

Groupoïdes orthogonaux.

Par A. SADE à Marseille.

I. Orthogonalité en général.

1. Définition. Un système orthogonal est un ensemble E sur lequel deux lois de composition $(\cdot)$ et $(\times)$ ont été définies, de manière que, pour tous $x, y, z, t \in E$, on ait :

$$\left. \begin{array}{l} x \cdot y = z \cdot t \\ x \times y = z \times t \end{array} \right\} \begin{array}{l} \longrightarrow \\ \longleftarrow \end{array} x = z, y = t.$$

Exemple I. Sur le corps des nombres réels,

$$x \cdot y = ax + by; \quad x \times y = cx + dy,$$

est un système orthogonal, sous la condition :

$$ad - bc \neq 0.$$

Exemple II. Si $\mathbb{Z}$ désigne l'anneau des nombres entiers rationnels et $\mathbb{Z}/n$ celui des classes résiduelles, modulo n dans $\mathbb{Z}$, les mêmes lois définissent deux quasigroupes orthogonaux d'ordre n , sous les conditions, $a, b, c, d \in \mathbb{Z}/n$ et $(ad - bc, n) = 1$.

L'étude de tels systèmes sous l'angle des équations fonctionnelles serait digne d'intérêt ; nous nous bornerons à l'aborder au point de vue de l'algèbre abstraite.

Quand deux lois définissent un système orthogonal, on dira encore que ces lois, et aussi les deux grupoïdes qu'elles déterminent, sont *orthogonaux*.

2. Parastrophie. Si E est un système orthogonal avec des lois $(\cdot)$ et $(\times)$, *bicancellables*, et si $x \cdot y = u$, $x \times y = v$, alors deux quelconques, a et b , des quatre éléments x, y, u, v , déterminent les deux autres, quand ils existent. Si $a \oplus b = c$ et $a \otimes b = d$ sont les deux lois ainsi construites, le nouveau système est orthogonal. On définit de cette manière une *parastrophie*, ([5], p. 362), plus étendue que dans le cas d'un grupoïde.

Cette parastrophie, sauf dans le cas où $a = y$ et $b = x$, ne s'identifie pas avec celles que l'on obtiendrait en opérant sur les deux grupoïdes $A(\cdot)$

et $B(\times)$ séparément. Ainsi les réciproques $(x \cdot y = z \implies z * y = x)$ de deux groupoïdes orthogonaux ne sont pas nécessairement orthogonaux.

Exemple. Sur l'anneau $\mathbb{Z}/25$, les deux groupoïdes $z = x + 2y$ et $z = 3x + 7y$, sont orthogonaux. Les quasigroupes réciproques $x = z - 2y$ et $x = 17z + 6y$ ne le sont pas.

3. On rappelle que deux groupoïdes sont *conjointes* ([2], p. 60), si le produit de deux éléments quelconques, x, y , dans l'un est égal au produit de y par x dans le second.

Le conjoint d'un système orthogonal est un système orthogonal.

Par conjoint d'un système orthogonal il faut entendre le système obtenu en remplaçant chacun des groupoïdes $A(\cdot)$ et $B(\times)$ par son conjoint, soit :

$$\begin{aligned} x \cdot y = z & \xrightarrow{\quad} y \circ x = z, \\ x \times y = t & \xrightarrow{\quad} y * x = t. \end{aligned}$$

Les nouvelles lois définissent encore un système orthogonal, car si $m = x \cdot y = x' \cdot y'$ et $p = x \times y = x' \times y'$, on aura $m = y \circ x = y' \circ x'$ et $p = y * x = y' * x'$; donc la seconde hypothèse, comme la première, impliquera $x = x'$ et $y = y'$.

4. Composition. Si $A(\cdot)$ et $B(\times)$ sont deux groupoïdes orthogonaux sur un ensemble E et si $G(\circ)$ est un groupoïde quelconque bicancellable sur E , alors la loi $(*)$ définie sur E par :

$$x * y = (x \cdot y) \circ (x \times y),$$

symboliquement : $A \circ B = C$, est orthogonale aux deux autres $(\cdot)$ et $(\times)$.

