi_4,\ \eta_2 = a_2(\xi_2 + \omega'\,\xi_5),\ \eta_5 = \xi_2 - \omega'\,\xi_5,\ \eta_3 = \xi_3,\ \eta_6 = \xi_6$

et on voit que les transformations de $GO_6^+(K, f)$ sont celles de $GO_6^+(K_3, f_1)$ qui permutent aux deux transformations semi-linéaires de E_3 (espace obtenu à partir de E en étendant K à K_3)

$$(58)\qquad \begin{cases} (\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6) \to (a_1\eta_4^\sigma, \eta_2^\sigma, \eta_3^\sigma, a_1^{-1}\eta_1^\sigma, \eta_5^\sigma, \eta_6^\sigma) \\ (\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6) \to (\eta_1^\tau, a_2\eta_5^\tau, \eta_3^\tau, \eta_4^\tau, a_2^{-1}\eta_2^\tau, \eta_6^\tau) \end{cases}$$

σ et τ désignant les deux automorphismes de K_3 tels que $\omega^\sigma = -\omega$, $\omega'^\sigma = \omega'$, et $\omega^\tau = \omega$, $\omega'^\tau = -\omega'$. On voit comme au n° 29 que les transformations de $GO_6^+(K, f)$ sont de la forme $\mu \cdot v^{(2)}$, où v est une transformation linéaire de $K_3^4 = F_3$ qui doit permuter projectivement aux deux corrélations involutives ψ_0 et ψ_1 définies par les conditions

$$\psi_0(e_1) = e_2', \quad \psi_0(e_2) = -e_1', \qquad \psi_0(e_3) = -a_1 e_4', \quad \psi_0(e_4) = a_1 e_3'$$

$$\psi_1(e_1) = e_3', \quad \psi_1(e_2) = -a_2 e_4', \quad \psi_1(e_3) = -e_1', \qquad \psi_1(e_4) = a_2 e_2'$$

relatives respectivement aux automorphismes σ et τ; comme ces deux corrélations sont telles que $\psi_1^{-1} \cdot \psi_0$ soit une collinéation involutive, il revient au même de dire que v doit permuter projectivement à ψ_0 et à $a_2\psi_1^{-1} \cdot \psi_0 = \theta$, définie par

$$\theta(e_1) = e_4, \quad \theta(e_2) = a_2 e_3, \quad \theta(e_3) = a_1 e_2, \quad \theta(e_4) = a_1 a_2 e_1$$

et relative à l'automorphisme $\varpi = \sigma\tau$ de K_3. On a $\theta^2(x) = a_1 a_2 x$, et nous allons voir que $a_1 a_2$ n'est pas de la forme $\lambda\lambda^\varpi$. On peut en effet écrire $\lambda = \alpha + \beta\,\omega'$, où α et β appartiennent à $K(\omega)$. La relation $\lambda\lambda^\varpi = a_1 a_2$ donne alors les conditions

$$a_2\,\alpha\,\alpha^\sigma + a_5\,\beta\,\beta^\sigma = a_1 a_2^2$$

et

$$\beta\,\alpha^\sigma - \alpha\,\beta^\sigma = 0.$$

La seconde de ces conditions s'écrit $\left(\frac{\beta}{\alpha}\right)^\sigma = \frac{\beta}{\alpha}$ (en supposant $\alpha \neq 0$; le cas $\alpha = 0$ se traite de façon analogue); elle signifie donc que $\beta = \xi\,\alpha$, où $\xi \in K$; en posant alors $\frac{1}{\alpha} = \xi' + \omega\,\xi''$, où ξ' et ξ'' sont dans K, il vient $a_1(a_2\xi')^2 + a_4(a_2\xi'')^2 - a_2 - a_5\,\xi^2 = 0$, ce qui contredit l'hypothèse que la forme $a_1\xi_1^2 + a_4\xi_4^2 - a_2\xi_2^2 - a_5\xi_5^2$ est d'indice 0. Nous pouvons donc appliquer la méthode de la II^e partie (n° 19); comme on a $\psi_0 \cdot \theta = a_1 a_2\,\check{\theta} \cdot \psi_0$, on considère l'extension quadratique L de K_3, ayant pour base 1 et ϱ, avec $\varrho^2 = a_1 a_2$, $\zeta^\varpi = \varrho^{-1}\zeta\,\varrho$ pour $\zeta \in K_3$ et σ se prolonge en un antiautomorphisme $\xi \to \bar{\xi}$ de L en posant $\bar{\varrho} = \varrho$. On voit comme au n° 26 que si $K_0 = K(\sqrt{-d})$

est le corps des invariants de ϖ dans K_3, L est un corps de *quaternions* (généralisés) sur K_0, correspondant au couple $(-a_4/a_1, a_1 a_2)$.[1] La forme $g_1(x, y) = \langle \psi_0(x), y\rangle$ sur F_3 correspond sur l'espace F (espace F_3 considéré comme espace vectoriel à droite sur L) à la forme $g(x, y) = g_1(x, y) + (a_1 a_2)^{-1} \varrho\, g_1(\theta(x), y)$, telle que $g(y, x) = -\overline{g(x, y)}$ (il faudrait multiplier par exemple g par ω pour avoir une forme hermitienne); par rapport à la base (e_1, e_2) de F sur L, on a $g(x, y) = \bar{\xi}_1 \eta_2 - \bar{\xi}_2 \eta_1$. Cela étant, si on a $\theta \cdot v = \lambda(v \cdot \theta)$, on doit avoir $\lambda \lambda^{\varpi} = 1$ (n° 19); déterminant $\beta \in K_1$ par la condition $\beta^{1-\varpi} = \lambda$, $w = \beta v$ est une application linéaire de F sur lui-même, qui permute projectivement avec ψ_0 et par suite (n° 18) est un élément de $G U_2(L, g)$; et on a par hypothèse $u = \mu_0 \cdot w^{(2)}$, avec $\mu_0 \in K_1$. Inversement, si $w \in G U_2(L, g)$, on a $g_1(w(x), w(y)) = \lambda_0 g_1(x, y)$, avec $\lambda_0^{\sigma} = \lambda_0^{\varpi} = \lambda_0$ (n° 19), autrement dit, $\lambda_0 \in K$; cela s'écrit aussi $\psi_0 \cdot w = \lambda_0 \cdot \check{w} \cdot \psi_0$, et comme $w \cdot \theta = \theta \cdot w$, on a aussi $\psi_1 \cdot w = \lambda_0 \cdot \check{w} \cdot \psi_1$. Alors pour que $u = \mu_0 \cdot w^{(2)}$ appartienne à $G O_6^{+}(K, f)$, il faut et il suffit que, si $\Delta = \det w$, on ait $\Delta = \mu_0^{\sigma-1} \lambda_0^2 = \mu_0^{\tau-1} \lambda_0^2$ (n° 29); ces relations montrent d'abord que l'on doit avoir $\mu_0^{\sigma} = \mu_0^{\tau}$, donc $\mu_0 \in K_0 = K(\omega \omega')$, ce qui est compatible avec les relations $\Delta \Delta^{\sigma} = \Delta \Delta^{\tau} = \lambda_0^4$, qui donnent $\Delta \in K_0$. Comme dans K_0 les automorphismes σ et τ coïncident, on déterminera $\beta_0 \in K_0$ tel que $\Delta = \beta_0^{\sigma-1} \lambda_0^2$, et alors on a $\mu_0 = \gamma \beta_0$, où γ est arbitraire dans K^*. Finalement, on voit que *$G O_6^{+}(K, f)$ est isomorphe au quotient du sous-groupe Γ de $K_0^* \times G U_2(L, g)$ formé des couples (μ_0, w) tels que $\mu_0^{\sigma-1} = \chi(w)$, par le sous-groupe des couples (γ^2, γ^{-1}), où γ parcourt K^*.*

32. Lorsque $n = 6$ et $\nu = 0$, on peut supposer la forme f rapportée à une base telle que $f(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2 + a_3 \xi_3^2 + a_6 \xi_6^2$. Désignons par $\omega_1, \omega_2, \omega_3$ des racines des polynômes $a_1 X^2 + a_4$, $a_2 X^2 + a_5$, $a_3 X^2 + a_6$; le corps $K_1 = K(\omega_1, \omega_2, \omega_3)$ peut être une extension de K de degré 2, 4 ou 8. Dans le premier cas, on peut supposer que $\omega_1 = \omega_2 = \omega_3$, et le discriminant d de f est produit de $-\omega_3^2$ et d'un carré dans K; donc *$-d$ n'est pas un carré* dans K, on a $K_1 = K(\sqrt{-d})$, et l'indice de la forme f étendue à K_1 est 3. Lorsque K_1 est de degré 4 sur K, les trois corps $K(\omega_1)$, $K(\omega_2)$ et $K(\omega_3)$ peuvent être distincts ou non; s'ils sont distincts, ce sont les trois seuls sous-corps quadratiques du corps K_1, donc ω_3 appartient nécessairement à $K(\omega_1 \omega_2)$, et comme son carré est dans K, il est de la forme $c\, \omega_1 \omega_2$, avec $c \in K$; *$-d$ est alors un carré* dans K. Si au contraire, deux des trois corps $K(\omega_1)$, $K(\omega_2)$ et $K(\omega_3)$ sont confondus, on peut supposer par exemple que $\omega_1 = \omega_2$, ω_3 n'appartenant pas à $K(\omega_1)$; alors d est produit de $-\omega_3^2$ et d'un carré dans K, donc *$-d$ n'est pas un carré* dans K. Mais comme $-d$ est un carré dans $K(\sqrt{-d})$,

[1] On notera d'ailleurs que L n'est autre que le corps obtenu en étendant à K_0 le centre K du corps de quaternions généralisés sur K, relatif au couple $(-a_4/a_1, a_1 a_2)$.

il résulte du n° 29 que sur ce corps, la forme f a un indice égal à 1 ou à 3. Nous allons voir que si l'indice de f sur $K(\sqrt{-d})$ est 3, on peut par un changement de base se ramener au premier cas; cela va résulter du lemme élémentaire suivant:

Lemme. — *Soit f une forme bilinéaire symétrique sur un espace vectoriel E par rapport à un corps commutatif K. Soit α un élément non carré dans K, et soit E' l'espace vectoriel obtenu par extension du corps des scalaires de E à $K' = K(\sqrt{\alpha})$, et f' la forme bilinéaire f étendue à E'. S'il existe un vecteur $z \neq 0$ dans E' tel que $f'(z, z) = 0$, il existe deux vecteurs x, y de E non tous deux nuls et tels que $f(x, x) = -\alpha f(y, y)$ et $f(x, y) = 0$.*

Il suffit en effet de remarquer qu'on peut écrire $z = x + y\sqrt{\alpha}$, et que $f'(z, z) = f(x, x) + \alpha f(y, y) + 2\sqrt{\alpha} f(x, y)$.

Revenons alors à notre problème, et supposons que f ait un indice 3 sur $K(\sqrt{-d})$ (ce qui peut fort bien se produire, comme le montre l'exemple de la forme $\xi_1^2 + 2\xi_4^2 + 3\xi_2^2 + 6\xi_5^2 + \xi_3^2 + 3\xi_6^2$ sur le corps des rationnels). Alors, dans l'espace E' (obtenu par extension de K à $K(\sqrt{-d})$ à partir de E), un sous-espace isotrope de dimension 3 rencontre le sous-espace $\xi_3 = \xi_6 = 0$, donc sur $(K\sqrt{-d})$ la forme $a_1\xi_1^2 + a_4\xi_4^2 - a_2\xi_2^2 - a_5\xi_5^2$ a un indice au moins égal à 1. Le lemme prouve alors qu'on peut trouver une nouvelle base dans le sous-espace $\xi_3 = \xi_6 = 0$ de E, de sorte que la restriction de f à ce sous-espace s'écrive $b_1\eta_1^2 + b_4\eta_4^2 - b_2(\eta_2^2 + d\eta_5^2)$; comme en outre le discriminant $a_1a_2a_4a_5$ de cette restriction doit être un carré, on peut supposer que $b_4 = b_1 d$, et on se trouve bien alors ramené au premier cas. Le seul nouveau cas est donc celui où l'indice de f sur $K(\sqrt{-d})$ est égal à 1; alors l'indice de $a_1\xi_1^2 + a_4\xi_4^2 - a_2\xi_2^2 - a_5\xi_5^2$ sur ce corps est nécessairement égal à 0, et le discriminant de cette forme est un carré dans $K(\sqrt{-d})$.

Reste enfin à examiner le cas où $K_1 = K(\omega_1, \omega_2, \omega_3)$ est de degré 8 sur K; alors aucun des ω_i n'appartient au corps engendré par les deux autres; $-d$ est le produit de $(\omega_1\omega_2\omega_3)^2$ par un carré dans K, donc, comme $\omega_1\omega_2\omega_3$ ne peut appartenir à K, $-d$ *n'est pas un carré* dans K. Il résulte alors du n° 29 que l'indice de f sur le corps $K(\sqrt{-d})$ est nécessairement 0, 1 ou 3. Mais si l'indice de f est égal à 3 sur $K(\sqrt{-d})$ (ce qui peut fort bien se produire, comme le montre l'exemple $\xi_1^2 + 3\xi_4^2 + 2\xi_2^2 + 10\xi_5^2 + 5\xi_3^2 + 6\xi_6^2$ sur le corps des rationnels), on voit comme ci-dessus que par un changement de base dans E on peut se ramener au premier cas examiné dans ce n°. D'autre part, si l'indice de f sur $K(\sqrt{-d})$ est égal à 1, le lemme montre qu'un changement de base permet de se ramener au cas où $\omega_3^2 = -d$, et comme alors $(\omega_1\omega_2)^2$ est un carré dans K, les corps $K(\omega_1)$ et $K(\omega_2)$ sont identiques, et on est ramené au troisième des cas envisagés dans ce n°. Le seul cas nouveau est donc celui où l'indice de f sur $K(\sqrt{-d})$ est égal à 0.

On voit ainsi que tous les cas qui peuvent se présenter lorsque $\nu = 0$ sont caractérisés intrinsèquement par les propriétés du discriminant d, ou par la valeur de l'indice de f par rapport à $K(\sqrt{-d})$ lorsque $-d$ n'est pas un carré dans K.

33. *Cas III e: $n = 6$, $\nu = 0$, $-d$ n'est pas un carré dans K et l'indice de f par rapport à $K(\sqrt{-d})$ est égal à 3.* On peut supposer que $\omega_1 = \omega_2 = \omega_3 = \sqrt{-d}$, que nous noterons simplement ω, σ désignant l'unique automorphisme de $K(\omega) = K_1$ sur K distinct de l'identité. Soit E_1 l'espace obtenu en étendant K à K_1, f_1 la forme f prolongée à E_1; on fait ici le changement de variables

$$\eta_1 = a_1(\xi_1 + \omega\,\xi_4), \quad \eta_2 = a_2(\xi_2 + \omega\,\xi_5), \quad \eta_3 = a_3(\xi_3 + \omega\,\xi_6)$$

$$\eta_4 = \xi_1 - \omega\,\xi_4 \qquad \eta_5 = \xi_2 - \omega\,\xi_5, \qquad \eta_6 = \xi_3 - \omega\,\xi_6,$$

et les transformations de $G O_6^+(K, f)$ sont les restrictions à E des transformations de $G O_6^+(K_1, f_1)$ qui permutent avec

$$(\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6) \to (a_1\,\eta_4^\sigma,\ a_2\,\eta_5^\sigma,\ a_3\,\eta_6^\sigma,\ a_1^{-1}\,\eta_1^\sigma,\ a_2^{-1}\,\eta_2^\sigma,\ a_3^{-1}\,\eta_3^\sigma).$$

En raisonnant comme au n° 29, on voit que les transformations ayant cette propriété sont de la forme $\mu \cdot v^{(2)}$, où $v \in G L_4(K_1)$ doit permuter projectivement avec la corrélation involutive ψ telle que

$$\psi(e_1) = e_1', \quad \psi(e_2) = -a_2 a_3 e_2', \quad \psi(e_3) = a_1 a_3 e_3', \quad \psi(e_4) = -a_1 a_2 e_4'.$$

Si on pose $g(x, y) = \langle \psi(x), y \rangle$, g est une forme hermitienne sur $F_1 = K_1^4$, et v doit appartenir à $G U_4(K_1, g)$; on en déduit comme au n° 29 que *$G O_6^+(K, f)$ est isomorphe au quotient du sous-groupe Γ de $K_1^* \times G U_4(K_1, g)$ formé des couples (μ, v) tels que $\mu^{\sigma-1} = \chi(v)$, par le sous-groupe des couples (γ^2, γ^{-1}), où γ parcourt K^*.* On a d'ailleurs $g(z, z) = \bar{\zeta}_1 \zeta_1 - a_2 a_3 \bar{\zeta}_2 \zeta_2 + a_1 a_3 \bar{\zeta}_3 \zeta_3 - a_1 a_2 \bar{\zeta}_4 \zeta_4$ (en écrivant $\bar{\zeta}$ au lieu de ζ^σ); montrons que cette forme est *d'indice* 0. En effet, si on avait $g(z, z) = 0$ pour un vecteur $z \neq 0$ de F_1, on pourrait écrire, pour ce vecteur

$$\bar{\zeta}_1 \zeta_1 + a_1 a_3^{-1}(a_3 \bar{\zeta}_3)(a_3 \zeta_3) = a_2 a_3 (\bar{\zeta}_2 \zeta_2 + a_1 a_3^{-1} \bar{\zeta}_4 \zeta_4). \tag{59}$$

Mais dans K_1, on a l'identité (pour $c \in K$)

$$(\bar{\alpha}\alpha + c\bar{\beta}\beta)(\bar{\gamma}\gamma + c\bar{\delta}\delta) = (\bar{\alpha}\bar{\gamma} + c\bar{\beta}\bar{\delta})(\alpha\gamma + c\beta\delta) + c(\bar{\alpha}\delta - \bar{\beta}\gamma)(\alpha\bar{\delta} - \beta\bar{\gamma}) \tag{60}$$

et il résulterait donc de (59) qu'il existerait dans K_1 trois éléments non tous nuls α, β, γ tels que

$$a_1\bar{\alpha}\alpha - a_2\bar{\beta}\beta + a_3\bar{\gamma}\gamma = 0.$$

En écrivant chacun des éléments α, β, γ sous la forme $\xi + \omega\eta$, on en déduirait immédiatement que f a un indice > 0, contrairement à l'hypothèse.

