Séminaire Dubreil.
Algèbre et théorie
des nombres

Günter Pickert

Conditions de transitivité pour les groupes d'automorphismes d'algèbres de dimension 2

Séminaire Dubreil. Algèbre et théorie des nombres, tome 21, n° 1 (1967-1968), exp. n° 6, p. 1-6
<http://www.numdam.org/item?id=SD_1967-1968__21_1_A6_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
21e année, 1967/68, n° 6

18 décembre 1967

CONDITIONS DE TRANSITIVITÉ POUR LES GROUPES D'AUTOMORPHISMES D'ALGÈBRES DE DIMENSION 2

par Günter PICKERT

Il est bien connu qu'on n'utilise pas de multiplication vectorielle en géométrie plane. Pour en connaître la raison, on doit d'abord établir la condition minimale que doit satisfaire une multiplication vectorielle dans un espace vectoriel V sur un corps (commutatif) K : celle-ci doit être une application bilinéaire de $V \times V$ dans V. Par la donnée d'une telle multiplication, V devient une algèbre ; dans ce qui suit, nous désignerons celle-ci aussi par V, et nous écrirons la multiplication $(x , y) \to xy$. Naturellement nous exclurons le cas trivial d'une zéro-algèbre ($xy = 0$ pour tout $x , y \in V$). De plus, la géométrie exige, au moins, que le groupe Φ des automorphismes de l'agèbre opère transitivement sur l'ensemble des sous-espaces de dimension 1 de V ; ici, on appelle automorphisme de l'algèbre V une application linéaire bijective φ de V sur V vérifiant

$$\varphi(xy) = \varphi(x)\,\varphi(y) \qquad \text{pour tout } x , y \in V \ ;$$

et la condition de transitivité s'écrit explicitement :

$$\text{(T)} \qquad \forall\, x , y \in V \setminus \{0\} , \quad \exists\, \varphi \in \Phi , s \in K , \qquad \varphi(x) = sy .$$

Le théorème (*) suivant montre la raison pour laquelle on ne peut pas utiliser une multiplication vectorielle dans le cas de la dimension 2.

THÉORÈME. - Si K est un corps non réduit à deux éléments, il n'y a pas d'algèbre V sur K de dimension 2 vérifiant la condition (T), en dehors de la zéro-algèbre. Si K possède seulement deux éléments, alors il y a exactement deux algèbres non isomorphes ayant ces propriétés ; ces algèbres sont commutatives et, en posant $V = \{0 , e , f , g\}$, leurs multiplications sont données par les équations (i), (ii) suivantes et les équations qui en découlent par permutation cyclique de e , f , g :

(i) $e^2 = e$, $ef = g$,

(ii) $e^2 = f$, $ef = e$;

dans le premier cas, Φ est isomorphe à S_3, dans le deuxième cas à A_3.

(*) Voir (G.) PICKERT. - Warum verwendet man in der ebenen Geometrie keine vektorielle Multiplikation, Math.-phys. Semesterberichte, t. 15, 1968, Fasc. 2 (à paraître).

Maintenant, nous allons modifier la condition (T) de façon que Φ laisse invariant un sous-espace $F = Kf$ $(f \neq 0)$ de dimension 1 et que Φ opère transitivement seulement sur l'ensemble des autres sous-espaces de dimension 1 . Si l'on choisit $e \notin F$ tel que (e , f) constitue une base de l'espace vectoriel V de dimension 2 , nous avons :

$$(T') \qquad \forall\ t \in K\ ,\quad \exists\ \varphi \in \Phi\ ,\ s \in K\ ,\qquad \varphi(e) = s(e + tf)\quad .$$

En vertu de $\varphi(f^2) = \varphi(f)^2 \in Kf^2$, $\forall\ \varphi \in \Phi$, on doit avoir $f^2 \in F$. Si on a $f^2 \neq 0$ c'est-à-dire $f^2 = rf$ pour un $r \neq 0$, on remplace f par $r^{-1} f$ et on obtient ainsi $f^2 = f$, $\forall\ \varphi \in \Phi$, $\varphi(f) = f$. Nous traitons d'abord ce cas

$$(I) \qquad f^2 = f\ ,\qquad e^2 = ae + bf\ ,\qquad ef = ce + df\ ,\qquad fe = c'e + d'f\quad .$$