Preuve. Supposons : $x * y = x' * y'$ et $x \cdot y = x' \cdot y'$; par définition : $(x \cdot y) \circ (x \times y) = (x' \cdot y') \circ (x' \times y')$, et puisque $G(\circ)$ est cancellable :

$$x \times y = x' \times y';$$

enfin, puisque A et B sont orthogonaux : $x = x'$ et $y = y'$. Donc $C(*)$ est orthogonal à $A(\cdot)$. On voit pareillement que C et B sont orthogonaux.

5. Réciproque. Si $A(\cdot)$, $B(\times)$ et $C(*)$ sont trois groupoïdes deux à deux orthogonaux sur un ensemble E , il existe un groupoïde $G(\circ)$, unique et déterminé, bicancellable, tel que, pour tous $x, y \in E$, on ait : $(x \cdot y) \circ (x \times y) = x * y$.

Soit

$$\begin{aligned} x \cdot y = a, & \quad x \times y = b, & \quad x * y = c, \\ x' \cdot y' = a', & \quad x' \times y' = b', & \quad x' * y' = c'. \end{aligned}$$

Puisque A, B et C sont orthogonaux, deux quelconques des égalités $a = a', b = b', c = c'$, impliquent $x = x'$ et $y = y'$ et par conséquent la

troisième. Posons :

$$a \circ b = c, \quad a' \circ b' = c'$$

1°. Si $a = a'$ et $b = b'$, il en résulte $c = c'$, ou $a \circ b = a' \circ b'$, donc le produit $(\circ)$ est défini univoque.

2°. Si $a = a'$ et $c = c'$, alors $b = b'$, donc $G(\circ)$ est cancellable à gauche.

3°. On voit de même qu'il est cancellable à droite.

Exemple. Sur le corps $\mathbb{Q}$ des fractions rationnelles, les trois quasi-groupes $A(\cdot)$, $B(\times)$, $C(*)$ définis par les relations: $x \cdot y = p^i x + q^i y$, $x \times y = p^j x + q^j y$, $x * y = p^k x + q^k y$, avec p et q non nuls et inégaux dans $\mathbb{Q}$ et i, j, k entiers naturels inégaux, sont deux à deux orthogonaux.

Si l'on pose, comme plus haut, $x \cdot y = a$, $x \times y = b$, ces équations sont linéaires en x et y ; à tout système de valeurs (a, b) correspond un système de valeurs (x, y) unique et bien déterminé, et par conséquent une valeur univoque de $c = x * y$. On trouve $a \circ b = ra + sb$ où $r = (p^k q^j - q^k p^j) / (p^i q^j - p^j q^i)$ et $s = (q^k p^i - p^k q^i) / (p^i q^j - p^j q^i)$.

Remarquons qu'en général $G(\circ)$ n'est homogène que si $(\exists x, y) \ x \cdot y = a$, $x \times y = b$, ce qui ne serait pas le cas, dans l'exemple précédent, pour tous a, b , si A, B, C étaient des groupoïdes sur $\mathbb{Z}$.

Observons aussi que les groupoïdes analogues à G , obtenus en permutant A, B, C , sont parastrophiques (au sens usuel); par exemple, en permutant A et C on obtient deux groupoïdes G et G' , réciproques.

6. L'ensemble L , dont les éléments sont les groupoïdes engendrés par deux groupoïdes orthogonaux $A(\cdot)$ et $B(\times)$, sous la loi de composition $X \circ Y = Z$ définie comme au N° 4, par un groupoïde bicancellable donné $G(\circ)$, 1°) est bicancellable, 2°) est homomorphe à G . Les éléments de L dont l'image est l'élément m de G sont ceux dans lesquels le produit de deux éléments fixés x, y est égal à m . 3°) L'ensemble de ces homomorphismes a une puissance inférieure ou égale à celle de E^2 . 4°) Deux groupoïdes de L et leur produit sont orthogonaux deux à deux, ou aucun n'est orthogonal à un autre.