34. *Cas III f: $n = 6$, $\nu = 0$, $-d$ est un carré dans K.* On notera que ce cas ne peut se produire lorsque K est le corps des nombres rationnels, car si $\nu = 0$, on peut supposer, en vertu du th. de Meyer, que tous les a_k sont de même signe, donc $-d$ ne peut être un carré. Par contre, ce cas se présente dans l'exemple suivant: si S_1 désigne le corps des séries formelles en t_1 à coefficients réels, K le corps des séries formelles en t_2 à coefficients dans S_1, la forme $\xi_1^2 + t_1\xi_4^2 + \xi_2^2 + t_2\xi_5^2 + \xi_3^2 - - t_1 t_2 \xi_6^2$ a un discriminant égal à $-(t_1 t_2)^2$, et il est facile de voir que cette forme est d'indice 0 (cf. [8], p. 35).

La discussion du n° 32 montre que sur $K_1 = K(\omega_1, \omega_2)$, la forme f s'écrit

$$f(x, x) = a_1(\xi_1^2 - \omega_1^2\xi_4^2) - a_2(\xi_2^2 - \omega_2^2\xi_5^2) + a_3(\xi_3^2 - \omega_1^2\omega_2^2\xi_6^2)$$

et la méthode habituelle montre que les transformations de $GO_6^+(K, f)$ sont de la forme $\mu\cdot v^{(2)}$, où $v \in GL_4(K_1)$ doit permuter projectivement aux deux collinéations θ_1, θ_2, définies par

$$\theta_1(e_1) = e_3, \quad \theta_1(e_2) = a_3 e_4, \quad \theta_1(e_3) = -a_1 a_3 e_1, \quad \theta_1(e_4) = -a_1 e_2$$

$$\theta_2(e_1) = e_2, \quad \theta_2(e_2) = a_2 a_3 e_1, \quad \theta_2(e_3) = -a_3 e_4, \quad \theta_2(e_4) = -a_2 e_3$$

et relatives respectivement aux automorphismes σ_1, σ_2 qui laissent invariants ω_2 et ω_1 respectivement. On a $\theta_1^2(x) = -a_1 a_3 x$, $\theta_2^2(x) = a_2 a_3 x$ et $\theta_1\cdot\theta_2 = -\theta_2\cdot\theta_1$. Appliquant la méthode générale (voir n° 20, note 1), montrons d'abord que $-a_1 a_3$ n'est pas de la forme $\lambda\lambda^{\sigma_1}$, avec $\lambda \in K_1$. On peut en effet écrire $\lambda = \alpha + \omega_2\beta$, où α et β appartiennent à $K(\omega_1)$. La relation $\lambda\lambda^{\sigma_1} = -a_1 a_3$ donne alors

$$\alpha\alpha^{\sigma_1} + \omega_2^2\beta\beta^{\sigma_1} = -a_1 a_3$$

et

$$\alpha\beta^{\sigma_1} + \beta\alpha^{\sigma_1} = 0.$$

De la seconde relation, on déduit, si $\alpha \neq 0$ (le cas $\alpha = 0$ se traiterait de même) que $\left(\frac{\beta}{\alpha}\right)^{\sigma_1} = -\frac{\beta}{\alpha}$, ce qui implique $\frac{\beta}{\alpha} = \omega_1\xi$, où $\xi \in K$. Il vient alors, en remarquant que $a_1 a_2 a_6 = -a_3 a_4 a_5$ par hypothèse, et en posant $\frac{1}{\alpha} = \xi' + \omega_1\xi''$, où ξ' et ξ'' sont dans K

$$a_1(a_3 + a_6\xi^2) + a_1 a_3^2(a_1\xi'^2 + a_4\xi''^2) = 0$$

ce qui est contraire à l'hypothèse $\nu = 0$. On peut donc définir l'extension quadratique L_1 de K_1, ayant pour base 1 et ϱ_1 sur K_1, avec $\varrho_1^2 = -a_1 a_3$ et $\zeta^{\sigma_1} = \varrho_1^{-1}\zeta\varrho_1$ pour $\zeta \in K_1$; en outre (n° 15) l'automorphisme σ_2 de K_1 se prolonge à L_1 en posant $\varrho^{\sigma_2} = -\varrho$. L'espace $F_1 = K_1^4$ de dimension 4 sur K_1 devient un espace F_1' de dimension 2 sur L_1, ayant pour base e_1 et e_2, et la collinéation θ_2 devient une collinéation de F_1', relative à l'automorphisme σ_2 de L_1 (n° 18). Enfin, si on a $\theta_1 \cdot v = \lambda_1 \cdot (v \cdot \theta_1)$, on doit avoir $\lambda_1 \lambda_1^{\sigma_1} = 1$ (n° 19) et $\mu^{1-\sigma_1} = \lambda_1^2$; en déterminant $\beta_1 \in K_1$ par la condition $\beta_1^{1-\sigma_1} = \lambda_1$, $w_1 = \beta_1 v$ devient une application linéaire de F_1' sur lui-même et $\mu = \mu_1\beta_1^2$, avec $\mu_1 \in K(\omega_2)$, d'où $u = \mu_1 \cdot w_1^{(2)}$.

Il faut en second lieu exprimer que w_1 permute projectivement avec la collinéation θ_2 de F_1'. Montrons cette fois que $a_2 a_3$ n'est pas de la forme $\lambda\lambda^{\sigma_2}$, où $\lambda \in L_1$. Si on pose $\lambda = \alpha + \varrho_1\beta$, où α et β appartiennent à K_1, la relation $\lambda\lambda^{\sigma_2} = a_2 a_3$ donne

$$\alpha\alpha^{\sigma_2} + a_1 a_3 \beta^{\sigma_1}\beta^{\sigma_2'} = a_2 a_3$$

$$\beta\alpha^{\sigma_2} - \alpha^{\sigma_1}\beta^{\sigma_2} = 0.$$

Posons $\beta = \zeta\alpha^{\sigma_1}$ (en supposant $\alpha \neq 0$); on a donc $\zeta\alpha^{\sigma_2} = \zeta^{\sigma_2}\alpha^{\sigma_1\sigma_2}$, et la première des équations précédentes devient

$$\alpha\alpha^{\sigma_2}(1 + a_1 a_3\zeta\zeta^{\sigma_1}) = a_2 a_3.$$

Or $\zeta\zeta^{\sigma_1}$ appartient à $K(\omega_2)$ et $\alpha\alpha^{\sigma_2}$ à $K(\omega_1)$; l'équation précédente n'est donc possible que si $\zeta\zeta^{\sigma_1}$ et $\alpha\alpha^{\sigma_2}$ appartiennent tous deux à K. Mais alors le raisonnement du début de ce n° prouve qu'il existe des éléments $\zeta_1 \in K(\omega_1)$, $\zeta_2 \in K(\omega_2)$, $\xi \in K$ et $\xi' \in K$ tels que $\zeta = \zeta_1(1 - \xi\omega_1\omega_2)^{-1}$ et $\alpha = \zeta_2^{-1}(1 + \xi'\omega_1\omega_2)$; la relation $\zeta\alpha^{\sigma_2} = \zeta^{\sigma_2}\alpha^{\sigma_1\sigma_2}$ donne alors $\xi = \xi'$, et en posant $\zeta_3 = 1 - \xi\omega_1\omega_2$, on a donc

$$\zeta\zeta^{\sigma_1} = \frac{\zeta_1\zeta_1^{\sigma_1}}{\zeta_3\zeta_3^{\sigma_1}} \text{ et } \frac{1}{\alpha\alpha^{\sigma_2}} = \frac{\zeta_2\zeta_2^{\sigma_2}}{\zeta_3\zeta_3^{\sigma_1}}.$$

On devrait alors avoir

$$a_1 a_3\zeta_1\zeta_1^{\sigma_1} - a_2 a_3\zeta_2\zeta_2^{\sigma_2} + \zeta_3\zeta_3^{\sigma_1} = 0$$

ce qui est encore contraire à l'hypothèse $\nu = 0$.

On peut alors former l'extension quadratique L de L_1, ayant pour base 1 et ϱ_2 sur L_1, avec $\varrho_2^2 = a_2 a_3$ et $\zeta^{\sigma_2} = \varrho_2^{-1}\zeta\varrho_2$ pour $\zeta \in L_1$; l'espace F_1' s'identifie avec le corps L, en identifiant e_1 avec l'unité. Si $\theta_2 \cdot w_1 = \lambda_2(w_1 \cdot \theta_2)$ avec $\lambda_2 \in K_1$, on doit avoir $\lambda_2\lambda_2^{\sigma_2} = 1$ et $\mu_1^{1-\sigma_2} = \lambda_2^2$; on détermine encore $\beta_2 \in K_1$ de sorte que $\beta_2^{1-\sigma_2} = \lambda_2$;

alors $\beta_2 w_1$ devient une *homothétie* à gauche $z \to t z$ du corps L, et si w désigne cette homothétie, on a $\mu_1 = \gamma \beta_2^2$ avec $\gamma \in K$ et $u = \gamma \cdot w^{(2)}$. On voit donc que $G O_6^+(K, f)$ *est isomorphe au quotient du groupe $K^* \times L^*$ par le sous-groupe des couples (γ^2, γ^{-1}), où γ parcourt K^*.* On notera que les éléments 1, ϱ_1, ϱ_2 et $\varrho_1 \varrho_2$ forment une base de L *sur* K_1, telle que $\varrho_1^2 = -a_1 a_3$, $\varrho_2^2 = a_2 a_3$ et $\varrho_2 \varrho_1 = -\varrho_1 \varrho_2$; le sous-corps L' de L ayant pour base 1, ϱ_1, ϱ_2 et $\varrho_1 \varrho_2$ *sur* K est donc un corps de quaternions généralisés sur K, correspondant au couple $(-a_1 a_3, a_2 a_3)$; si on cherche le sous-corps commutant L'' de L' dans L, on trouve que L'' a pour base 1, $\varrho_1 \omega_2$, $\varrho_2 \omega_1$ et $\varrho_1 \omega_2 \varrho_2 \omega_1$ sur K; comme on a $(\varrho_1 \omega_2)^2 = -a_3 a_4$, $(\varrho_2 \omega_1)^2 = a_3 a_5$ et $(\varrho_1 \omega_2)(\varrho_2 \omega_1) = -(\varrho_2 \omega_1)(\varrho_1 \omega_2)$, on voit que L'' est un corps de quaternions généralisés sur K, correspondant au couple $(-a_3 a_4, a_3 a_5)$; comme K est l'intersection de L' et L'', on voit que L *est le produit tensoriel $L' \otimes L''$ de deux corps de quaternions généralisés sur K.*[1]

35. *Cas III g: $n = 6$, $\nu = 0$, $-d$ n'est pas un carré dans K et l'indice de f par rapport à $K(\sqrt{-d})$ est égal à* 1. Ce cas ne peut se produire lorsque K est le corps des nombres réels; il peut par contre être réalisé lorsque K est le corps des nombres rationnels. En effet, considérons par exemple la forme $\xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2 + \xi_5^2 + 7\xi_6^2$ sur le corps des rationnels; on a $d = 7$; si la forme avait un indice égal à 3 sur le corps $K(\sqrt{-7})$, il existerait dans le sous-espace $\xi_3 = \xi_6 = 0$ une base par rapport à laquelle la forme $\xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2$ s'écrirait $a_1(\eta_1^2 + 7\eta_2^2) + a_2(\eta_3^2 + 7\eta_4^2)$ (cf. n° 32). Il résulte alors du n° 25 que, dans le corps des quaternions ordinaires sur K (c'est-à-dire relatifs au couple $(-1, -1)$) il existerait deux quaternions $\boldsymbol{q}_1$, $\boldsymbol{q}_2$ tels que l'on ait identiquement $\boldsymbol{q}_1^2 \boldsymbol{z} \boldsymbol{q}_2^2 = -7\boldsymbol{z}$ pour tout quaternion $\boldsymbol{z}$; on en conclut immédiatement qu'on devrait avoir $\boldsymbol{q}_2^2 = -7\boldsymbol{q}_1^{-2}$, et que $\boldsymbol{q}_1^2$ devrait appartenir à K; mais on peut aisément vérifier que cette condition ne peut être réalisée dans le corps des quaternions ordinaires sur le corps des rationnels, parce que 7 n'est pas la somme de trois carrés rationnels.

D'après l'étude faite au n° 32, on peut supposer la forme f rapportée à une base telle que, sur le corps $K_1 = K(\omega, \omega')$, où $\omega^2 = -a_4/a_1 = -a_5/a_2$ et $\omega'^2 = -a_6/a_3$, on ait

$$f(x, x) = a_1(\xi_1^2 - \omega^2 \xi_4^2) - a_2(\xi_2^2 - \omega^2 \xi_5^2) + a_3(\xi_3^2 - \omega'^2 \xi_6^2).$$

On a d'ailleurs $K(\omega') = K(\sqrt{-d})$ et la forme $a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2$ est d'indice 0 sur $K_0 = K(\sqrt{-d})$. On voit comme dans les autres cas que les transformations

[1] A. Albert a démontré [1] que si K est un corps de nombres algébriques, le produit tensoriel de deux corps de quaternions généralisés sur K n'est jamais un corps; le cas (III f) ne se présente donc pas dans ces circonstances.

de $GO_6^+(K, f)$ sont de la forme $\mu \cdot v^{(2)}$, où $v \in GL_4(K_1)$ doit permuter projectivement à la collinéation θ telle que

$$\theta(e_1) = e_4, \quad \theta(e_2) = a_2 e_3, \quad \theta(e_3) = a_1 e_2, \quad \theta(e_4) = a_1 a_2 e_1$$

relative à l'automorphisme σ de K_1 qui laisse invariant ω', et à la corrélation ψ telle que

$$\psi(e_1) = e_4', \quad \psi(e_2) = -a_3 e_3', \quad \psi(e_3) = a_3 e_2', \quad \psi(e_4) = -e_1',$$

relative à l'automorphisme τ de K_1 qui laisse invariant ω. On a $\theta^2(x) = a_1 a_2 x$, et l'hypothèse implique que $a_1 a_2$ n'est pas de la forme $\lambda \lambda^\sigma$, où $\lambda \in K_1$ (voir le raisonnement du n° 31). On a d'autre part $\psi \cdot \theta = -a_1 a_2 \check{\theta} \cdot \psi$; appliquant la méthode du n° 19, on considère l'extension quadratique L de K_1, ayant pour base 1 et ϱ, avec $\varrho^2 = a_1 a_2$, $\zeta^\sigma = \varrho^{-1} \zeta \varrho$ pour $\zeta \in K_1$, et on prolonge τ en un antiautomorphisme $\xi \to \bar{\xi}$ de L en posant $\bar{\varrho} = -\varrho$. L est un corps de quaternions généralisés sur K_0, correspondant au couple $(-a_4/a_1, a_1 a_2)$. Soit $F_1 = K_1^4$, et soit F l'espace F_1 considéré comme espace vectoriel à droite de dimension 2 sur L; la forme $g_1(x, y) = \langle \psi(x), y \rangle$ sur F_1 correspond sur l'espace F à la forme $g(x, y) = g_1(x, y) - (a_1 a_2)^{-1} \varrho\, g_1(\theta(x), y)$; par rapport à la base (e_1, e_2) de F, on a

$$g(x, y) = (a_1 a_2)^{-1} (\bar{\xi}_1 \varrho \eta_1 - a_2 a_3 \bar{\xi}_2 \varrho \eta_2);$$

on a $g(y, x) = -\overline{g(x, y)}$ (on obtiendrait une forme hermitienne en multipliant g par ω'). On termine alors le raisonnement exactement comme dans le n° 31, ce qui prouve que $GO_6^+(K, f)$ *est isomorphe au quotient du sous-groupe* Γ *de* $K_0^* \times GU_2(L, g)$ *formé des couples* (μ_0, w) *tels que* $\mu_0^{\tau-1} = \chi(w)$, *par le sous-groupe des couples* (γ^2, γ^{-1}), *où* γ *parcourt* K^*. On notera qu'ici la forme g est *d'indice* 0; en effet; dans le cas contraire, il existerait $x \in F_1$ tel que $g_1(\theta(x), x) = 0$, ce qui donne

$$\zeta_1^{\sigma\tau} \zeta_1 - a_2 a_3 \zeta_2^{\sigma\tau} \zeta_2 + a_1 a_3 \zeta_3^{\sigma\tau} \zeta_3 - a_1 a_2 \zeta_4^{\sigma\tau} \zeta_4 = 0$$

et on montre comme au n° 33 que cela est contraire à l'hypothèse $\nu = 0$.