D'après $\varphi(e) = s(e + tf)$, $f(f) = f$, l'application linéaire bijective φ est déjà entièrement déterminée par les $s , t \in K$ avec $s \neq 0$, et cette application appartient à Φ si, et seulement si, l'on a $\varphi(e)^2 = \varphi(e^2)$, $\varphi(ef) = \varphi(e)f$, $\varphi(fe) = f\ \varphi(e)$. Par conséquent, (T') peut s'écrire sous la forme :

Pour tout $t \in K$, il existe $s\ (\neq 0) \in K$ tel que

$$(1) \qquad s(a + t(c + c')) = a\ ,$$

$$(2) \qquad s^2(b + t(d + d') + t^2) = ast + b\ ,$$

$$(3) \qquad s(t(1 - c) + d) = d\ ,$$

$$(3') \qquad s(t(1 - c') + d') = d'\ .$$

De plus, (1) peut être transformé en

$$(1^*) \qquad c + c' = 0\ ;\quad a \neq 0 \implies s = 1\quad .$$

Car, dans le cas $a = 0$, en vertu de $s \neq 0$, on déduit $c + c' = 0$ en prenant $t = 0$; tandis que $a \neq 0$, $c + c' \neq 0$ sont incompatibles comme on le voit en prenant $t = -\,a(c + c')^{-1}$; ayant montré l'égalité $c + c' = 0$, l'équation (1) se réduit à $a \neq 0 \implies s = 1$. D'une façon analogue, (3), (3') s'écrivent sous la forme

$$(3^*) \qquad c = c' = 1\ ;\quad d' \neq 0 \text{ ou } d \neq 0 \implies s = 1\ .$$

Compte tenu de (1^*), la caractéristique de K est donc égale à 2 .

Si on a $a \neq 0$, l'équation (2) devient

$$(2^*) \qquad \forall\ t \in K\ ,\qquad t(d + d' - a) + t^2 = 0\ ,$$

en vertu de (1^*). Mais ceci est équivalent à $K = GF(2)$ (c'est-à-dire K est réduit à $\{0 , 1\}$) , et $a = 1$, $d = d'$. En posant $g = e + f$, nous obtenons, en vertu de (3^*) en dehors du type décrit dans (i) dans lequel cependant F n'est pas invariant par Φ, les trois possibilités suivantes :

(I_1) $$e^2 = e\ , \qquad ef = fe = e\ ,$$

(I_2) $$e^2 = g\ , \qquad ef = fe = e\ ,$$

(I_3) $$e^2 = g\ , \qquad ef = fe = g\ .$$

Dans le cas de (I_1), il s'agit de la somme directe des corps Ke, Kg ayant $f = e + g$ comme élément unité ; dans le cas de (I_2), il s'agit du corps à quatre éléments (ayant f comme élément unité), tandis que dans le cas de (I_3) il n'y a d'élément unité ni à gauche ni à droite.

Si l'on a $a = 0$, on ne peut pas avoir $d = d'$; car, puisque K est de caractéristique 2, avec $d = d'$, l'équation (2) s'écrirait

$$s^2 b + (st)^2 = b$$

ce qui montrerait que, pour $t = 1$, b est le carré d'un élément $b' \neq 0$ et, ensuite, $b = 0$ pour $t = b'$. Par conséquent nous avons $d \neq d'$, de sorte que (3^*) entraîne $s = 1$. Nous obtenons donc encore (2^*) et, par conséquent, $K = GF(2)$. Mais $a = 0$ entraîne maintenant $d + d' = 1$, donc $d = 1$, $d' = 0$ ou $d = 0$, $d' = 1$. Puisque $b = 0$ et $b = 1$ sont possibles, on obtient les possibilités