1° La loi de composition $X \circ Y = Z$, induite par $G(\circ)$ est évidemment bicancellable puisque G l'est.

2° Définissons une partition de L en rangeant dans un même bloc ([3], p. 574), K_m , tous les groupoïdes dans lesquels le produit de deux éléments déterminés x, y est égal à m . A chaque élément, $m \in E$, correspond un bloc. Cette partition est régulière par rapport à $(\circ)$ car, soit $A(\cdot) \in K_m$ et $B(\times) \in K_p$; on aura dans A : $x \cdot y = m$ et dans B : $x \times y = p$.

Mais, par définition, si $A \circ B = C(*)$, on a ($N^\circ 4$):

$$x * y = (x \cdot y) \circ (x \times y) = m \circ p,$$

donc $C \in K_{m \circ p}$, et ainsi :

$$K_m \circ K_p = K_{m \circ p},$$

ce qui établit l'homomorphisme.

3° L'homomorphisme est défini par la donnée des deux éléments fixes x, y . A chaque élément (x, y) de l'ensemble produit E^2 correspond donc un homomorphisme. Mais comme tous ces homomorphismes ne sont pas distincts, en général, la puissance de l'ensemble des homomorphismes est inférieure ou égale à celle de E^2 .

4° Si X et Y sont deux groupoïdes orthogonaux de L , d'après le $N^\circ 4$, ils seront orthogonaux à leur produit $X \circ Y$. Si X et Y ne sont pas orthogonaux, ils ne le seront pas à ce produit.

Exemple. Partons des deux quasigroupes orthogonaux du 3^{ème} ordre, construits sur $\mathbb{Z}/3: A(\cdot), x \cdot y = 2x + y + 1, B(\times), x \times y = 2x - y + 1$ et formons leur produit selon $G(\circ), x \circ y = 2 - x + y$. On trouve : $C(\wedge) = A \circ B, x \wedge y = y + 2, D(\vee) = B \circ A, x \vee y = 2 - y, E(\perp) = A \circ C, x \perp y = x, F(*) = C \circ A, x * y = 2x + 1, G(\otimes) = B \circ C, x \otimes y = x + 2y, H(\oplus) = E \circ A, x \oplus y = x + y, I(:) = A \circ A, x : y = 2$.

Si l'on met $I(:)$ à part, A est orthogonal à tous les autres groupoïdes, sauf G ; B à tous les autres, sauf H ; C à tous sauf D , E à tous sauf F . L est idempotent. Les translations à gauche de L sont :

$$\begin{aligned}(L \rightarrow A \circ L) &= a = (AIG)(BCE)(DHF) = g^{-1} \\ b &= (ADE)(B|H)(CGF) = h^{-1} \\ c &= (AFB)(CID)(EGH) = d^{-1} \\ e &= (AHC)(BGD)(EIF) = f^{-1} \\ i &= 1\end{aligned}$$

En prenant $x = y = 0$, on trouve l'homomorphisme :

$$ABF \rightarrow 1, \quad EGH \rightarrow 0, \quad CDI \rightarrow 2.$$

En prenant $x = 1, y = 0$, on trouve les mêmes cosets, mais avec l'homomorphisme :

$$ABF \rightarrow 0, \quad EGH \rightarrow 1, \quad CDI \rightarrow 2.$$

7. Plus généralement, Si $S = (x, y), (x', y'), \dots$ est un ensemble quelconque dans E^2 , $(x, x', \dots, y, y', \dots)$ fixés la partition de L dont les blocs $K_m, m', \dots$ sont composés des groupoïdes dans lesquels les produits $(x \cdot y), (x' \times y'), \dots$ ont des valeurs données $m, m', \dots$, est régulière par rapport à-la

loi de composition ($\circ$) et les blocs K forment un groupoïde quotient dont la loi de composition est :

$$K_{m, m', \dots} \circ K_{p, p', \dots} = K_{m \circ p, m' \circ p', \dots}$$

Chaque partition est pleinement définie par l'ensemble correspondant S .