36. *Cas III h:* $n = 6$, $\nu = 0$, $-d$ *n'est pas un carré dans* K *et l'indice de* f *par rapport à* $K(\sqrt{-d})$ *est égal à* 0. En vertu du th. de Meyer, ce cas ne peut se présenter si K est le corps des nombres rationnels, car si x est un vecteur quelconque $\neq 0$ dans E, le sous-espace orthogonal à x est de dimension 5, et par suite il existe y orthogonal à x et tel que $f(y, y) = d f(x, x)$, puisque $d > 0$. On a un exemple du cas III h en considérant le corps S_1 des séries formelles en t_1 à coefficients réels, le corps S_2 des séries formelles en t_2 à coefficients dans S_1, et le corps K des séries formelles en t_3 à coefficients dans S_2; il est facile de voir que la

forme $\xi_1^2 + t_1 \xi_4^2 + \xi_2^2 + t_2 \xi_5^2 + \xi_3^2 + t_3 \xi_6^2$ sur K est d'indice 0 sur $K(\sqrt{-t_1 t_2 t_3})$ (cf. [8], p. 35).

Avec les notations du n° 32, la forme f s'écrit sur le corps $K_1 = K(\omega_1, \omega_2, \omega_3)$

$$f(x, x) = a_1(\xi_1^2 - \omega_1^2 \xi_4^2) - a_2(\xi_2^2 - \omega_2^2 \xi_5^2) + a_3(\xi_3^2 - \omega_3^2 \xi_6^2).$$

Nous désignerons par σ_k l'automorphisme de K_1 qui laisse invariant les deux ω_i d'indices $\neq k$ et transforme ω_k en $-\omega_k$ $(k = 1, 2, 3)$. Les transformations de $GO_6^+(K, f)$ sont les transformations $u = \mu \cdot v^{(2)}$, où $\mu \in K_1$, $v \in GL_4(K_1)$, et où v doit permuter projectivement aux trois corrélations involutives ψ_1, ψ_2, ψ_3 définies respectivement par

$$\begin{array}{llll} \psi_1(e_1) = e_2', & \psi_1(e_2) = -e_1', & \psi_1(e_3) = -a_1 e_4', & \psi_1(e_4) = a_1 e_3' \\ \psi_2(e_1) = e_3', & \psi_2(e_2) = -a_2 e_4', & \psi_2(e_3) = -e_1', & \psi_2(e_4) = a_2 e_2' \\ \psi_3(e_1) = e_4', & \psi_3(e_2) = -a_3 e_3', & \psi_3(e_3) = a_3 e_2', & \psi_3(e_4) = -e_1' \end{array}$$

la corrélation ψ_k étant relative à l'automorphisme σ_k de K_1. Il revient au même de dire que v doit permuter projectivement à ψ_2 et aux deux collinéations involutives $\theta_1 = -a_3 \psi_3^{-1} \cdot \psi_2$ et $\theta_3 = a_1 \psi_1^{-1} \cdot \psi_2$; ces collinéations sont relatives respectivement aux automorphismes $\tau_1 = \sigma_2 \sigma_3$ et $\tau_3 = \sigma_1 \sigma_2$ de K_1, et on a

$$\begin{array}{llll} \theta_1(e_1) = e_2, & \theta_1(e_2) = a_2 a_3 e_1, & \theta_1(e_3) = -a_3 e_4, & \theta_1(e_4) = -a_2 e_3 \\ \theta_3(e_1) = e_4, & \theta_3(e_2) = a_2 e_3, & \theta_3(e_3) = a_1 e_2, & \theta_3(e_4) = a_1 a_2 e_1. \end{array}$$

On a $\theta_1^2(x) = a_2 a_3 x$, $\theta_3^2(x) = a_1 a_2 x$, $\theta_1 \cdot \theta_3 = -\theta_3 \cdot \theta_1$; en outre, ${}^t\psi_2 = -\psi_2$, $\psi_2 \cdot \theta_1 = a_2 a_3 \check{\theta}_1 \cdot \psi_2$, $\psi_2 \cdot \theta_3 = a_1 a_2 \check{\theta}_3 \cdot \psi_2$. Nous allons appliquer la méthode de n° 19.

Montrons en premier lieu que $a_2 a_3$ n'est pas de la forme $\lambda \lambda^{\tau_1}$, où $\lambda \in K_1$. Si $K_0 = K(\sqrt{-d}) = K(\omega_1 \omega_2 \omega_3)$, il suffit de remarquer que τ_1 laisse invariants les éléments de K_0, et que l'on peut écrire $K_1 = K_0(\omega_2, \omega_3)$; on raisonne alors comme au début du n° 34, en utilisant l'hypothèse que l'indice de f sur K_0 est égal à 0. On considère alors l'extension quadratique L_1 de K_1, ayant pour base 1 et ϱ_1, avec $\varrho_1^2 = a_2 a_3$ et $\zeta^{\tau_1} = \varrho_1^{-1} \zeta \varrho_1$ pour $\zeta \in K_1$; on prolonge σ_2 en un antiautomorphisme $\xi \to \bar{\xi}$ de L_1 en posant $\bar{\varrho}_1 = \varrho_1$, et τ_3 en un automorphisme de L_1 en posant $\varrho_1^{\tau_3} = -\varrho_1$. L'espace $F_1 = K_1^4$ devient un espace F_1' de dimension 2 sur L_1, ayant pour base e_1 et e_3; la corrélation ψ_2 correspond à la corrélation ψ_0 de F_1', relative à l'antiautomorphisme $\xi \to \bar{\xi}$, et telle que

$$\langle \psi_0(x), y \rangle = \langle \psi_2(x), y \rangle + (a_2 a_3)^{-1} \varrho_1 \langle \psi_2(\theta_1(x)), y \rangle.$$

La collinéation θ_3 devient une collinéation de F_1' relative à τ_3, telle que $\psi_0 \cdot \theta_3 = a_1 a_2 \check{\theta}_3 \cdot \psi_0$. Enfin, si $\theta_1 \cdot v = \lambda_1 (v \cdot \theta_1)$, avec $\lambda_1 \in K_1$ on doit avoir $\lambda_1 \lambda^{\tau_1} = 1$; en déterminant $\beta_1 \in K_1$ par la condition $\beta_1^{1-\tau_1} = \lambda_1$, $\beta_1 v$ devient une application linéaire w_1 de F_1' sur lui-même, qui doit permuter projectivement avec ψ_0 et θ_3.

On montre ensuite que $a_1 a_2$ n'est pas de la forme $\lambda \lambda^{\tau_3}$, avec $\lambda \in L_1$, en utilisant le fait que f est d'indice 0 sur K_0, et en raisonnant comme au n° 34 (K_0 jouant ici le rôle tenu par K dans le n° 34). On peut alors former l'extension quadratique L de L_1, ayant pour base 1 et ϱ_3 sur L_1, avec $\varrho_3^2 = a_1 a_2$, $\zeta^{\tau_3} = \varrho_3^{-1} \zeta \varrho_3$ pour $\zeta \in L_1$; l'espace F_1' s'identifie avec le corps L en identifiant e_1 avec l'unité. On prolonge l'antiautomorphisme $\xi \to \bar{\xi}$ à L en posant $\bar{\varrho}_3 = \varrho_3$; la corrélation correspond alors à la forme bilinéaire sur L

$$g(x, y) = (a_1 a_2 a_3)^{-1} \bar{x} \varrho_3 \varrho_1 y$$

telle que $g(y, x) = -\overline{g(x, y)}$. Si $\theta_3 \cdot w_1 = \lambda_3 (w_1 \cdot \theta_3)$ avec $\lambda_3 \in K_1$, on doit avoir $\lambda_3 \lambda_3^{\tau_3} = 1$. On détermine encore $\beta_3 \in K_1$ de sorte que $\beta_3^{1-\tau_3} = \lambda_3$; alors $w = \beta_3 w_1$ devient une *homothétie* à gauche du corps L, qui doit permuter projectivement avec la corrélation involutive correspondant à la forme g; si $w(z) = t z$, on constate aisément que cela signifie que l'on a $\bar{t} \varrho_3 \varrho_1 t = \lambda_0(t) \varrho_3 \varrho_1$, où $\lambda_0(t)$ est un élément de K. Par hypothèse, on a $u = \mu_0 \cdot w^{(2)}$, où $\mu_0 \in K_1$. Inversement, si w appartient à $G U_1(L, g)$, on a $\psi_2 \cdot w = \lambda_0 \cdot \check{w} \cdot \psi_0$ avec $\lambda_0 \in K$, et comme w permute avec θ_1 et θ_3, on a aussi $\psi_1 \cdot w = \lambda_0 \cdot \check{w} \cdot \psi_1$ et $\psi_3 \cdot w = \lambda_0 \cdot \check{w} \cdot \psi_3$. Pour que $u = \mu_0 \cdot w^{(2)}$ appartienne à $G O_6^+(K, f)$, il faut et il suffit que, si $\Delta = \det w$ (où w est considéré comme transformation de F_1), on ait $\Delta = \mu_0^{\sigma_1 - 1} \lambda_0^2 = \mu_0^{\sigma_2 - 1} \lambda_0^2 = \mu_0^{\sigma_3 - 1} \lambda_0^2$ (n° 29); on en tire d'abord que $\mu_0 \in K_0$, puisque $\mu_0^{\sigma_1} = \mu_0^{\sigma_2} = \mu_0^{\sigma_3}$; d'ailleurs on a aussi $\Delta \in K_0$, puisque $\Delta \Delta^{\sigma_1} = \Delta \Delta^{\sigma_2} = \Delta \Delta^{\sigma_3} = \lambda_0^4$. On déterminera alors $\beta_0 \in K_0$ tel que $\beta_0^{\sigma_1 - 1} \lambda_0^2 = \Delta$, et on aura alors $\mu_0 = \gamma \beta_0$, où γ est arbitraire dans K^*. On voit donc que *$G O_6^+(K, f)$ est isomorphe au quotient du sous-groupe Γ de $K_0^* \times G U_1(L, g)$ formé des couples (μ_0, w) tels que $\mu_0^{\sigma_1 - 1} = \chi(w)$, par le sous-groupe des couples (γ^2, γ^{-1}), où γ parcourt K^*.*

On notera que les éléments 1, ϱ_1, ϱ_3 et $\varrho_1 \varrho_3$ forment une base de L sur K_1, telle que $\varrho_1^2 = a_2 a_3$, $\varrho_3^2 = a_1 a_2$ et $\varrho_3 \varrho_1 = -\varrho_1 \varrho_3$; le sous-corps L' ayant pour base 1, ϱ_1, ϱ_3 et $\varrho_1 \varrho_3$ *sur* $K_0 = K(\sqrt{-d})$ est un corps de quaternions généralisés sur K_0, correspondant au couple $(a_2 a_3, a_1 a_2)$; le sous-corps commutant L'' de L' dans L a pour base 1, $\varrho_1 \omega_1$, $\varrho_3 \omega_3$ et $\varrho_1 \omega_1 \varrho_3 \omega_3$ sur K_0; c'est un corps de quaternions généralisés sur K_0, correspondant au couple $(-a_1 a_2 a_3 a_4, -a_1 a_2 a_3 a_6)$; *$L$ est le produit tensoriel $L' \otimes L''$ de deux corps de quaternions généralisés sur $K_0 = K(\sqrt{-d})$.*

37. *Cas IV a: $n = 5$, $\nu = 2$.* On peut ici supposer la forme f rapportée à une base de E telle que $f(x, x) = \xi_1 \xi_4 - \xi_2 \xi_5 + \xi_3^2$; on considère E comme le sous-espace $\xi_6 = 0$ d'un espace E' de dimension 6 sur K, f étant la restriction à E de la forme

f' telle que $f'(x, x) = \xi_1 \xi_4 - \xi_2 \xi_5 + \xi_3^2 - \xi_6^2$, et le groupe $O_5^+(K, f)$ est le sous-groupe de $GO_6^+(K, f')$ formé des transformations qui laissent invariant ξ_6. On ramène la forme f' à l'écriture du cas III a, par le changement de variables

$$\eta_k = \xi_k \text{ pour } k = 1, 2, 4, 5, \quad \eta_3 = \xi_3 + \xi_6, \quad \eta_6 = \xi_3 - \xi_6.$$

Or, dire que $u = \mu \cdot v^{(2)}$ laisse invariant $\eta_3 - \eta_6$ signifie encore que $\mu \cdot {}^t v^{(2)}$ laisse invariante la forme alternée $e'_1 \wedge e'_4 - e'_2 \wedge e'_3$ sur $F = K^4$. En d'autres termes, si on pose

$$g(x, y) = \langle x \wedge y, e'_1 \wedge e'_4 - e'_2 \wedge e'_3 \rangle = \xi_1 \eta_4 - \xi_4 \eta_1 + \xi_3 \eta_2 - \xi_2 \eta_3$$

on doit avoir $g(v(x), v(y)) = \mu^{-1} g(x, y)$; donc v doit appartenir au groupe $GSp_4(K)$ des transformations de F laissant invariante g à un facteur près, et si λ est le multiplicateur de v, la transformation $u \in GO_6^+(K, f')$ correspondant à v est bien déterminée et égale à $\lambda^{-1} \cdot v^{(2)}$. Comme lorsqu'on remplace v par γv (avec $\gamma \in K^*$), λ est multiplié par γ^2, on voit que *$O_5^+(K, f)$ est isomorphe au quotient par K^* du groupe $GSp_4(K, f)$*[1] [14, p. 27].