(I_4) $$e^2 = f\ , \qquad ef = g\ , \qquad fe = e\ ,$$

(I_5) $$e^2 = 0\ , \qquad ef = g\ , \qquad fe = e\ ,$$

ainsi que les opposées obtenues par permutation des facteurs. D'après notre démonstration, ces sept algèbres satisfont toutes la condition (T'). Si dans une de ces algèbres, f ne reste pas fixe par Φ, on aura même (T), ce qui est impossible en vertu de la non-isomorphie avec les types donnés par (i) et (ii) respectivement. Dans le cas de (I_4) et (I_5), f est un élément unité à gauche, mais pas à droite ; par conséquent les quatre algèbres nouvelles ne sont isomorphes à aucun des types (I_{1-3}). En résumé nous avons un résultat semblable **à** celui que nous avons obtenu dans le cas de l'hypothèse (T) :

<u>Si le groupe</u> Φ <u>des automorphismes de l'algèbre</u> $V = Ke + Kf$ <u>de dimension</u> 2 <u>laisse invariant le sous-espace</u> Kf, <u>si ce sous-espace n'est pas une zéro-algèbre et si la condition (T') est vérifiée, alors</u> K <u>est le corps à deux éléments, et il y a exactement sept possibilités non isomorphes pour</u> V ; <u>pour chacune de celles-ci,</u> Φ <u>est isomorphe à</u> S_2 .

Traitons maintenant le cas $f^2 = 0$:

(II) $f^2 = 0$, $e^2 = ae + bf$, $ef = ce = df$, $fe = c'e + d'f$.

En posant $\varphi(f) = rf$, la condition (T') s'écrit comme suit :

Pour tout $t \in K$, il existe $r , s \in K \setminus \{0\}$ tels que

(1) $$s(a + t(c + c')) = a ,$$

(4) $$s^2(b + t(d + d')) = ast + br ,$$

(5) $$c = cr , \quad s(dr - ct) = dr ,$$

(5') $$c' = c'r , \quad s(d'r - c't) = d'r ,$$

Ainsi on fait correspondre à tout $\varphi \in \Phi$, de façon biunivoque, un triple (r , s , t) et le groupe Φ est isomorphe au groupe des matrices

(6) $$\begin{pmatrix} s & 0 \\ st & r \end{pmatrix}$$

où $r , s \neq 0$,(1), (4), (5), (5'). Dans le cas $d = 0$, la deuxième équation dans (5) donne $c = 0$ pour $t = 1$; mais $c \neq 0$ et $d \neq 0$ sont aussi incompatibles, puisque $c \neq 0$ et $d \neq 0$ entraîneraient $r = 0$, en posant $t = drc^{-1}$. Par conséquent, (5) et (5') se réduisent à

(5^*) $$c = c' = 0 \ ; \quad d \neq 0 \text{ ou } d' \neq 0 \implies s = 1 .$$

Dans le cas $a \neq 0$, d'après (1^*), l'équation (4) peut s'écrire

$$t(d + d' - a) = b(r - 1) ,$$

d'où, pour $t = 0$,

(4^*) $$d + d' = a ,$$

pourvu que $b = 0$. L'équation (4^*) reste vraie pour $b \neq 0$, puisque, dans le cas contraire, on pourrait poser $t = - b(d + d' - a)^{-1}$, ce qui entraînerait $r = 0$. Dans le cas $a = 0$, l'équation (4) peut s'écrire $s^2(b + t(d + d')) = br$, d'où on tire encore (4^*) : dans le cas $b = 0$, on pose $t = 1$, et dans le cas $b \neq 0$, on pose $t = - b(d + d')^{-1}$. Compte tenu de (1^*), l'équation (4) est équivalente à (4^*) , (4^{**}), où

(4^{**}) $$a , b \neq 0 \implies r = 1 \ ; \quad a = 0 , \ b \neq 0 \implies r = s^2 .$$

Puisque (1^*) est une conséquence de (4^*), (5^*), on peut formuler (T') de la manière suivante :

Pour tout $t \in K$, il existe $r , s \in K \setminus \{0\}$ tels que l'on ait (4^*), (4^{**}), (5^*).