La partition est régulière car si $A(\cdot) \in K_{m, m' \dots}$ et si $B(\times) \in K_{p, p' \dots}$, on aura :

$$A \circ B = C(*)$$

si

$$\begin{aligned} (x \cdot y) \circ (x \times y) &= x * y \\ (x' \cdot y') \circ (x' \times y') &= x' * y', \text{ etc,} \end{aligned}$$

ou :

$$\begin{aligned} x * y &= m \circ p, \\ x' * y' &= m' \circ p' \text{ etc.} \end{aligned}$$

Donc $C \in K_{m \circ p, m' \circ p', \dots}$.

Ainsi les blocs K forment un groupoïde, avec la loi de composition :

$$K_{m, m', \dots} \circ K_{p, p', \dots} = K_{m \circ p, m' \circ p', \dots}$$

8. L est un quasigroupe, un semi-groupe, un groupoïde commutatif, en même temps que $G(\circ)$. Il obéit à toute identité à laquelle G satisfait.

1°. Si $G(\circ)$ satisfait à la loi du quotient, soit :

$$(x \cdot y) \circ (x \times y) = x * y$$

et $x \times y = a$, $x * y = b$. L'équation : $u \circ a = b$ a une solution unique en u , d'où : $x \cdot y = u$. Cela pouvant être répété pour tous $x, y \in E$, on voit que A , tel que $A \circ B = C$ est entièrement déterminé par B et C . Donc L obéit à la loi du quotient à gauche. On verrait pareillement qu'il obéit à cette loi, à droite.

2°. Soit, avec les mêmes notations :

$$\begin{aligned} x : y &= d, & x \otimes y &= f, & x \oplus y &= g, & u \circ g &= f' \\ (x \cdot y) \circ (x \times y) &= x * y & \text{ et } & (x * y) \circ (x : y) &= x \otimes y &= f, \end{aligned}$$

puis :

$$(x \times y) \circ (x : y) = x \oplus y \text{ et } (x \cdot y) \circ (x \oplus y) = f'.$$

Cela s'écrit : $(u \circ a) \circ d = f$, $u \circ (a \circ d) = f'$.

Pour que L soit associatif il faut et il suffit que $f = f'$, c'est-à-dire que $G(\circ)$ soit un semi-groupe.

3°. On voit de même que L est commutatif en même temps que G .

Ces propositions ne sont pas évidentes, car un groupoïde dont un groupoïde quotient est associatif ou commutatif n'est pas nécessairement associatif ou commutatif lui-même.

9. Complexes. Si $A \in L$ est orthogonal à chacun des éléments d'un complexe $K = B, C, D, \dots \in L$, alors A sera orthogonal à $K \circ A$ et à $A \circ K$.

En effet, si A est orthogonal à B , alors, A, B , et $A \circ B$ sont orthogonaux deux à deux ($N^\circ 4$), donc A est orthogonal à tous les groupoïdes du complexe $A \circ K$. La démonstration est la même pour $K \circ A$. Si G est un semi-groupe, A sera orthogonal à $B \circ A^\alpha$, quel que soit α , entier.

10. Diviseurs. Il est évident que si deux groupoïdes orthogonaux ont un diviseur commun, les deux sous groupoïdes correspondants à ce diviseur sont encore orthogonaux.

Par exemple, le système orthogonal du $N^\circ 1$, défini sur le corps des réels et où a, b, c, d sont supposés rationnels, a pour diviseur le système orthogonal, représenté par les mêmes équations, sur le corps des nombres rationnels.