38. *Cas IV b:* $n = 5$, $\nu = 1$. On peut supposer la forme f rapportée à une base de E telle que $f(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - \xi_2 \xi_5 + \xi_3^2$, $-a_4/a_1$ n'étant pas un carré dans K. Soit K_1 le corps obtenu par adjonction à K d'une racine ω de $a_1 X^2 + a_4$; on considère l'espace E_1 sur K_1, obtenu à partir de E par extension à K_1 du corps des scalaires, comme le sous-espace $\xi_6 = 0$ d'un espace E'_1 de dimension 6 sur K_1, et la forme f comme la restriction à E de la forme f' (sur E'_1) telle que $f'(x, x) = a_1(\xi_1 + \omega \xi_4)(\xi_1 - \omega \xi_4) - \xi_2 \xi_5 + \xi_3^2 - \xi_6^2$. Les raisonnements des n^{os} 29 et 37 montrent alors que $O_5^+(K, f)$ est isomorphe au sous-groupe des transformations de $GO_6^+(K, f')$ qui laissent invariant $\eta_3 - \eta_6$ et permutent à la transformation involutive (53); et toute transformation de ce sous-groupe est de la forme $u = \mu \cdot v^{(2)}$, où $v \in GL_4(K_1)$ est assujettie aux conditions suivantes. Si on considère la corrélation involutive ψ_1, relative à l'automorphisme σ de K_1, telle que

$$\psi_1(e_1) = e'_2, \quad \psi_1(e_2) = -e'_1, \quad \psi_1(e_3) = -a_1 e'_4, \quad \psi_1(e_4) = a_1 e'_3$$

et la corrélation involutive (relative à l'automorphisme identique) ψ_2 telle que

$$\psi_2(e_1) = e'_4, \quad \psi_2(e_2) = -e'_3, \quad \psi_2(e_3) = e'_2, \quad \psi_2(e_4) = -e'_1$$

---

[1] Il est facile de voir que si v est un élément du groupe $GSp_{2m}(K)$, le déterminant de v est lié à son multiplicateur λ_v par la relation $\det v = \lambda_v^m$; en effet, ${}^t v^{(2)}$ multiplie par λ_v une biforme g sur l'espace K^{2m}; la puissance extérieure m-ème de g transformée par la puissance extérieure m-ème de ${}^t v^{(2)}$ (égale à la puissance extérieure $2m$-ème de ${}^t v$) est donc multipliée par λ_v^m; mais la puissance extérieure $2m$-ème de ${}^t v$ est l'homothétie de rapport $\det v$, d'où la proposition.

v doit permuter projectivement avec ψ_1 et ψ_2; de façon précise, on doit avoir $\psi_2 \cdot v = \mu^{-1} \cdot \check{v} \cdot \psi_2$, et si $\psi_1 \cdot v = \lambda \cdot \check{v} \cdot \psi_1$ (avec $\lambda = \lambda^\sigma \in K$), il faut que $\Delta = \mu^{\sigma-1} \lambda^2$, où $\Delta = \det v$. Soit θ la collinéation involutive de $F_1 = K_1^4$ telle que $\theta = \psi_2^{-1} \cdot \psi_1$, relative à l'automorphisme σ, et définie par

$$\theta(e_1) = e_3, \quad \theta(e_2) = e_4, \quad \theta(e_3) = -a_1 e_1, \quad \theta(e_4) = -a_1 e_2.$$

Il revient au même de dire qu'on doit avoir $\psi_1 \cdot v = \lambda \cdot \check{v} \cdot \psi_1$ et $\theta \cdot v = \lambda \mu \cdot v \cdot \theta$, cette dernière relation entraînant $\lambda^2 \mu \mu^\sigma = 1$.

Cela étant, on a $\theta^2(x) = -a_1 x$ et $\psi_1 \cdot \theta = -a_1 \check{\theta} \cdot \psi_1$. L'élément $-a_1$ n'est pas de la forme $\zeta \zeta^\sigma$, où $\zeta \in K_1$, car on voit aussitôt que cela entraînerait que la forme quadratique $a_1 \xi_1^2 + a_4 \xi_4^2 + \xi_3^2$ aurait un indice > 0 sur K, ce qui est contraire à l'hypothèse. On peut donc former l'extension quadratique L de K_1, ayant pour base 1 et ϱ, avec $\varrho^2 = -a_1$ et $\zeta^\sigma = \varrho^{-1} \zeta \varrho$ pour $\zeta \in K_1$; on vérifie aussitôt que L est un corps de quaternions généralisé sur K, relatif au couple $(-a_4/a_1, -a_1)$; on prolonge l'automorphisme σ de K_1 en un antiautomorphisme $\xi \to \bar{\xi}$ de L en posant $\bar{\varrho} = \varrho$. La corrélation ψ_1 correspond, sur l'espace F (espace F_1 considéré comme espace de dimension 2 sur L) à la forme

$$g(x, y) = \langle \psi_1(x), y \rangle + \varrho \langle \psi_1(\theta(x)) y \rangle$$

qui, par rapport à la base de F formée de e_1 et e_2, s'écrit $g(x, y) = \bar{\xi}_1 \eta_2 - \bar{\xi}_2 \eta_1$. Si alors on détermine $\beta \in K_1$ tel que $\beta^{1-\sigma} = \lambda \mu$, $w = \beta v$ est une transformation linéaire de F, telle que $\psi_1 \cdot w = \alpha \cdot \check{w} \cdot \psi_1$, avec $\alpha = \mu^{-1} \beta^2$, et on a $u = \mu \beta^{-2} w^{(2)} = \alpha^{-1} \cdot w^{(2)}$. On en conclut que *$O_5^+(K, f)$ est isomorphe au quotient par K^* du groupe $GU_2(L, g)$*.

39. Lorsque $n = 5$ et $\nu = 0$, on peut supposer la forme f rapportée à une base telle que $f(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2 + \xi_3^2$; nous distinguerons deux cas, suivant qu'il existe une extension quadratique de K par rapport à laquelle f est d'indice 2, ou qu'il n'existe pas de telle extension.

Cas IV c: $n = 5$, $\nu = 0$, il existe une extension quadratique de K par rapport à laquelle f est d'indice 2. En utilisant le lemme du n° 32, on voit qu'on peut alors supposer que $a_4/a_1 = a_5/a_2$, l'élément $-a_4/a_1$ n'étant pas un carré dans K. Soit K_1 le corps obtenu en adjoignant à K une racine ω de $a_1 X^2 + a_4$; l'espace E_1 sur K_1, obtenu à partir de E par extension à K_1 du corps des scalaires, est considéré comme le sous-espace $\xi_6 = 0$ d'un espace E_1' de dimension 6 sur K_1, et la forme f comme la restriction à E de la forme f' (sur E_1') telle que $f'(x, x) = a_1(\xi_1 + \omega \xi_4)(\xi_1 - \omega \xi_4) - a_2(\xi_2 + \omega \xi_5)(\xi_2 - \omega \xi_5) + \xi_3^2 - \xi_6^2$. On voit alors comme aux n^{os} 30 et 37 que

$O_5^+(K, f)$ est isomorphe au sous-groupe de $GO_6^+(K_1, f')$ qui laisse invariant $\eta_3 - \eta_6$ et permute à la transformation involutive (57); et toute transformation de ce sous-groupe est de la forme $u = \mu \cdot v^{(2)}$ où $v \in GL_4(K_1)$ est assujettie aux conditions suivantes. Soit θ la collinéation involutive de $F_1 = K_1^4$ relative à l'automorphisme σ de K_1, et définie par

$$\theta(e_1) = e_4, \quad \theta(e_2) = a_2 e_3, \quad \theta(e_3) = a_1 e_2, \quad \theta(e_4) = a_1 a_2 e_1;$$

soit d'autre part ψ la corrélation involutive (relative à l'automorphisme identique) telle que

$$\psi(e_1) = e'_4, \quad \psi(e_2) = -e'_3, \quad \psi(e_3) = e'_2, \quad \psi(e_4) = -e'_1.$$

On doit avoir $\psi \cdot v = \mu^{-1} \check{v} \cdot \psi$ et $\theta \cdot v = \lambda \cdot v \cdot \theta$, avec $\lambda \lambda^\sigma = 1$. On a $\theta^2(x) = a_1 a_2 x$ et $\psi \cdot \theta = -a_1 a_2 \check{\theta} \cdot \psi$. On voit comme au n° 25 que $a_1 a_2$ n'est pas de la forme $\lambda \lambda^\sigma$ pour $\lambda \in K_1$, car cela entraînerait que la forme $a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2$ serait d'indice > 0 sur K, contrairement à l'hypothèse. Appliquant la méthode générale (cf. n° 22, note 1), on considère l'extension quadratique L de K_1 ayant pour base 1 et ϱ, avec $\varrho^2 = a_1 a_2$ et $\zeta^\sigma = \varrho^{-1} \zeta \varrho$ pour $\zeta \in K_1$, et on prolonge σ en un anti-automorphisme $\xi \to \bar{\xi}$ de L en posant $\bar{\varrho} = -\varrho$. Si F est l'espace $F_1 = K_1^4$ considéré comme espace de dimension 2 sur L, la corrélation ψ correspond à la forme bilinéaire sur F

$$g(x, y) = \langle \psi(\theta(x)), y \rangle - \varrho \langle \psi(x), y \rangle$$

qui, par rapport à la base de F formée de e_1 et e_2, s'écrit $g(x, y) = -\bar{\xi}_1 \eta_1 + a_2 \bar{\xi}_2 \eta_2$. Le corps L est d'ailleurs un corps de quaternions généralisé sur K correspondant au couple $(-a_4/a_1, a_1 a_2)$, et g est une forme *d'indice* 0 sur F: en effet, dans le cas contraire, il existerait $\zeta = \alpha + \omega\beta + \varrho(\gamma + \omega\delta)$ dans L ($\alpha, \beta, \gamma, \delta$ dans K) tel que $a_2 = \bar{\zeta}\zeta$; compte tenu de l'hypothèse $a_2 a_4 = a_1 a_5$, cela s'écrit

$$a_2^2 + a_2^2(a_1 \gamma^2 + a_4 \delta^2) - a_2 \alpha^2 - a_5 \beta^2 = 0$$

ce qui est contraire à l'hypothèse $\nu = 0$. Cela étant, si on détermine $\beta \in K_1$ tel que $\beta^{1-\sigma} = \lambda$, $w = \beta v$ est une transformation linéaire de F telle que $\psi \cdot w = \alpha \cdot \check{w} \cdot \psi$ avec $\alpha = \mu^{-1} \beta^2$, et on a $u = \alpha^{-1} \cdot w^{(2)}$. On voit donc que *$O_5^+(K, f)$ est isomorphe au quotient par K^* du groupe $GU_2(L, g)$.*

40. *Cas IV d: $n = 5$, $\nu = 0$, il n'existe pas d'extension quadratique de K par rapport à laquelle f soit d'indice* 2. Soient ω et ω' des racines de $a_1 X^2 + a_4$ et $a_2 X^2 + a_5$ respectivement, et soit $K_1 = K(\omega, \omega')$; l'espace E_1 obtenu à partir de E par extension à K_1 du corps des scalaires, est considéré comme le sous-espace $\xi_6 = 0$

d'un espace E_1' de dimension 6 sur K_1, et la forme f comme la restriction à E de la forme f' sur E_1', telle que

$$f'(x, x) = a_1(\xi_1 + \omega\xi_4)(\xi_1 - \omega\xi_4) - a_2(\xi_2 + \omega'\xi_5)(\xi_2 - \omega'\xi_5) + \xi_3^2 - \xi_6^2.$$

Alors $O_5^+(K, f)$ est isomorphe au sous-groupe de $GO_6^+(K, f)$ qui laisse invariant $\eta_3 - \eta_6$ et permute aux deux transformations semi-linéaires (58) (n° 31). Toute transformation de ce sous-groupe est de la forme $u = \mu \cdot v^{(2)}$, où $v \in GL_4(K_1)$ est assujettie aux conditions suivantes. Soient ψ, ψ_1, ψ_2 les trois corrélations involutives définies par

$$\begin{array}{llll} \psi(e_1) = e_4', & \psi(e_2) = -e_3', & \psi(e_3) = e_2', & \psi(e_4) = -e_1' \\ \psi_1(e_1) = e_2', & \psi_1(e_2) = -e_1', & \psi_1(e_3) = -a_1 e_4', & \psi_1(e_4) = a_1 e_3' \\ \psi_2(e_1) = e_3', & \psi_2(e_2) = -a_2 e_4', & \psi_2(e_3) = -e_1', & \psi_2(e_4) = a_2 e_2' \end{array}$$

relatives respectivement à l'automorphisme identique et aux automorphismes σ et τ qui laissent respectivement invariant ω' et ω. On doit alors avoir $\psi \cdot v = \mu^{-1} \cdot \check{v} \cdot \psi$, $\psi_1 \cdot v = \lambda_1 \check{v} \cdot \psi_1$, $\psi_2 \cdot v = \lambda_2 \cdot \check{v} \cdot \psi_2$, avec $\Delta = \mu^{\sigma-1}\lambda_1^2 = \mu^{\tau-1}\lambda_2^2$, où $\Delta = \det v$. Posons $\theta_1 = \psi^{-1} \cdot \psi_1$ et $\theta_2 = -\psi^{-1} \cdot \psi_2$; ce sont des collinéations involutives relatives à σ et τ respectivement et telles que

$$\begin{array}{llll} \theta_1(e_1) = e_3, & \theta_1(e_2) = e_4, & \theta_1(e_3) = -a_1 e_1, & \theta_1(e_4) = -a_1 e_2 \\ \theta_2(e_1) = e_2, & \theta_2(e_2) = a_2 e_1, & \theta_2(e_3) = -e_4, & \theta_2(e_4) = -a_2 e_3. \end{array}$$

La transformation linéaire v doit permuter projectivement avec ψ, θ_1 et θ_2. On a $\theta_1^2(x) = -a_1 x$, $\theta_2^2(x) = a_2 x$, $\theta_1 \cdot \theta_2 = -\theta_2 \cdot \theta_1$, $\psi \cdot \theta_1 = -a_1 \check{\theta}_1 \cdot \psi$ et $\psi \cdot \theta_2 = a_2 \check{\theta}_2 \cdot \psi$. En premier lieu, $-a_1$ n'est pas de la forme $\lambda\lambda^\sigma$, où $\lambda \in K_1$; cela résulte aussitôt de ce que la forme quadratique $a_1\xi_1^2 + a_4\xi_4^2 + \xi_3^2$ est d'indice 0 sur K. On forme alors l'extension quadratique L_1 de K_1, ayant pour base 1 et ϱ_1, telle que $\varrho_1^2 = -a_1$, $\zeta^\sigma = \varrho_1^{-1}\zeta\varrho_1$ pour $\zeta \in K_1$; on prolonge σ en un antiautomorphisme $\xi \to \bar{\xi}$ de L_1 en posant $\bar{\varrho}_1 = \varrho_1$, et τ en un automorphisme de L_1 en posant $\varrho_1^\tau = -\varrho_1$. L'espace $F_1 = K_1^4$ devient un espace F_1' de dimension 2 sur L_1, ayant pour base e_1 et e_2; la corrélation ψ correspond à la corrélation ψ' de F_1', relative à l'antiautomorphisme $\xi \to \bar{\xi}$, et telle que

$$\langle \psi'(x), y \rangle = \langle \psi(\theta_1(x)), y \rangle + \varrho_1 \langle \psi(x), y \rangle.$$

La collinéation θ_2 devient une collinéation de F_1' relative à l'automorphisme τ, telle que $\psi' \cdot \theta_2 = -a_2 \cdot \check{\theta}_2 \cdot \psi'$. Si on a $\theta_1 \cdot v = \lambda_1 \cdot v \cdot \theta_1$ avec $\lambda_1 \lambda_1^\sigma = 1$, on détermine $\beta_1 \in K_1$ tel que $\beta_1^{1-\sigma} = \lambda_1$; alors $w_1 = \beta_1 v$ est une application linéaire de F_1' sur lui-même; en posant $\mu_1 = \mu \beta_1^{-2}$, on a $u = \mu_1 \cdot w_1^{(2)}$ et $\psi' \cdot w_1 = \mu_1^{-1} \cdot \check{w}_1 \cdot \psi'$; en outre, w_1 doit permuter projectivement avec θ_2.

Montrons ensuite que a_2 n'est pas de la forme $\lambda \lambda^\tau$, avec $\lambda \in L_1$. Pour cela, on raisonne comme au n° 34, et on voit ainsi que si a_2 était de cette forme, il existerait des éléments ξ_k $(1 \leq k \leq 6)$ de K non tous nuls tels que

$$f''(x, x) = a_1 \xi_1^2 + a_4 \xi_4^2 - a_2 \xi_2^2 - a_5 \xi_5^2 + \xi_3^2 - \frac{a_4 a_5}{a_1 a_2} \xi_6^2 = 0.$$

Comme le discriminant d de f'' est tel que $-d$ soit un carré, et que par ailleurs f'' n'est pas d'indice 3 ou 2 (sans quoi un sous-espace totalement isotrope de dimension 3 ou 2 couperait l'hyperplan $\xi_6 = 0$ suivant un sous-espace non réduit à 0, contrairement à l'hypothèse $\nu = 0$ pour f), f'' est nécessairement d'indice 1, et rentre donc dans le cas III c (n° 30): Mais alors, il existerait une extension quadratique $K(\sqrt{-d})$ de K dans laquelle f'' serait d'indice 3, et comme un sous-espace totalement isotrope de dimension 3 rencontre alors $\xi_6 = 0$ suivant un sous-espace de dimension ≥ 2, la forme f serait d'indice 2 sur $K(\sqrt{-d})$, contrairement à l'hypothèse.