Maintenant nous allons énumérer les différents types possibles.

Dans le cas $a = b = 0$, $d = 0$ conduit à la zéro-algèbre d'après (4^*), de sorte qu'on doit avoir d , $d' \neq 0$. En remplaçant e par $d^{-1} e$, on peut supposer $d = 1$;

(II_1) $$e^2 = f^2 = 0 , \qquad ef = - fe = f .$$

Compte tenu de (5^*), le groupe des matrices, isomorphe à Φ selon (6), est constitué par $\begin{pmatrix} 1 & 0 \\ t & r \end{pmatrix}$, où $r \neq 0$. Dans le cas $a = 0$, $b \neq 0$, on peut évidemment obtenir $b = 1$ en modifiant f , et, comme dans le cas précédent, on peut supposer $d = 1$, pourvu que $d \neq 0$:

(II_2) $$e^2 = f , \qquad f^2 = 0 , \qquad ef = - fe = f ;$$

d'après (4^{**}), (5^*), le groupe de matrices isomorphe à Φ est constitué par les matrices de la forme $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$, il est donc isomorphe au groupe additif de K .

(II_3) $$e^2 = f , \qquad f^2 = 0 , \qquad ef = fe = 0 ;$$

d'après (4^{**}), le groupe de matrices est constitué par les matrices de la forme $s\begin{pmatrix} 1 & 0 \\ t & s \end{pmatrix}$, où $s \neq 0$. Dans le cas $a \neq 0$, on peut supposer $a = 1$ (en modifiant e) et $b = 1$ (en modifiant f) si, de plus, $b \neq 0$:

(II_4) $$e^2 = e , \qquad f^2 = 0 , \qquad ef = df , \qquad fe = (1 - d)f ;$$

(II_5) $$e^2 = e + f , \qquad f^2 = 0 , \qquad ef = df , \qquad fe = (1 - d)f .$$

Dans le cas (II_4), le groupe des automorphismes est le même que dans le cas (II_1), d'après (5^*), et dans le cas (II_5), il est le même que dans le cas (II_2), d'après (4^{**}), (5^*).

Afin de voir que les cinq types sont deux à deux non isomorphes et que, de plus, d est invariant par isomorphie, nous utilisons les ensembles

$$J = \{x \mid x^2 = x \neq 0\} , \qquad N = \{x \mid x^2 = 0\}$$

qui eux sont invariants par isomorphie. Dans le cas (II_1), $J = \emptyset$, $N = V$; dans les cas $(II_{2,3,5})$, $J = \emptyset$, $N = F$; dans le cas (II_4), $J = e + F$, $N = F$. De plus, (II_3) se distingue de tous les autres types par $xf = fx = 0$, $\forall\, x \in V$, tandis que, contrairement à $(II_{4,5})$, les types (II_{1-3}) possèdent la propriété $xy \in F$, $\forall\, x \in V$, $y \in V$. Ainsi, nous avons montré la non-isomorphie des cinq types. Dans le cas (II_4), la multiplication peut être décrite à l'aide de J , N , d

de la manière suivante :

$$x\ ,\ y \in J \implies xy = (1-d)x + dy\ ;\quad x \in J\ ,\ y \in N \implies xy = dy\ ,\quad yx = (1-d)y,$$

ce qui entraîne l'invariance de d par isomorphie. D'ailleurs, le groupe des automorphismes est constitué par les applications linéaires bijectives laissant J invariant. Pour la description de (II_5), nous utilisons l'ensemble

$$J' = \{x \mid x^2 \neq 0\ ,\ x^2 - x \in F\} = e + F$$

invariant par isomorphie. D'après $x \in J' \implies x^2 - x = f$, le vecteur f est aussi invariant, et la multiplication peut être donnée sous la forme suivante :

$$x\ ,\ y \in J' \implies xy = (1-d)x + dy + f\ ,\quad x \in J'\ ,\ y \in N$$

$$\implies xy = dy\ ,\ yx = (1-d)y\ ,$$

ce qui montre encore l'invariance de d par isomorphie.