11. Le produit direct de deux systèmes orthogonaux est un système orthogonal.

Il faut entendre par là que si $S = A(\cdot)$, $B(\times)$ et $S' = A'(\circ)$, $B'(*)$ sont ces deux systèmes, les produits direct AA' et BB' sont encore orthogonaux. La proposition résulte immédiatement de la définition du produit direct et on la vérifie par un calcul facile. On pourra donc, dans le cas fini, construire des systèmes orthogonaux d'ordre quelconque comme produits directs de systèmes d'ordre premier. En particulier, on pourra construire des quasigroupes orthogonaux d'ordre composé.

Réciproquement, tout système bicancellable fini d'ordre composé est-il isotope ([1], p. 696) au produit de deux systèmes orthogonaux? La réponse est négative. Il n'existe aucun système orthogonal cancellable d'ordre 2, alors que, pour $n = 4$ on trouve des quasigroupes orthogonaux.

On vérifie aussi que les produits directs de deux groupoïdes orthogonaux par un troisième, ne se réduisant pas à $x \circ y = \text{Constante}$, ne sont pas orthogonaux.

II. Groupoïdes isonomes.

12. Transformation T^* sur l'ensemble produit. Soit $G(\cdot)$ un groupoïde défini sur un ensemble E et soient $(x, y), (x', y'), (x'', y''), \dots$ les éléments de l'ensemble produit E^2 . Dans le groupoïde G , à chacun de ces couples correspond un élément de E qui est le produit $x \cdot y$. Faisons une transformation de E^2 en lui-même, c'est-à-dire une application biunivoque de E^2 sur lui-même. Soit (x_1, y_1) l'image de (x, y) dans cette transformation, alors, si

$x \cdot y = m$, après la transformation T , on aura obtenu un nouveau groupoïde $G_1(\times)$ tel que :

$$x_1 \times y_1 = m.$$

Si deux groupoïdes sont orthogonaux, les images de ces groupoïdes par une même transformation T seront encore orthogonales.

Soient $A(\cdot)$ et $B(\oplus)$ deux groupoïdes orthogonaux et soient $C(\times)$ et $D(*)$ leurs images par T . Alors, si :

$$x \cdot y = m = z \cdot t \quad \text{et} \quad x \oplus y = p, \quad z \oplus t = q,$$

on aura, en appelant (x_1, y_1) et (z_1, t_1) les images par T de (x, y) et de (z, t) :

$$x_1 \times y_1 = m \quad \text{et} \quad x_1 * y_1 = p$$

$$z_1 \times t_1 = m \quad \text{et} \quad z_1 * t_1 = q.$$

Comme A et B sont orthogonaux, $p = q \implies x = z, y = t$, donc aussi $x_1 = z_1$ et $y_1 = t_1$. Donc C et D sont orthogonaux.

En particulier,

13. *Si deux quasigroupes sont orthogonaux, leurs images par une isotopie quelconque, ou par une isométrie ([4], p. 8), sont encore des quasigroupes orthogonaux.*

Par ce moyen, on pourra donc, dans la recherche des groupoïdes orthogonaux à un groupoïde donné G , transformer G en un groupoïde particulier ($x \cdot y = x + y$, ou $x \cdot y = y$). Exemple : On prend pour G le groupe cyclique C du 4^e ordre. Il est orthogonal à $B(\times)$: $x \times y = y$. En multipliant C par B , au moyen d'un quasigroupe quelconque, d'après la règle du N° 4, tous les groupoïdes obtenus seront orthogonaux à C .

14. Isotopies. Si $A(\cdot)$ et $B(\times)$ sont deux groupoïdes orthogonaux sur l'ensemble E , leurs images par les isotopies respectives (ξ, η, ζ) et (ξ, η, ζ') sont encore orthogonales.