On peut alors former l'extension quadratique L de L_1, ayant pour base 1 et ϱ_2, avec $\varrho_2^2 = a_2$, et $\zeta^\tau = \varrho_2^{-1} \zeta \varrho_2$ pour $\zeta \in L_1$; l'espace F_1' s'identifie au corps L, en identifiant e_1 à l'élément unité. On prolonge l'antiautomorphisme $\xi \to \bar{\xi}$ à L en posant $\bar{\varrho}_2 = -\varrho_2$; la corrélation ψ' correspond alors à la forme bilinéaire sur L

$$g(x, y) = -a_2^{-1} \bar{x} \varrho_2 y$$

telle que $g(y, x) = -\overline{g(x, y)}$. Si $\theta_2 \cdot w_1 = \lambda_2 \cdot \check{w}_1 \cdot \theta_2$, avec $\lambda_2 \in K_1$ et $\lambda_2 \lambda_2^\tau = 1$, on détermine $\beta_2 \in K_1$ tel que $\beta_2^{1-\tau} = \lambda_2$; alors $w = \beta_2 w_1$ devient une *homothétie* à gauche du corps L, qui doit permuter projectivement avec la corrélation involutive correspondant à g; en outre on a $\psi \cdot w = \alpha \cdot \check{w} \cdot \psi$, avec $\alpha = \mu_1^{-1} \beta_2^2$, et $u = \alpha^{-1} w^{(2)}$. On voit donc que *$O_6^+(K, f)$ est isomorphe au quotient par K^* du groupe $GU_1(L, g)$.*

Les éléments 1, ϱ_1, ϱ_2 et $\varrho_1 \varrho_2$ forment une base de L sur K_1, telle que $\varrho_1^2 = -a_1$, $\varrho_2^2 = a_2$ et $\varrho_2 \varrho_1 = -\varrho_1 \varrho_2$; le sous-corps L' ayant pour base ces éléments sur K est donc un corps de quaternions généralisé sur K, correspondant au couple $(-a_1, a_2)$; le sous-corps commutant L'' de L' dans L a pour base 1, $\varrho_1 \omega'$, $\varrho_2 \omega$ et $\varrho_1 \omega' \varrho_2 \omega$ sur K; c'est un corps de quaternions généralisé correspondant au couple $(a_1 a_2 a_5, -a_1 a_2 a_4)$: le corps L est donc *le produit tensoriel $L' \otimes L''$ de deux corps de quaternions généralisés sur K.*[1]

[1] Voir note 1 du n° 34.

Remarquons pour terminer cette partie que la méthode de «descente» que nous avons appliquée pour passer de $n = 6$ à $n = 5$ et de $n = 4$ à $n = 3$ pourrait aussi être utilisée pour passer de $n = 5$ à $n = 4$, et redonnerait ainsi les résultats relatifs à ce dernier cas (n$^{\text{os}}$ 24 à 26). Enfin, il n'existe *aucun* autre isomorphisme, valable pour un corps *quelconque* K de caractéristique $\neq 2$, entre les groupes $G O_n^+(K, f)$ et d'autres types de groupes classiques dont une suite de composition contiendrait comme groupe quotient un groupe de l'une des formes PSL_m, PSp_m, $P\Omega_m$ (pour $m \neq n$) ou PU_m^+; en effet, en spécialisant le corps K en un corps *fini*, le groupe simple $P\Omega_n(K, f)$ serait isomorphe à un des groupes de l'une des formes précédentes, et j'ai démontré ailleurs [10, p. 71–75 et 92] qu'un tel isomorphisme n'existe pas pour un corps fini quelconque.

IV. Involutions de seconde espèce dans les groupes unitaires projectifs.

41. Nous allons maintenant appliquer la méthode générale de la II$^{\text{e}}$ partie pour déterminer les involutions de seconde espèce et leurs centralisateurs dans les groupes unitaires projectifs $PU_n(K, f)$, où K est un corps infini de caractéristique $\neq 2$, commutatif ou non, et f une forme hermitienne sur un espace vectoriel à droite E de dimension $n > 1$ sur K, relative à un antiautomorphisme involutif $\xi \to \bar{\xi}$ de K, distinct de l'identité. Une *involution de seconde espèce* $\bar{u}$ dans le groupe unitaire projectif $PU_n(K, f) = U_n(K, f)/Z_n$ (Z_n centre de U_n, formé des homothéties $x \to x\beta$, où β appartient au centre Z de K et est tel que $\bar{\beta}\beta = 1$) est l'image d'une transformation $u \in U_n(K, f)$ telle que $u^2(x) = x\gamma$ avec $\gamma \in Z$, et telle que $\bar{u}$ ne soit pas l'image d'une involution de U_n (c'est-à-dire une transformation $v \in U_n$ telle que $v^2(x) = x$). Nous allons distinguer plusieurs cas.

A) $\gamma = \alpha^2$, *où α appartient au centre Z de K.* Comme $\bar{\gamma}\gamma = 1$, on a ici $(\bar{\alpha}\alpha)^2 = 1$, et par suite $\bar{\alpha}\alpha = 1$ ou $\bar{\alpha}\alpha = -1$. Le cas $\bar{\alpha}\alpha = 1$ est à écarter, car alors $v = u\alpha^{-1}$ appartient à U_n, et est une involution de U_n, dont l'image canonique dans PU_n est $\bar{u}$; $\bar{u}$ ne serait donc pas de seconde espèce. Examinons le cas où $\bar{\alpha}\alpha = -1$, et posons $v = u\alpha^{-1}$; on a encore $v^2(x) = x$, mais cette fois v n'appartient plus au groupe U_n. De façon précise, on a $f(v(x), v(y)) = -f(x, y)$ identiquement; soient V et W les sous-espaces supplémentaires de E dans lesquels on a respectivement $v(x) = x$ et $v(x) = -x$; si x et y sont tous deux dans V, on a nécessairement $f(x, y) = 0$, ce qui signifie que V et W sont *totalement isotropes*. Cela n'est possible que si $n = 2m$ est pair, et si la forme est d'indice maximum m. Inversement, si V et W sont deux sous-espaces totalement isotropes supplémentaires dans E, v la transformation égale à x dans V, à $-x$ dans W, et si α est un élément de Z tel que $\bar{\alpha}\alpha = -1$, $u = v\alpha$ appartient à U_n et $\tilde{u}$ est une involution de seconde espèce dans PU_n. En outre, on peut prendre dans V une base $(e_i)_{1\le i\le m}$ et dans W une base $(e_{m+i})_{1\le i\le m}$ telles que $f(e_i, e_{m+j}) = \delta_{ij}$; le centralisateur de u dans U_n est alors formé des transformations dont la matrice par rapport à la base $(e_i)_{1\le i\le n}$ est de la forme $\begin{pmatrix} A & 0 \\ 0 & \check{\bar{A}} \end{pmatrix}$, où A est une matrice carrée inversible arbitraire d'ordre m, à éléments dans K, et $\check{\bar{A}}$ la contragrédiente de sa transformée par $\xi \to \bar{\xi}$. Le centralisateur de u est donc *isomorphe à* $GL_m(K)$.

B) γ *n'est pas un carré dans* K. Si ψ est la corrélation involutive de E telle que $f(x, y) = \langle\psi(x), y\rangle$, on a alors $\psi\cdot u = \check{u}\cdot\psi$; comme u est linéaire et que γ n'est pas un carré, on est dans les conditions d'application de la méthode de la II[e] partie. On forme l'extension quadratique L de K, produit tensoriel (sur Z) de K et de $Z(\varrho)$, où $\varrho^2 = \gamma$; et on prolonge l'antiautomorphisme $\xi \to \bar{\xi}$ de K en un antiautomorphisme de L en posant $\bar{\varrho} = \varrho\gamma^{-1}$ (n° 19). La dimension n de E sur K est alors nécessairement un nombre pair $2m$, et E devient un espace E' de dimension m sur L; la corrélation ψ correspond alors à la forme hermitienne $g(x, y) = \langle\psi(x), y\rangle + \varrho\langle\psi(u(x)), y\rangle$ sur E', et le centralisateur de u dans U_n n'est autre que le *groupe unitaire* $U_m(L, g)$.

C) $\gamma = \alpha^2$, *où* α *n'appartient pas au centre de* K. Posons encore $v(x) = u(x)\alpha^{-1}$; on a $v^2(x) = x$, et v est une application semi-linéaire de E sur lui-même, relative à l'automorphisme $\xi \to \xi^\tau = \alpha\xi\alpha^{-1}$ de K. Cet automorphisme est involutif; en outre, on a $f(v(x), v(y)) = h(f(x, y))^\tau$, où $h = (\alpha\bar{\alpha})^{-1}$. Comme ici $1 = \lambda\lambda^\tau$, avec $\lambda = 1$, on est dans les conditions d'application de la méthode du n° 21. Soit donc M le sous-corps de K formé des invariants de τ; K est un espace vectoriel de dimension 2 sur M (à gauche et à droite), admettant par rapport à M une base formée de 1 et d'un élément θ tel que $\theta^\tau = -\theta$. Soit E_1 l'espace vectoriel de dimension $2n$ sur M, obtenu en restreignant à M le corps des scalaires de E; v est alors une involution dans $GL_{2n}(M)$, et E_1 est somme directe des deux sous-espaces V et W tels que $v(x) = x$ dans V et $v(x) = -x$ dans W; en outre, on a $W = V\theta$, V est de dimension n sur M, et une base de V sur M est aussi une base de E sur K.

Cela étant, supposons d'abord qu'il existe $r \in K$ tel que $\bar{r} = r$ et $h^{-1}r = r^\tau$; si on pose $\xi^\varpi = r^{-1}\bar{\xi^\tau}r$, ϖ est un antiautomorphisme involutif de K, permutable avec τ; remplaçant $f(x, y)$ par la forme $g(x, y) = r^{-1}f(x, y)$, on voit que l'on a identiquement $g(v(x), v(y)) = (g(x, y))^\tau$; en outre, *dans* V, $g(x, y)$ a ses valeurs dans le corps M, et on a $g(y, x) = (g(x, y))^\varpi$. Si une transformation linéaire w de E permute avec u, elle permute aussi avec v; comme on peut considérer w comme une transformation linéaire dans E_1, w laisse invariants les sous-espaces V et W, et est entièrement déterminée par sa restriction à V. Si en outre w appartient au groupe $U_n(K, f)$ on a $g(w(x), w(y)) = g(x, y)$ quels que soient x et y dans V et réciproquement. On voit donc que le centralisateur de u dans $U_n(K, f)$ est isomorphe au *groupe unitaire* $U_n(M, g)$.

Supposons ensuite qu'il n'existe aucun élément r ayant les propriétés précédentes; on a vu au n° 22 que cela ne peut se produire que si $h = -1$ et si M est *commutatif*, $\bar{\theta} = -\theta$ et $\bar{\zeta} = \theta \zeta \theta^{-1}$ pour tout $\zeta \in M$. Si on pose alors $g(x, y) = f(x, y)\theta$, on a $g(v(x), v(y)) = (g(x, y))^{\tau}$, et *dans* V, g prend ses valeurs dans le corps M, et est telle que $g(y, x) = -g(x, y)$, autrement dit, est une forme *alternée*. On observera que cela n'est possible que si $n = 2m$ est pair, et en outre, comme une base symplectique (pour g) de V est aussi une base de E, la forme f est nécessairement d'indice (maximum) m. Le même raisonnement que ci-dessus montre alors que le centralisateur de u dans $U_n(K, f)$ est ici *isomorphe au groupe symplectique* $Sp_n(M, g)$.

42. Ce qui précède détermine le centralisateur G *dans* $U_n(K, f)$ de la transformation u. Le centralisateur *dans* $PU_n(K, f)$ de l'involution de seconde espèce $\tilde{u}$ est formé des images des transformations w de $U_n(K, f)$ telles que $wu = \beta uw$, où $\beta \in Z$; mais cela entraîne $wu^2 = \beta^2 u^2 w$, et comme u^2 appartient au centre, $\beta^2 = 1$. Le centralisateur de $\tilde{u}$ dans PU_n est donc l'image du groupe G' formé des transformations unitaires w telles que $wu = \pm uw$; il est clair que le produit de deux quelconques de ces transformations est permutable avec u; en d'autres termes, G est un sous-groupe (distingué) d'indice 2 dans G'.

APPENDICE.

Compléments et corrections à mon article «Sur les systèmes maximaux d'involutions conjuguées et permutables dans les groupes projectifs» [9].

43. Je me propose dans ce qui suit de revenir sur certains points de l'article précité, où les démonstrations sont insuffisantes ou contiennent des inexactitudes.[1]

Nous étudierons d'abord le cas D) du n° 6 [9, p. 20–26]. Considérons en premier lieu les valeurs de m distinctes de 2, 4 et 8 (cette dernière valeur ne nécessitant un traitement spécial que dans le cas D 3)).

[1] Je signale en outre dans cet article les fautes d'impression suivantes: page 15, ligne 19 du bas, lire w au lieu de W; même page, ligne 15 du bas, lire $u_k u = -u u_k$; page 18, ligne 15 du bas, lire $B_4(K'_0)$; page 20, ligne 14 du bas, lire $u_8(e_4)$; page 28, ligne 17 du bas, lire $u_0(uv) = -\varepsilon(uv)u_0$.

Dans l'étude du cas D 2) [9, p. 22] pour $m \neq 2$ et $m \neq 4$, il n'est pas exclu (contrairement à ce qui est affirmé ligne 19–20 de la p. 22) que u_0 soit permutable avec tous les éléments v d'un système maximal T de 2^{m+1} éléments, lorsque K_0 contient un corps de quaternions. Mais on a alors $b = b' = 2^{m-1}$ et $c'' = 0$, donc $b + b' + c'' = 2^m$, et par suite on a bien $D_{2m}(K, \gamma) = 3.2^{m-1}$ dans le cas envisagé.

Dans l'étude du cas D 3) pour les valeurs de m distinctes de 2, 4 et 8, il faut au préalable exclure le cas où T aurait 2^{m+1} éléments (ce qui n'est pas fait dans [9], p. 23, lignes 9–10 du bas). Mais dans ce cas, on voit comme au début du cas D 2) qu'on devrait avoir $u_0(e_i) = e_i \lambda_i$ pour tout indice i. Les hypothèses montrent alors que u_0 est nécessairement permutable à tous les éléments de T, donc que $b = b' = 2^{m-1}$ et $c'' = 0$, d'où $b + b' + c'' = 2^m$. Le reste de la démonstration est alors inchangé; on notera simplement que le fait qu'il est impossible que toutes les transformations de T permutent avec v_1 résulte de ce que la relation $v_1 w = w v_1$ entraîne $(v_1 w)^2 = -w^2$.

44. Abordons maintenant l'étude des cas $m = 2$, $m = 4$ et $m = 8$ (dans le cas D)); leur examen dans [9] n'est pas complet, est souvent insuffisamment développé et contient des assertions inexactes; nous allons le reprendre complètement et nous verrons qu'il faut alors faire la division du cas D) en plusieurs cas d'une tout autre façon que pour les autres valeurs de m.

Nous distinguerons d'abord deux possibilités, suivant que K_0 contient ou ne contient pas de corps de quaternions sur son centre.

D') *K_0 contient un corps de quaternions sur son centre;* autrement dit, il existe dans K_0 deux éléments α, β tels que $\alpha^2 = \beta^2 = -1$ et $\beta\alpha = -\alpha\beta$. Un système maximal T de 16 éléments comprend alors 6 involutions qui engendrent T, à savoir celles définies par

$$\begin{array}{ll}
u_1(e_1) = e_1 & u_1(e_2) = e_2 \\
u_2(e_1) = e_1 & u_2(e_2) = -e_2 \\
u_3(e_1) = e_2 & u_3(e_2) = e_1 \\
u_4(e_1) = e_2\alpha & u_4(e_2) = -e_1\alpha \\
u_5(e_1) = e_2\beta & u_5(e_2) = -e_1\beta \\
u_6(e_1) = e_2\alpha\beta & u_6(e_2) = -e_1\alpha\beta.
\end{array}$$

Si u_0 est telle que $u_0 v = \pm v u_0$ pour tous les éléments $v \in T$, il y a deux possibilités: ou bien $u_0(e_1) = e_2\lambda$, $u_0(e_2) = e_1\mu$; dans ce cas on doit avoir $\lambda\mu^\sigma = -1$ et $\mu = \pm\lambda$. Ou bien $u_0(e_1) = e_1\lambda$, $u_0(e_2) = e_2\mu$; il faut alors $\lambda\lambda^\sigma = \mu\mu^\sigma = -1$.

On notera en outre qu'on a la relation $u_3 u_2 u_4 u_5 u_6 = -1$, si bien que 5 quelconques des involutions de T engendrent déjà T tout entier; si u_0 est permutable avec 5 involutions de T, il l'est donc avec tous les éléments de T, autrement dit on a alors $b + b' + c'' = 12$. Nous distinguerons les cas suivants:

D′ 1) *Il existe un élément $\mu \in K_0$ satisfaisant à l'une des deux conditions suivantes:*

a) $\mu \mu^\sigma = 1$, $\alpha \mu = \mu \alpha^\sigma$ *et* $\beta \mu = \mu \beta^\sigma$.

b) $\mu \mu^\sigma = -1$, $\alpha \mu = -\mu \alpha^\sigma$ *et* $\beta \mu = -\mu \beta^\sigma$.

On notera que chacune de ces deux conditions peut être satisfaite lorsque K contient lui-même un corps de quaternions.

On peut alors former une transformation u_0 qui permute avec 4 des involutions de T: on prendra $u_0(e_1) = e_2 \mu$, $u_0(e_2) = -e_1 \mu$ dans le cas a), et $u_0(e_1) = e_1 \mu$, $u_0(e_2) = e_2 \mu$ (ou $u_0(e_1) = e_2 \mu$, $u_0(e_2) = e_1 \mu$) dans le cas b). On a alors $b + b' + b'' = 2b' + 8 = 16$, et la remarque ci-dessus montre que dans tout autre cas on aurait $b + b' + c'' \leq 16$; d'où $D_4(K, \gamma) = 16$.

D′ 2) *Les hypothèses de D′ 1) ne sont pas remplies mais il existe un élément $\mu \in K_0$ satisfaisant à l'une des deux conditions suivantes:*

a) $\mu \mu^\sigma = 1$, $\alpha \mu = -\mu \alpha^\sigma$ *et* $\beta \mu = -\mu \beta^\sigma$.

b) $\mu \mu^\sigma = -1$, $\alpha \mu = \mu \alpha^\sigma$ *et* $\beta \mu = \mu \beta^\sigma$.

Dans le cas a), on peut prendre u_0 permutant avec 2 involutions de T, et anticommutant avec les autres, en posant $u_0(e_1) = e_2 \mu$, $u_0(e_2) = -e_1 \mu$. Dans le cas b), on a une transformation u_0 ayant les mêmes propriétés en posant $u_0(e_1) = e_2 \mu$ et $u_0(e_2) = e_1 \mu$; on obtient une transformation u_0 qui permute avec tous les éléments de T en prenant $u_0(e_1) = e_1 \mu$ et $u_0(e_2) = e_2 \mu$. Dans tous ces cas, on a $b + b' + c'' = 12$, et en raison des hypothèses faites, on vérifie facilement que ces trois cas sont les seuls possibles. D'autre part, si on considère un système T de 8 éléments, il ne peut comprendre que 4 involutions au plus; si une transformation u_0 permute avec toutes les transformations d'un tel système, on a $b + b' + c'' = b + b' \leq 8$; si elle permute avec la moitié des transformations de T, on a $b + b' + c'' = 2b' + 4 \leq 12$. On voit donc qu'on a $D_4(K, \gamma) = 12$ dans le cas D′ 2).

45. Lorsque les hypothèses de D′ 1) ou D′ 2) ne sont pas vérifiées, il n'existe pas de transformation semi-linéaire u_0 de carré -1 et telle que $u_0 v = \pm v u_0$ pour tous les éléments d'un système maximal T de 16 éléments; il faut donc considérer les systèmes T de 8 éléments. Montrons que, dans un tel système, il y a *exactement* 4

involutions. Nous avons déjà vu qu'il ne peut y en avoir plus de 4. Soit $v_0 \in T$ telle que $v_0^2 = -1$; pour tout $w \in T$ permutant avec v_0, on a $(v_0 w)^2 = -w^2$; soit H l'ensemble des éléments de T permutant avec v_0; si $H = T$, il y a donc exactement la moitié des éléments de T qui sont des involutions. Dans le cas contraire, H a 4 éléments, et l'image $\bar{H}$ de H dans $PGL_2(K_0)$ est un sous-groupe de $\bar{T}$. Soit H' e complémentaire de H dans T; si H' ne contient aucune involution, et si $w_0 \in H'$, tous les éléments de H' sont de la forme $w_0 w$, où w parcourt H, et l'hypothèse $(w_0 w)^2 = -1$ entraîne $w_0 w = w w_0$; w_0 est donc permutable avec tous les éléments de T, et en remplaçant v_0 par w_0 dans le raisonnement précédent, on est ramené au cas $H = T$. Si maintenant $v_1 \in H'$ est une involution, il en est de même de $v_2 = v_0 v_1$. Comme d'autre part $w \to v_0 w$ est une application de H sur lui-même, il y a exactement 2 éléments de H qui sont des involutions, et en tout au moins 4 éléments de T. Notre assertion est donc démontrée.

On montre facilement (cf. [9], p. 4–5) que, par rapport à une base convenable, les 4 involutions d'un système T de 8 éléments sont nécessairement de la forme u_1, u_2, u_3, u_4. On est alors amené à distinguer les cas suivants:

D′ 3) *Aucune des hypothèses de* D′ 1), D′ 2) *n'est vérifiée, mais il existe un élément* $\mu \in K_0$ *satisfaisant aux relations* $\mu \mu^\sigma = -1$ *et* $\alpha \mu = -\mu \alpha^\sigma$.

On peut prendre alors, soit $u_0(e_1) = e_1 \mu$, $u_0(e_2) = e_2 \mu$, soit $u_0(e_1) = e_2 \mu$, $u_0(e_2) = e_1 \mu$; avec le premier choix, u_0 commute avec u_1, u_2, u_3 et anticommute avec u_4; avec le second, u_0 commute avec u_1, u_3, u_4 et anticommute avec u_2. Dans tous les cas, on a $b + b' + c'' = 2b' + 4 = 10$. Si u_0 commutait avec toutes les involutions de T, il commuterait avec tous les éléments de T, et on aurait $b + b' + c'' = 2b = 8$. On a donc $D_4(K, \gamma) = 10$ dans le cas envisagé.

D′ 4) *Aucune des hypothèses de* D′ 1), D′ 2), D′ 3) *n'est vérifiée, mais il existe un élément* $\mu \in K_0$ *satisfaisant à l'une des deux conditions suivantes:*

a) $\mu \mu^\sigma = -1$ *et* $\alpha \mu = \mu \alpha^\sigma$.

b) $\mu \mu^\sigma = 1$ *et* $\alpha \mu = \mu \alpha^\sigma$.

Dans le cas a), on peut prendre, soit $u_0(e_1) = e_1 \mu$, $u_0(e_2) = e_2 \mu$, soit $u_0(e_1) = e_2 \mu$, $u_0(e_2) = e_1 \mu$; avec le premier choix, u_0 commute avec tous les éléments de T; avec le second, il commute avec u_1 et u_3 et anticommute avec u_2 et u_4. Dans le cas b), on prend $u_0(e_1) = e_2 \mu$, $u_0(e_2) = -e_1 \mu$; u_0 commute avec u_1 et u_4, anticommute avec u_2 et u_3. Dans tous les cas, $b + b' + c'' = 8$, et il est clair que ce nombre ne peut être dépassé, d'où $D_4(K, \gamma) = 8$.

D′ 5) *Aucune des hypothèses de* D′ 1), D′ 2), D′ 3), D′ 4) *n'est vérifiée.* Il n'existe pas alors de transformation u_0 commutant avec plus d'une involution d'un système T de 8 éléments et anticommutant avec les autres; pour un système T de 8 éléments, on a donc nécessairement $b + b' + c'' = 2b' + 4 = 6$. D'autre part, un système T de 4 éléments tel que $\bar{T}$ soit un sous-groupe de $PGL_2(K_0)$ ne peut comprendre que 3 involutions au plus, et si une transformation u_0 commute avec ces 3 involutions, elle commute avec le quatrième élément de T; on a donc $b + b' + c'' \leq 6$ pour un tel système. On voit ainsi que le nombre $b + b' + c''$ ne peut jamais dépasser 6 dans le cas que nous envisageons. Comme d'ailleurs, il y a 6 involutions dans un système maximal T de 16 éléments, on a bien ici $D_4(K, \gamma) = 6$ (cf. [9], p. 15–16).

46. Continuant l'étude du cas D) de [9], n° 6 pour $m = 2$, considérons maintenant le second cas, savoir

D″) K_0 *ne contient pas de corps de quaternions.*

Comme il existe par hypothèse un élément $\alpha \in K_0$ de carré -1, un système maximal T de 8 éléments comprend 4 involutions qui engendrent T, savoir (par rapport à une base convenable) les involutions u_1, u_2, u_3 et u_4 définies ci-dessus. On est alors amené à faire les distinctions suivantes:

D″ 1) *Il existe un élément* $\mu \in K_0$ *satisfaisant aux conditions* $\mu\mu^\sigma = -1$ *et* $\alpha\mu = -\mu\alpha^\sigma$.

Le raisonnement du cas D′ 3) s'applique sans modification, et on a donc $D_4(K, \gamma) = 10$.

D″ 2) *Les hypothèses de* D″ 1) *ne sont pas vérifiées, mais il existe un élément* $\mu \in K_0$ *satisfaisant à l'une des deux conditions suivantes:*

a) $\mu\mu^\sigma = -1$ *et* $\alpha\mu = \mu\alpha^\sigma$.

b) $\mu\mu^\sigma = 1$ *et* $\alpha\mu = \mu\alpha^\sigma$.

On raisonne ici comme dans les cas a) et b) de D′ 4), et on voit que $D_4(K, \gamma) = 8$.

D″ 3) *Aucune des hypothèses de* D″ 1) *et* D″ 2) *n'est vérifiée, mais il existe un élément* $\mu \in K_0$ *satisfaisant à l'une des deux conditions:*

a) $\mu\mu^\sigma = 1$ *et* $\alpha\mu = -\mu\alpha^\sigma$.

b) $\mu\mu^\sigma = -1$.

Il n'existe pas alors de transformation u_0 commutant avec plus d'une involution d'un système T de 8 éléments et anticommutant avec les autres. Dans le cas a), en prenant $u_0(e_1) = e_2\mu$, $u_0(e_2) = -e_1\mu$, u_0 commute avec u_1, anticommute avec u_2, u_3, u_4, d'où $b + b' + c'' = 6$. Dans le cas b), il n'existe pas de transformation u_0 de carré -1 telle que $u_0 v = \pm v u_0$ pour tous les éléments v d'un système T de 8 éléments. Il faut donc considérer les systèmes T de 4 éléments; comme un tel système ne comprend que 3 involutions au plus, on a alors $b + b' + c'' \leq 6$. Ce maximum est atteint dans le cas b) en considérant le système de 4 éléments engendré par u_1, u_2, u_3 et prenant $u_0(e_1) = e_1\mu$, $u_0(e_2) = e_2\mu$, ou $u_0(e_1) = e_2\mu$, $u_0(e_2) = e_1\mu$. On a donc $D_4(K, \gamma) = 6$.

D'' 4) *Aucune des hypothèses de* D'' 1), D'' 2), D'' 3) *n'est remplie.*

Comme il n'existe pas d'élément $\mu \in K_0$ tel que $\mu\mu^\sigma = -1$, aucune transformation semi-linéaire u_0 de carré -1 ne peut commuter avec une involution distincte de l'identité. Comme ici seuls les systèmes T de 4 éléments peuvent être envisagés (pour la recherche de u_0), on a $b + b' + c'' \leq 4$. Comme d'ailleurs un système T de 8 éléments a 4 involutions, on a nécessairement $D_4(K, \gamma) = 4$.

47. Nous abordons maintenant l'étude du cas D) de [9], n° 6, lorsque $m = 4$. Au préalable, nous allons montrer comment on peut déterminer le nombre d'involutions dans un système G de 2^r transformations linéaires de carré ± 1, tel que $\bar{G}$ soit un sous-groupe abélien de $PGL_4(K_0)$ (ici $r \leq 6$). Tout d'abord G ne peut se composer uniquement d'involutions que si $r \leq 2$, car ces involutions doivent alors être deux à deux permutables. Si $v_0 \in G$ est de carré -1, on a $(v_0 w)^2 = -w^2$ pour toute transformation $w \in G$ qui permute avec v_0. Cherchons d'abord s'il est possible que les transformations $v \in G$ de carré -1 permutent toutes avec tous les éléments de G, auquel cas, d'après ce qui précède, exactement la moitié des éléments de G sont des involutions. Alors, si w_1 et w_2 sont deux involutions de G, $v_0 w_1$ et $v_0 w_2$, qui sont des transformations de carré -1, doivent être permutables entre elles et avec v_0, ce qui entraîne que w_1 et w_2 sont permutables. Autrement dit, l'ensemble (à 2^{r-1} éléments) des involutions de G devrait être un groupe d'involutions, ce qui n'est possible que si $r \leq 3$. Si on n'est pas dans ce cas, on peut supposer que l'ensemble H des éléments de G permutables avec v_0 a 2^{r-1} éléments, et est tel que l'image $\bar{H}$ de H dans $PGL_4(K_0)$ soit un groupe. D'après la relation $(v_0 w)^2 = -w^2$, H contient donc 2^{r-2} involutions. Cherchons si le complémentaire H' de H dans G peut contenir uniquement des transformations de carré -1. Dans ce cas, si v_1 est une telle transformation et $w \in H$ une involution, comme $v_1 w \in H'$, on doit avoir $(v_1 w)^2 = -1$, ce qui entraîne $v_1 w = w v_1$; les éléments de H' devraient donc permuter avec toutes les involutions de H. Or, si w_1 et w_2 sont deux involutions de H, $v_1 w_2$

est dans H', et si w_1 permute avec v_1 et $v_1 w_2$, il permute aussi avec w_2; toutes les involutions de H devraient donc être permutables, ce qui n'est possible que si $r \leq 4$. Si on n'est pas dans ce cas, H' contient une involution v_1; alors $v_0 v_1 = - v_1 v_0$, et v_2 est par suite une seconde involution dans H' telle que $v_0 v_2 = - v_2 v_0$ et $v_1 v_2 = - v_2 v_1$. Soit alors L l'ensemble des $w \in H$ qui permutent avec v_1; comme v_0 ne permute pas avec v_1, l'image $\bar{L}$ de L dans $PGL_4(K_0)$ est un sous-groupe de $\bar{H}$ de 2^{r-2} éléments. Si L' est le complémentaire de L dans G, et si L contient h involutions, $H \cap L'$ en contient $2^{r-2} - h$, et H' en contient $2h$, savoir les éléments $v_1 w$ où w parcourt les h involutions de L, et les h éléments de carré -1 de $H \cap L'$. Finalement, on voit que G contient en tout $2^{r-2} + 2h$ involutions. En outre, les involutions $w \in L$ permutent avec les involutions v_1, v_2 telles que $v_1 v_2 = - v_2 v_1$; on est donc dans la situation de la p. 4, 1° de [9], et les restrictions des involutions w au sous-espace positif de v_1 sont distinctes. Comme ce sous-espace est de dimension 2 sur K_0, le nombre maximum de ces involutions est donc 6 si K_0 contient un corps de quaternions [9, p. 13, th. 3], et 4 dans le cas contraire [9, p. 14, th. 4]; dans le premier cas, le groupe engendré par les 6 involutions considérées contient 16 éléments [9, p. 13, th. 3], et comme il est contenu dans L, cela n'est possible que si $r = 6$ (auquel cas le nombre d'involutions de G est bien $28 = 2^4 + 12$). Pour $r = 5$, on ne peut non plus avoir $h = 5$, car les 5 involutions de L engendrent encore un groupe à 16 éléments; on a donc nécessairement au plus $2^3 + 8 = 16$ involutions dans G. Pour $r = 4$, on voit de même que G a au plus $2^2 + 6 = 10$ involutions.[1]

48. Nous considérons encore deux grands cas, suivant que K_0 contient ou non un corps de quaternions.

D') K_0 *contient un corps de quaternions sur son centre.* Un système maximal T a alors 64 éléments, dont 28 involutions, qui engendrent T, et peuvent s'écrire

$$\begin{array}{llll}
u_1(e_1) = e_1, & u_1(e_2) = e_2, & u_1(e_3) = e_3, & u_1(e_4) = e_4 \\
u_2(e_1) = e_1, & u_2(e_2) = e_2, & u_2(e_3) = -e_3, & u_2(e_4) = -e_4 \\
u_3(e_1) = e_1, & u_3(e_2) = -e_2, & u_3(e_3) = e_3, & u_3(e_4) = -e_4 \\
u_4(e_1) = e_1, & u_4(e_2) = -e_2, & u_4(e_3) = -e_3, & u_4(e_4) = e_4 \\
u_5(e_1) = e_2, & u_5(e_2) = e_1, & u_5(e_3) = e_4, & u_5(e_4) = e_3 \\
u_6(e_1) = e_3, & u_6(e_2) = e_4, & u_6(e_3) = e_1, & u_6(e_4) = e_2
\end{array}$$

[1] A la p. 10 de [9], on obtient un système G contenant 12 involutions, mais $\bar{G}$ n'est pas un groupe.