Soit T l'application biunivoque de E sur lui-même telle que $\zeta' = \zeta T$. Les isotopes de A et B par (ξ, η, ζ) étant orthogonaux (N° 13), il suffit de montrer que l'isotope de B par $(1, 1, T)$ est orthogonal à A . Or soit : $x \times y = v$ et $C(*)$ l'image de B par $(1, 1, T)$. On aura :

$$x * y = v T.$$

Si maintenant $z \times t = v$, on aura : $z * t = v T$, donc :

$$x \times y = z \times t \implies x * y = z * t.$$

Par suite, A et B étant orthogonaux, :

$$x \cdot y = z \cdot t \quad \text{et} \quad x * y = z * t \implies x = y \quad \text{et} \quad z = t.$$

En particulier,

15. Si $f(x)$ et $g(x)$ sont deux transformations quelconques de E en lui-même, les deux groupoïdes $x \cdot y = f(x)$ et $x \times y = g(y)$ sont orthogonaux entre eux et à tout groupoïde cancellable $G(*)$ construit sur E .

Car $x \cdot y = z \cdot t$ et $x \times y = z \times t \iff x = z$ et $y = t$.

De même $x \cdot y = z \cdot t$ et $x * y = z * t \iff x = z$, et puisque G est cancellable, $y = t$.

Si l'on peut trouver une transformation commune T qui fasse de $(\cdot)$ et $(\times)$ deux quasigroupes, on aura construit un système orthogonal de deux quasigroupes.

16. Définition. Un groupoïde $G(\cdot)$, défini sur un ensemble E , est isonome s'il existe une partition de son ensemble produit E^2 en classes K_m , $((x, y) \in K_m \text{ si } x \cdot y = m; m, x, y \in E)$ de même puissance que E , appelées classes d'isonomie.

Tout quasigroupe est isonome. Sur l'ensemble des entiers naturels le semi-groupe multiplicatif $f(x, y) = xy$ n'est pas isonome.

17. S'il existe, sur un groupoïde isonome $G(\cdot)$ une partition régulière P dont les blocs (mod. P) aient même puissance, p , finie le groupoïde quotient G/P est isonome. Si G est fini, d'ordre n , les classes d'isonomie de G/P sont d'ordre n/p .

Soit E l'ensemble des éléments (X, Y) de l'ensemble produit $(G/P)^2$ tels que $X \times Y = Z$, où $(\times)$ est l'opération du groupoïde quotient G/P .

Si $x \in X$, $y \in Y$, alors $x \cdot y \in Z$. Soit z un élément quelconque de Z . Tous les éléments (x, y) de l'ensemble produit G^2 tels que $x \cdot y = z$ sont contenus dans E . Soit:

$$z_1, z_2, z_3, \dots, z_i, \dots, z_p$$

le bloc Z . Soit:

$$K^1 = (x_1^1, y_1^1), (x_2^1, y_2^1), (x_3^1, y_3^1), \dots, (x_i^1, y_i^1) \dots$$

l'ensemble des éléments de G^2 tels que $x_i^1 \cdot y_i^1 = z_1$,

$$K^2 = (x_1^2, y_1^2), (x_2^2, y_2^2), (x_3^2, y_3^2), \dots, (x_i^2, y_i^2), \dots$$

l'ensemble des éléments G^2 tels que $x_i^2 \cdot y_i^2 = z_2$, etc, les indices inférieurs des (x, y) ne signifiant pas que les K^j soient dénombrables. Par hypothèse, tous ces ensembles ont même puissance puisque G est isonome. L'ensemble F des éléments (x_i^j, y_i^j) de toutes ces classes d'isonomie K^j a même puissance que l'ensemble produit GZ , car chacune des classes K a même puissance que G et l'ensemble des K a même puissance que Z . Donc F a même puissance que l'ensemble produit GZ .

Mais les éléments de G^2 contenus dans (X, Y) forment un ensemble dont la puissance est celle de l'ensemble produit Z^2 . Donc, finalement, les ensembles produits Z^2E et GZ ont même puissance, donc aussi ZE et G , puisque Z est fini. Mais tous les blocs X, Y, Z ont même puissance finie, p ; il en résulte que E a même puissance quel que soit le bloc Z , autrement dit, G/P est isonome. Si G est fini, E aura pour puissance n/p , ordre de G/P .