$$\begin{array}{llll}
u_7(e_1)=e_4, & u_7(e_2)=e_3, & u_7(e_3)=e_2, & u_7(e_4)=e_1\\
u_8(e_1)=e_2, & u_8(e_2)=e_1, & u_8(e_3)=-e_4, & u_8(e_4)=-e_3\\
u_9(e_1)=e_3, & u_9(e_2)=-e_4, & u_9(e_3)=e_1, & u_9(e_4)=-e_2\\
u_{10}(e_1)=e_4, & u_{10}(e_2)=-e_3, & u_{10}(e_3)=-e_2, & u_{10}(e_4)=e_1\\
u_{11}(e_1)=e_2\,\alpha, & u_{11}(e_2)=-e_1\,\alpha, & u_{11}(e_3)=e_4\,\alpha, & u_{11}(e_4)=-e_3\,\alpha\\
u_{12}(e_1)=e_2\,\alpha, & u_{12}(e_2)=-e_1\,\alpha, & u_{12}(e_3)=-e_4\,\alpha, & u_{12}(e_4)=e_3\,\alpha\\
u_{13}(e_1)=e_3\,\alpha, & u_{13}(e_2)=e_4\,\alpha, & u_{13}(e_3)=-e_1\,\alpha, & u_{13}(e_4)=-e_2\,\alpha\\
u_{14}(e_1)=e_3\,\alpha, & u_{14}(e_2)=-e_4\,\alpha, & u_{14}(e_3)=-e_1\,\alpha, & u_{14}(e_4)=e_2\,\alpha\\
u_{15}(e_1)=e_4\,\alpha, & u_{15}(e_2)=e_3\,\alpha, & u_{15}(e_3)=-e_2\,\alpha, & u_{15}(e_4)=-e_4\,\alpha\\
u_{16}(e_1)=e_4\,\alpha, & u_{16}(e_2)=-e_3\,\alpha, & u_{16}(e_3)=e_2\,\alpha, & u_{16}(e_4)=-e_1\,\alpha
\end{array}$$

les 12 dernières involutions s'obtenant à partir de $u_{11}, \ldots, u_{16}$ en remplaçant partout α par β ou $\alpha\beta$. On notera en outre les relations $u_2 u_3 = u_4$, $u_5 u_6 = u_7$, $u_8 = u_2 u_5$, $u_9 = u_3 u_6$, $u_{10} = u_4 u_7$, $u_{12} = u_2 u_{11}$, $u_{14} = u_3 u_{13}$, $u_{16} = u_4 u_{15}$, $u_6 u_{11} = u_{16}$ et $u_{10} u_{11} = -u_{13}$. Si une transformation u_0 est telle que $u_0 v = \pm v u_0$ pour toutes les transformations $v \in T$, ou bien u_0 permute avec u_2, u_3, u_4, ou bien u_0 permute avec une de ces trois involutions, et anticommute avec les deux autres. Dans le premier cas, on a $u_0(e_i) = e_i \lambda_i$ $(1 \leq i \leq 4)$ avec $\lambda_i \lambda_i^{\sigma} = -1$; dans le second, on peut par exemple supposer que $u_0(e_1) = e_2 \lambda$, $u_0(e_2) = e_1 \mu$, $u_0(e_3) = e_4 \lambda'$, $u_0(e_4) = e_3 \mu'$, avec $\lambda \mu^{\sigma} = \lambda' \mu'^{\sigma} = -1$. En examinant les produits de u_0 avec les transformations engendrant T, on obtient aisément la classification suivante (les notations restant celles du n° 44):

D′ 1) Dans le cas a) on peut prendre $u_0(e_1) = e_2 \mu$, $u_0(e_2) = -e_1 \mu$, $u_0(e_3) = e_4 \mu$, $u_0(e_4) = -e_3 \mu$; u_0 commute avec les involutions $u_1, u_2, u_6, u_{10}, u_{11}, u_{12}, u_{13}, u_{16}$ et les 8 analogues de ces quatre dernières involutions (où α est remplacé par β et $\alpha\beta$ respectivement). On a alors $b' = 16$, d'où $b + b' + c'' = 2b' + 32 = 64$. Dans le cas b), on peut prendre $u_0(e_i) = e_i \mu$ pour $1 \leq i \leq 4$; u_0 commute alors avec les u_i d'indice tel que $1 \leq i \leq 10$ et avec les analogues de $u_{11}, \ldots, u_{16}$, où α est remplacé par $\alpha\beta$; on a encore $b' = 16$ et $b + b' + c'' = 2b' + 32 = 64$. Comme, d'après le résultat du n° 47 ci-dessus, le raisonnement de [9, n° 6, p. 21–22] prouve que u_0 ne peut permuter avec plus de 16 involutions du système T à moins qu'il ne permute avec toutes, on a $D_8(K, \gamma) = 64$ dans le cas que nous envisageons.

D′ 2) Dans le cas a), on prend $u_0(e_1) = e_2 \mu$, $u_0(e_2) = -e_1 \mu$, $u_0(e_3) = e_4 \mu$, $u_0(e_4) = -e_3 \mu$; u_0 commute alors avec $u_1, u_2, u_6, u_{10}, u_{14}, u_{15}$, les analogues de u_{14}, u_{15} où α est remplacé par β, et les analogues de $u_{11}, u_{12}, u_{13}, u_{16}$ où α est remplacé par $\alpha\beta$; elle anticommute avec les autres involutions de T, et par suite on a $b' = 12$

et $b + b' + c'' = 2b' + 32 = 56$. Dans le cas b), ou on prend $u_0(e_i) = e_i \mu$ pour $1 \leq i \leq 4$, et alors u_0 commute avec tous les éléments de T, d'où $b + b' + c'' = 2b = 56$; ou on prend $u_0(e_1) = e_2\mu$, $u_0(e_2) = e_1\mu$, $u_0(e_3) = e_4\mu$, $u_0(e_4) = e_3\mu$, et alors u_0 commute avec $u_1, u_2, u_5, u_6, u_7, u_8, u_{13}, u_{16}$ et les analogues de u_{13} et u_{16}, où α est remplacé par β ou $\alpha\beta$; d'où $b + b' + c'' = 2b' + 32 = 56$. Dans tous les cas, on a donc $D_8(K, \gamma) = 56$.

D′ 3) Il n'existe pas alors de transformation semi-linéaire u_0 de carré -1 telle que $u_0 v = \pm v u_0$ pour tous les éléments v d'un système maximal T de 64 éléments; il faut donc considérer les systèmes T de 32 éléments. Un tel système a au plus 16 involutions (n° 47); comme en outre il est engendré par ses involutions, si u_0 commute avec toutes les involutions de T, on a $b + b' + c'' = 2b \leq 32$. Si au contraire u_0 ne permute pas avec tous les éléments de T, il permute avec 16 éléments de T, formant un système H tel que $\bar{H}$ soit un sous-groupe de $PGL_4(K_0)$; on a vu au n° 47 que H contient au plus 10 involutions, d'où $b + b' + c'' = 2b' + 16 \leq 36$. Montrons que dans le cas D′ 3), ce dernier nombre peut être atteint; en effet, un système T de 32 éléments est obtenu en considérant le système engendré par les involutions u_1 telles que $1 \leq i \leq 16$; en outre, en prenant $u_0(e_i) = e_i\mu$ pour $1 \leq i \leq 4$, on voit que u_0 commute avec les u_i tels que $1 \leq i \leq 10$. On a donc ici $D_8(K, \gamma) = 36$.

D′ 4) Avec les notations du n° 47, pour $r = 5$, un système L de 8 éléments est tel que les restrictions de ses éléments au sous-espace positif de v_1 forment un système dont les images dans $PGL_2(K_0)$ constituent un groupe; d'après ce qu'on a vu au n° 45, L contient nécessairement 4 involutions, donc T en contient exactement 16; en outre, les constructions des n^{os} 45 et 47 montrent aisément que T peut (pour une base convenable) être considéré comme le système engendré par les involutions u_i $(1 \leq i \leq 16)$ ci-dessus. Si on prend alors dans le cas a), $u_0(e_i) = e_i\mu$ pour $1 \leq i \leq 4$, u_0 commute avec tous les u_k d'où $b + b' + c'' = 2b = 32$; si, dans ce même cas, on prend $u_0(e_1) = e_2\mu$, $u_0(e_2) = e_1\mu$, $u_0(e_3) = e_4\mu$, $u_0(e_4) = e_3\mu$, u_0 commute avec $u_1, u_2, u_5, u_6, u_7, u_8, u_{13}, u_{16}$ et anticommute avec les autres u_k, d'où $b + b' + c'' = 2b' + 16 = 32$. De même, dans le cas b), si on prend $u_0(e_1) = e_2\mu$, $u_0(e_2) = -e_1\mu$, $u_0(e_3) = e_4\mu$, $u_0(e_4) = -e_3\mu$, u_0 commute avec $u_1, u_2, u_6, u_{10}, u_{11}, u_{12}, u_{13}, u_{16}$, et anticommute avec les autres u_k, d'où encore $b + b' + c'' = 32$. Cela montre que u_0 ne peut commuter avec plus de 8 involutions de T s'il ne commute pas avec toutes, d'où $D_8(K, \gamma) = 32$.

D′ 5) Il n'existe pas alors de transformation semi-linéaire u_0 de carré -1 telle que $u_0 v = \pm v u_0$ pour tous les éléments v d'un système T de 32 éléments; il faut ici considérer les systèmes T de 16 éléments. Mais un tel système a au plus 10 involutions (n° 47), d'où $b + b' + c'' \leq 2b + 8 \leq 28$. Comme d'autre part un système maximal T de 64 éléments comporte 28 involutions, on a ici $D_8(K, \gamma) = 28$.

49. Considérons maintenant le cas

D″) K_0 *ne contient pas de corps de quaternions.* Un système maximal T a alors 32 éléments, dont 16 involutions qui engendrent T et peuvent s'écrire sous la forme u_k $(1 \leq k \leq 16)$ par rapport à une base convenable. En conservant les notations du n° 44, on a encore la classification suivante:

D″ 1) On raisonne comme dans le cas D′ 3), et on a donc $D_8(K, \gamma) = 36$.

D″ 2) Ici, on raisonne comme dans le cas D′ 4), et on a donc $D_8(K, \gamma) = 32$.

D″ 3) Dans le cas a), on prend $u_0(e_1) = e_2\mu$, $u_0(e_2) = -e_1\mu$, $u_0(e_3) = e_4\mu$, $u_0(e_4) = -e_3\mu$; u_0 commute avec $u_1, u_2, u_6, u_{10}, u_{14}, u_{15}$ et anticommute avec les autres u_k, d'où $b + b' + c'' = 2b' + 16 = 28$, et c'est la plus grande valeur que puisse prendre $b + b' + c''$ pour un système T de 32 éléments. Pour un système T de 16 éléments, a vu ci-dessus (dans l'examen du cas D′ 5)) qu'il y a au plus 10 involutions dans T et par suite que $b + b' + c'' \leq 28$. On a donc $D_8(K, \gamma) = 28$ dans le cas a). Dans le cas b), il n'y a pas de transformation semi-linéaire u_0 de carré -1, telle que $u_0 v = \pm v u_0$ pour tous les éléments d'un système T de 32 éléments; il faut donc considérer les systèmes T de 16 éléments. Si u_0 commute avec tous les éléments d'un tel système, comme il y a au plus 10 involutions dans T, on a $b + b' + c'' \leq 20$; si au contraire, u_0 ne commute qu'avec 8 éléments de T, l'ensemble H de ces éléments est tel que $\bar{H}$ soit un sous-groupe de $PGL_4(K_0)$, et il résulte du n° 47 que H contient au plus 6 involutions; d'où alors $b + b' + c'' = 2b' + 8 \leq 20$. Cette limite peut d'ailleurs être atteinte: il suffit en effet de considérer le système T de 16 éléments engendré par les 10 involutions u_k d'indice $1 \leq k \leq 10$, et de prendre $u_0(e_i) = e_i\mu$ pour $1 \leq i \leq 4$, u_0 commute alors avec tous les éléments de T. On a donc $D_8(K, \gamma) = 20$ dans le cas b).

D″ 4) Aucune transformation semi-linéaire u_0 de carré -1 ne peut alors commuter avec une involution distincte de l'identité. L'étude faite au n° 47 montre alors qu'il n'existe pas de telle transformation semi-linéaire telle que $u_0 v = \pm v u_0$ pour les éléments v d'un système T de 16 éléments. Mais pour un système T de 8 éléments, on a $b + b' + c'' \leq 16$. Comme d'autre part un système maximal T de 32 éléments contient 16 involutions, on a ici $D_8(K, \gamma) = 16$.

50. Il reste encore à examiner le cas D 3) de [9, p. 23] lorsque $m = 8$; avec les notations employées à l'endroit cité, l'ensemble $Q \cap R \cap S$ a alors 32 éléments, et les restrictions des transformations de cet ensemble au sous-espace W de dimen-

sion 4 les déterminent entièrement. Or, nous avons vu au n° 47 qu'un système de 32 transformations de carré ± 1, dont l'image dans $PGL_4(K_0)$ est un groupe, contient 16 involutions; on a donc $b' = 2^{m-3} + 2h = 2^{m-2}$ d'où $D_{16}(K, \gamma) = 2^8$.

51. Passons maintenant aux problèmes considérés au n° 7 de [9], et tout d'abord donnons quelques compléments pour les dimensions $n = 2$ et $n = 4$ dans les cas A) et B), qui sont traités un peu rapidement.

Dans le cas A), il faut vérifier que s'il n'existe pas dans K de couple d'éléments α, β tels que $\alpha^2 = \beta^2 = \gamma$ et $\alpha\beta = -\beta\alpha$, il est impossible de trouver une application linéaire u_0 de carré γ, telle que $u_0 u = -uu_0$, et $u_0 v = \pm v u_0$ pour tous les éléments v d'un système maximal T. Il est clair que u_0 ne peut permuter avec une involution de T (distincte de l'identité) lorsque $n = 2$; si trois des involutions du système T sont données par les formules du n° 44 ci-dessus qui définissent u_1, u_2, u_3, on doit donc avoir $u_0(e_1) = e_2\lambda$, $u_0(e_2) = e_1\mu$, et $\lambda\mu = \gamma$; en écrivant que $uu_0 = -u_0 u$, il vient $\alpha\lambda = -\lambda\alpha$, $\alpha\mu = -\mu\alpha$; d'autre part, en écrivant $u_0 u_3 = \pm u_3 u_0$, on obtient $\lambda = \pm\mu$; on aurait donc $\lambda^2 = \pm\gamma$, et $\alpha\lambda = -\lambda\alpha$. Mais comme -1 est carré d'un élément de Z, si $\lambda^2 = -\gamma$ il existe ϱ tel que $\varrho^2 = \gamma$ et $\alpha\varrho = -\varrho\alpha$, contrairement à l'hypothèse.

Lorsque $n = 4$, 10 des éléments d'un système maximal T peuvent être représentés par les formules du n° 48 qui donnent u_k pour $1 \leq k \leq 10$. On devra encore avoir par exemple $u_0(e_1) = e_2\lambda$, $u_0(e_2) = e_1\mu$, $u_0(e_3) = e_4\lambda'$, $u_0(e_4) = e_3\mu'$, avec $\lambda\mu = \lambda'\mu' = \gamma$. Mais alors le même raisonnement que pour $n = 2$ s'applique (u_3 étant remplacé par u_5).

Passons au cas B), et tout d'abord lorsque K contient un corps de quaternions; pour voir que $D_2(K, \gamma) = 10$ et $D_4(K, \gamma) = 36$, il faut montrer que ces nombres sont des bornes supérieures pour $b + b' + c''$ dans tous les cas, puisqu'on voit aisément qu'ils sont atteints en prenant $u_0(e_i) = e_i\beta$. Il suffit de considérer le cas où u_0 ne permute pas avec tous les éléments d'un système maximal T, puisque dans le cas contraire on aurait $b + b' + c'' = 2b$, c'est-à-dire 8 pour $n = 2$ et 32 pour $n = 4$. Or, l'ensemble H des éléments de T qui commutent avec u_0 est tel que $\overline{H}$ soit un sous-groupe d'indice 2 de $\overline{T}$. Pour $n = 2$, H a donc 4 éléments, et pour $n = 4$, H a 16 éléments; mais pour $n = 2$, un système H tel que $\overline{H}$ soit un groupe de 4 éléments ne peut être formé uniquement d'involutions, puisqu'elles devraient être toutes permutables; on a donc $b' \leq 3$; de même pour $n = 4$, le raisonnement du n° 47 montre que H contient au plus 10 involutions; d'où les bornes supérieures cherchées.

Considérons enfin le cas B) pour $n = 2$ ou $n = 4$, lorsque K ne contient pas de corps de quaternions. On peut alors raisonner comme ci-dessus pour le cas A); comme $\gamma = -1$, la relation $\lambda^2 = -\gamma$ donnerait $\lambda = \pm 1$, et on ne pourrait avoir $\alpha\lambda = -\lambda\alpha$; il n'existe donc pas d'application linéaire u_0 telle que $u_0 v = \pm v u_0$ pour tous les éléments v d'un système maximal T.