18. Pour qu'il existe un groupoïde orthogonal à un groupoïde donné $A(\cdot)$, il suffit que A soit isonome.

Preuve. Soit K_m la classe des éléments de A^2 pour lesquels $x \cdot y = m$. Les ensembles A et K_m ayant même puissance, il existe une application biunivoque de K_m sur A :

$$((x, y) \rightarrow z), \quad (x, y) \in K_m, \quad z \in A.$$

On peut donc construire une transformation T ($N^\circ 12$) de A^2 en lui-même qui donne naissance à un nouveau groupoïde $A(\times)$ tel que $x \times y = y$, quels que soient x et y . En effet, soit L_m l'ensemble des éléments (x, m) de A^2 où m a la valeur constante qui définit K_m et où x parcourt tout le champ A , symboliquement (A, m) . Les ensembles K_m et (A, m) ont même puissance. On peut donc appliquer biunivoquement K_m sur L_m . Dans le nouveau groupoïde, $A(\times)$, on aura donc $x \times m = m$, et, cela pouvant être fait quel que soit $m \in A$, on a $x \times y = y$ pour tous $x, y \in A$.

Mais $A(\times)$ est évidemment orthogonal à $A(*) : x * y = x$. Opérant sur $A(\times)$ et $A(*)$ la transformation inverse T^{-1} , $A(*)$ deviendra un groupoïde orthogonal à $A(\cdot)$, ($N^\circ 12$).

19. Si T est la transformation ($N^\circ 12$) de A^2 qui remplace le groupoïde isonome $A(\cdot)$ par le groupoïde $x \times y = y$, l'ensemble des groupoïdes orthogonaux à A est BT^{-1} , où $B(*)$ est un groupoïde quelconque, cancellable à droite, sur l'ensemble A .

Tout groupoïde orthogonal à $A(\cdot)$ peut être construit par la méthode du N° précédent. Pour trouver tous les groupoïdes orthogonaux à A , il suffit de chercher ceux qui sont orthogonaux à $x \times y = y$. Or, $x \times y = z \times t$ implique $y = t$, d'où :

$$x \times y = z \times y \quad \text{et} \quad x * y = z * y, \implies x = z$$

ce qui exprime que $B(*)$ est cancellable à droite.

20. Dans tout système orthogonal E , chaque classe $K_m ((x, y) \in K_m \text{ si } x \cdot y = m)$ a une puissance inférieure ou égale à celle de E .

Soient $A(\cdot)$ et $B(\times)$ deux groupoïdes orthogonaux définis sur E . Considérons la classe :

$$K_m : x \cdot y = m, \quad x' \cdot y' = m, \quad x'' \cdot y'' = m, \dots$$

et l'ensemble

$$\beta: x \times y = b, x' \times y' = b', x'' \times y'' = b'', \dots$$

Ce dernier a même puissance que K_m et d'autre part tous ses éléments sont inégaux car, à cause de l'orthogonalité de A et de B :

$$x \cdot y = x' \cdot y' \text{ et } x \times y = x' \times y' \text{ entraînerait } x = x', y = y'.$$

Donc K_m a même puissance que l'ensemble $\beta' = b, b', b'', \dots$ et celui-ci est contenu dans E . Il en résulte que la puissance de K_m est au plus égale à celle de E .

Si A et B sont des quasigroupes, ils sont évidemment isonomes.

21. *Pour qu'un groupoïde fini G admette un groupoïde orthogonal il faut et il suffit que G soit isonome. Tout quasigroupe (fini ou non) admet un groupoïde orthogonal (qui n'est pas forcément un quasigroupe).*

1° D'après le N° 18, la condition est suffisante.