52. Passons au cas C) de [9, p. 30]. Le résultat relatif au cas où il n'existe pas d'éléments α, β de K tels que $\alpha^2 = \beta^2 = \gamma$ et $\alpha\beta = -\beta\alpha$, et où $n = 2$ ou $n = 4$, n'est pas établi de façon tout à fait complète. Il faut encore envisager la possibilité d'existence d'un élément β tel que $\beta^2 = -\gamma$ et $\alpha\beta = -\beta\alpha$; mais alors on aurait $(\alpha\beta^{-1})^2 = -\alpha^2\beta^{-2} = 1$, d'où $\alpha\beta^{-1} = \pm 1$, et par suite α et β seraient permutables, ce qui est contradictoire. On voit donc comme ci-dessus pour le cas A) qu'il n'existe pas de transformation linéaire u_0 de carré γ telle que $u_0 v = \pm v u_0$ pour tous les éléments d'un système maximal T. Pour $n = 2$, il faut donc envisager un système T de 2 éléments, comportant nécessairement la transformation identique et une involution. Mais comme u_0 ne peut permuter alors avec une involution distincte de l'identité, on a $b' = 1$, et $b + b' + c'' = 2b' + 1 = 3$, ce qui prouve que $D_2(K, \gamma) = 3$. Si $n = 4$, il faut de même envisager un système T de 8 éléments; dans ce cas, si u_0 ne permute pas avec tous les éléments de T, l'ensemble H de 4 éléments qui permutent avec u_0 est tel que $\overline{H}$ soit un groupe, donc contient au plus 3 involutions, car u_0 ne peut permuter avec 3 involutions distinctes de l'identité et 2 à 2 permutables; on a donc alors $b' \leq 3$, d'où $b + b' + c'' = 2b' + 4 \leq 10$. Reste à voir si u_0 pourrait permuter avec tous les éléments d'un système T de 8 éléments; le raisonnement du n° 47 montre aisément qu'un tel système contient toujours trois involutions qui, par rapport à une base convenable, sont identiques aux involutions notées u_2, u_3, u_4 au n° 48. Mais comme u_0 ne peut laisser une droite invariante, elle ne peut évidemment permuter à la fois à ces trois involutions. Comme par ailleurs un système maximal T de 16 éléments contient 10 involutions, on a bien ici $D_4(K, \gamma) = 10$.

53. Reste à examiner le cas D) de [9, p. 30], qui contient plusieurs énoncés erronés. Tout d'abord, contrairement à ce qui est affirmé à l'endroit cité, on peut parfaitement avoir $\alpha^2 = \beta^2 = \gamma$, $\alpha\beta = -\beta\alpha$, $\lambda^2 = -1$, $\alpha\lambda = \lambda\alpha$ et $\beta\lambda = -\lambda\beta$ dans K; l'erreur provient de ce que le centre du sous-corps de K engendré par $1, \lambda, \mu = \gamma^{-1}\alpha\beta$ et α n'est pas Z, mais $Z(\alpha\lambda)$. Un exemple où les relations précédentes sont satisfaites est obtenu en prenant pour K un produit tensoriel d'un corps de quaternions L' et d'un corps de quaternions généralisés L'' sur un corps commutatif Z

(cf. n° 34; il suffit, avec les notations de ce n°, de supposer $a_1 = a_3 = 1$, $a_2 = -1$); on prendra $1, \lambda, \mu, \lambda\mu$ identiques aux éléments de la base canonique de L', et $\alpha\lambda$ égal à un élément de L'' dont le carré appartient à Z.

Ce fait entraîne que le calcul de $D_n(K, \gamma)$ fait dans [9, p. 30–31] n'est pas correct. Il faut considérer trois sous-cas de D), et non deux.

D 1) *Il existe* $\beta \in K$ *et* $\lambda \in K$ *tels que* $\beta^2 = \gamma$, $\alpha\beta = -\beta\alpha$, $\alpha\lambda = \lambda\alpha$ *et* $\beta\lambda = -\lambda\beta$. Considérons d'abord le cas où $n \neq 2$ et $n \neq 4$. Lorsque K_1 contient un corps de quaternions, il y a lieu de considérer un système maximal T de 2^{n+1} éléments; mais si u_0 était tel que $u_0 v = \pm v u_0$ pour tous les éléments de ce système, on voit aisément qu'il devrait y avoir dans K_1 deux éléments λ, μ de carré -1, tels que $\beta\lambda = -\lambda\beta$, $\beta\mu = -\mu\beta$ et $\lambda\mu = -\mu\lambda$. Mais on aurait alors $\beta(\lambda\mu) = (\lambda\mu)\beta$ et $(\lambda\mu)^2 = -1$; or on sait [9, p. 30] que ces relations sont incompatibles. Il faut donc considérer un système T de 2^n éléments; il en est de même lorsque K_1 ne contient pas de corps de quaternions (mais alors T est maximal). Un tel système contient au plus 2^{n-1} involutions [9, p. 13–14, th. 3 et 4], et par suite $b + b' + c'' \leq 2b + 2^{n-1} \leq 3 \cdot 2^{n-1}$. Ce maximum est d'ailleurs atteint, car en vertu des hypothèses, on peut pour un système T formé de 2^{n-1} involutions, et des transformations de carré -1 obtenues en les composant avec l'application w telle que $w(e_i) = e_i\lambda$, prendre $u_0(e_i) = e_i\beta$, ce qui donne $b = b' = c'' = 2^{n-1}$. On a donc alors $D_n(K, \gamma) = 3 \cdot 2^{n-1}$.

Lorsque $n = 2$, on a nécessairement $u_0(e_1) = e_1\lambda'$, $u_0(e_2) = e_2\mu'$ avec $\lambda'^2 = \mu'^2 = \gamma$, $\lambda'\alpha = -\alpha\lambda'$, $\mu'\alpha = -\alpha\mu'$, ou $u_0(e_1) = e_2\lambda'$, $u_0(e_2) = e_1\mu'$ avec $\lambda'\mu' = \gamma$, $\lambda'\alpha = -\alpha\lambda'$, $\mu'\alpha = -\alpha\mu'$. Dans les deux cas, on constate pour la même raison que ci-dessus, que l'on ne peut avoir $u_0 v = \pm v u_0$ pour tous les éléments d'un système T maximal de 16 éléments. Il faut donc considérer un système T de 8 éléments, contenant 4 involutions, à savoir u_1, u_2, u_3 (notations du n° 44) et u_4 telle que $u_4(e_1) = e_2\lambda$, $u_4(e_2) = -e_1\lambda$. On vérifie alors que u_0 ne peut permuter à plus de trois de ces involutions, et qu'il permute effectivement avec u_1, u_2, u_3 quand on prend $u_0(e_i) = e_i\beta$. On a donc alors $b' = 3$, $b + b' + c'' = 2b' + 4 = 10$, d'où $D_2(K, \gamma) = 10$.

Pour $n = 4$, on voit de la même façon que l'on ne peut avoir $u_0 v = \pm v u_0$ pour un système maximal T de 64 éléments. On a vu plus haut (n° 48, cas D′ 4)) qu'un système T de 32 éléments est engendré par les 16 involutions qu'il contient, et qui sont (pour une base convenable) les involutions u_k $(1 \leq k \leq 16)$ définies au n° 48, en remplaçant ici α par λ. Comme on ne peut avoir $\beta\lambda = \lambda\beta$, u_0 ne peut permuter avec toutes ces involutions; mais en prenant $u_0(e_i) = e_i\beta$, on voit que u_0 permute avec les u_k tels que $1 \leq k \leq 10$, et anticommute avec les autres. D'ailleurs, des raisonnements déjà faits plusieurs fois montrent que si u_0 permute avec 16 éléments de T, il y a au plus 10 involutions parmi ces éléments, donc $b' \leq 10$, et $D_4(K, \gamma) = 2b' + 16 = 36$ dans le cas considéré.

D 2) *Lcs hypothèses de* D 1) *ne sont pas remplies, mais il existe* $\beta \in K$ *tel que* $\beta^2 = \gamma$ *et* $\alpha\beta = -\beta\alpha$. Le cas $n \neq 2$ et $n \neq 4$ est traité correctement dans [9, p. 30–31], et donne $D_n(K, \gamma) = 2^n$. Bornons-nous aux cas $n = 2$ et $n = 4$.

Pour $n = 2$, en tenant compte du fait qu'il n'existe pas d'élément $\beta' \in K$ tel que $\beta'^2 = -\gamma$ et $\alpha\beta' = -\beta'\alpha$, on voit qu'on ne peut considérer que les systèmes T de 4 éléments; un tel système est engendré par les 3 involutions u_1, u_2, u_3 et u_0 peut permuter avec ces 3 involutions en prenant $u_0(e_i) = e_i\beta$; on a donc $D_2(K, \gamma) = 6$, puisque dans un système T maximal il y a au plus 6 involutions.

Pour $n = 4$, on vérifie de même qu'on ne peut considérer que les systèmes T de 16 éléments, et on voit comme dans le cas D'' 3) du n° 49 que $b + b' + c'' \leq 20$ dans ce cas, la limite pouvant être atteinte. Mais il faut tenir compte de ce que, lorsque K_1 contient un corps de quaternions, un système T maximal de 64 éléments contient 28 .involutions; on a donc $D_4(K, \gamma) = 28$ lorsque K_1 contient un corps de quaternions, et $D_4(K, \gamma) = 20$ dans le cas contraire.

D 3) *Il n'existe pas d'élément* $\beta \in K$ *tel que* $\beta^2 = \gamma$ *et* $\alpha\beta = -\beta\alpha$. Pour $n \neq 2$ et $n \neq 4$, l'indication donnée dans [9, p. 31] n'est pas suffisante. En effet, on montre comme dans le cas B) [9, p. 29] que si u_0 est permutable avec toutes les involutions d'un système T, l'intersection des sous-espaces (positifs ou négatifs) d'un nombre quelconque d'involutions du système T est de dimension paire. Mais rien ne dit que les involutions de T sont deux à deux permutables; reprenons donc la question plus en détail.

Il s'agit de prouver que pour un système T non maximal de 2^n ou 2^{n-1} éléments (le cas où T a 2^n éléments sans être maximal peut se présenter lorsque K_1 contient un corps de quaternions), on a nécessairement $b + b' + c'' \leq 2^{n-1}$. Cela sera certainement vérifié si on prouve qu'un système S de transformations de carré ± 1 permutables avec u_0, et tel que $\bar{S}$ forme un groupe dans $PGL_n(K)$, a au plus 2^{n-3} éléments.

Le raisonnement de [9, p. 29] montre qu'il en est bien ainsi lorsque tous les éléments de S sont des involutions, car alors ces involutions sont nécessairement permutables deux à deux. Supposons ensuite qu'il existe dans S une transformation v_0 de carré -1, et raisonnons comme dans [9, p. 11], en tenant compte du fait que K_1 contient un élément λ de carré -1 et non situé dans son centre. On voit ainsi que l'ensemble S' des transformations de S permutables avec v_0 contient autant d'involutions que de transformations de carré -1, et que S a au plus deux fois autant d'éléments que S. Nous savons que toute intersection de sous-espaces positifs ou négatifs d'involutions de S' doit être de dimension paire sur K_1. Soit K' le sous-corps de K_1 formé des éléments permutables avec λ, et soit U le sous-espace (sur K') de W tel que $v_0(x) = x\lambda$ dans U. Les restrictions à U des involutions de S' forment un système d'involutions S'' dans U tel que toute intersection de sous-espaces positifs ou négatifs d'involutions de S'' doit être de dimension paire sur K'. Cela étant, comme -1 est carré d'un élément du centre de K', on peut, pour déterminer le nombre maximum d'éléments de S'', reprendre la méthode de récurrence «de n à $n/2$» développée dans [9, p. 4–5], car on vérifie aussitôt que le passage de n à $n/2$ conserve la condition de parité des dimensions des intersections des sous-espaces des involutions considérées (la méthode consistant à se ramener toujours à ne considérer que des involutions permutables avec l'involution désignée par u dans [9, p. 4]). La conclusion est donc que si $n = 2m$, le nombre maximum d'éléments de S est $C_m(K_1)$, et le nombre maximum d'involutions dans S est $B'_m(K_1) = B_m(K_1)$, nombres qui sont donnés par les théorèmes 3 et 4 de [9]. Supposons d'abord que K_1 ne contienne pas de corps de quaternions; alors on a pour $n \neq 2$ et $n \neq 4$, $C_m(K_1) = 2^m$ sauf pour $n = 8$, ou $C_4(K_1) = 32$; on a bien dans tous les cas $C_m(K_1) \leq 2^{n-3}$. Si au contraire K_1 contient un corps de quaternions, on a $C_m(K_1) = 2^{m+1}$ sauf pour $n = 8$ où $C_4(K_1) = 64$; ici l'inégalité $C_m(K_1) \leq 2^{n-3}$ est vérifiée sauf pour $n = 6$ et $n = 8$. Mais pour $n = 6$, un système S de 16 éléments contient au plus $B_3(K_1) = 4$ involutions; dans un système T de 32 éléments, on a donc $b + b' + c'' = 2b' + 16 \leq 24 < 2^5$. De même, si $n = 8$, un système S de 64 éléments contient au plus 28 involutions; dans un système T de 2^7 éléments, on a par suite $b + b' + c'' = 2b' + 64 \leq 120 < 2^7$. On a ainsi prouvé la relation $D_n(K, \gamma) = 2^{n-1}$ dans le cas que nous considérons.

Le même raisonnement s'applique d'ailleurs aussi pour $n = 2$ et $n = 4$. Pour $n = 2$, on a $C_1(K_1) = 2$ si K_1 ne contient pas de corps de quaternions, $C_1(K_1) = 4$ dans le cas contraire; comme u_0 ne peut alors permuter à aucune involution autre que l'identité, on a $b + b' + c'' \leq 4$ dans le premier cas, $b + b' + c'' \leq 6$ dans le second; d'ailleurs un système T maximal contenant 4 involutions dans le premier cas, et 6 dans le second, on a bien respectivement $D_2(K, \gamma) = 4$ et $D_2(K, \gamma) = 6$. Pour $n = 4$, $C_2(K_1) = 8$ si K_1 ne contient pas de corps de quaternions, $C_2(K_1) = 16$ dans le cas opposé; en outre, il y a dans un système S au plus 4 involutions dans le premier cas, et 6 dans le second, d'où les limites 16 et 28 pour $b + b' + c''$; on en déduit comme précédemment $D_4(K, \gamma) = 16$ et $D_4(K, \gamma) = 28$ respectivement.

Bibliographie.

[1] A. A. ALBERT, Division algebras over an algebraic field, *Bulletin of the American Mathematical Society*, t. 37 (1931), p. 777–784.

[2] N. BOURBAKI, *Eléments de Mathématique:* Algèbre, chap. III *(Actual. Scient. et Ind.)*, n° 1044, Paris (Hermann), 1948).

[3] ——, *Eléments de Mathématique:* Algèbre, chap. IV–V *(Actual. Scient. et Ind.*, n° 1102, Paris (Hermann), 1950).

[4] R. BRAUER, On a theorem of H. Cartan, *Bulletin of the American Mathematical Society*, t. 55 (1949), p. 619–620.

[5] H. CARTAN, Théorie de Galois pour les corps non commutatifs, *Annales de l'Ecole Normale Supérieure*, t. 64 (1947), p. 59–77.

[6] W. L. CHOW, On the geometry of algebraic homogeneous spaces, *Annals of Mathematics*, t. 50 (1949), p. 32–67.

[7] J. DIEUDONNÉ, La théorie de Galois des anneaux simples et semi-simples, *Commentarii Mathematici Helvetici*, t. 21 (1947), p. 154–184.

[8] ——, Sur les groupes classiques (*Actual. Scient. et Ind.*, n° 1040, Paris (Hermann), 1948).

[9] ——, Sur les systèmes maximaux d'involutions conjuguées et permutables dans les groupes projectifs, *Summa Brasiliensis Mathematicae*, t. 2, fasc. 6 (1950), p. 1–36.

[10] ——, On the automorphisms of the classical groups, *Memoirs of the American Mathematical Society*, n° 2 (1951).

[11] L. K. HUA, Some properties of a sfield, *Proceedings of the national Academy of Sciences*, t. 35 (1949), p. 533–537.

[12] N. JACOBSON, The theory of rings (*Mathematical Surveys*, n° 2 (1943)).

[13] ——, A note on division rings, *American Journal of Mathematics*, t. 69 (1947), p. 27–36.

[14] B. L. VAN DER WAERDEN, Gruppen von linearen Transformationen (*Ergebnisse der Math.*, t. 4, fasc. 2, Berlin (Springer), 1935).

[15] E. WITT, Theorie der quadratischen Formen in beliebigen Körpern, *Journal de Crelle*, t. 176 (1937), p. 31–44.