2° Si E est fini, la condition nécessaire du N° 20 exprime que K_m est équivalente à E car dans toute partition d'un ensemble de n^2 éléments en n classes d'ordres inférieurs ou égaux à n , chaque classe est d'ordre n .

22. *Si un système orthogonal cancellable admet une partition régulière, dont les blocs soient finis, alors le système quotient est orthogonal.*

Soit un système orthogonal cancellable $A(\cdot), B(\times)$, construit sur l'ensemble E ; soit p l'ordre des blocs définis par une partition régulière P et $(\circ), (\oplus)$ les opérations des deux groupoïdes quotients, définis sur E/P . Enfin;

$$(1) \quad \begin{cases} X \circ Y = Z = X' \circ Y' \\ X \oplus Y = T = X' \oplus Y' \end{cases}$$

où X, Y, Z, T, X', Y' sont des blocs (mod P). Nous allons montrer que les égalités (1) sont incompatibles avec:

$$(X, Y) \neq (X', Y').$$

Considérons les ensembles produits $F = E^2, F' = (E/P)^2$. Le système A, B étant cancellable, dans l'élément $(X, Y) \in F'$, le nombre des éléments $(x, y) \in F$ tels que $x \cdot y = m$ ($m \in Z$) est p . Et puisque $X \circ Y = X' \circ Y'$, il en est de même dans l'élément $(X', Y') \in F'$; soit en tout $2p$ pour (X, Y) et (X', Y') réunis. Considérons, pour chacun de ces $2p$ éléments (x, y) la valeur de $x \times y$. Puisque $X \oplus Y = X' \oplus Y' = T, x \times y \in T$. Mais comme T contient seulement p éléments, pour les $2p$ éléments (x, y) tels que $x \cdot y = m$, la valeur de $x \times y$ parcourt seulement p valeurs inégales. Il y en a au moins une qui est obtenue plus d'une fois. Il existera donc des éléments distincts de $F: (x, y), (x', y')$ tels que: $x \times y = x' \times y'$. On aura donc à la fois

$x \cdot y = x' \cdot y'$ et $x \times y = x' \times y'$, ce qui est impossible puisque A et B sont orthogonaux. Ainsi (1) est incompatible avec $(X, Y) \neq (X', Y')$ et le système quotient est bien orthogonal.

23. Remarques. Si les blocs ne sont pas finis, la proposition précédente n'est pas vraie en général, car un ensemble infini peut avoir même puissance qu'une de ses parties. Exemple:

Sur l'ensemble $\mathbb{Z}$ des entiers rationnels,

$$A(\cdot): x \cdot y = 2x + 3y$$

est bicancellable. La partition (mod 3) est régulière, les cosets sont les classes résiduelles (mod 3). Le groupoïde quotient $A/3$ est: $X \circ Y = 2X$. Ce n'est pas un quasigroupe. Sur l'anneau $\mathbb{Z}$, le groupoïde $B(\times): x \times y = x - 3y$ est orthogonal à A . Son groupoïde quotient $B/3: X \oplus Y = X$ n'est pas orthogonal à $A/3$.

Contre exemple. Soit le système orthogonal, sur le corps $\mathbb{Q}$ des fractions rationnelles:

$$(S) \quad \begin{aligned} A(\cdot): x \cdot y &= ax + by \\ B(\times): x \times y &= cx + dy \end{aligned}$$

a, b, c, d, n, k entiers, $a, b, c, d, ad - bc$ premiers avec n . Le module n définit sur chaque quasigroupe A et B une partition régulière dont les classes sont composées des fractions x' telles que $x - x'$ soit un multiple entier de n . Représentons chaque classe par son résidu minimum positif x , ($0 \leq x < n$).

Si $ax' + by' = z'$ et si $x' \equiv x, y' \equiv y$, on a: $z = ax + by = a(x' + kn) + b(y' + k'n) = ax' + by' + k'n \equiv z'$. C'est-à-dire: $x \cdot y \equiv x' \cdot y'$ et de même $x \times y \equiv x' \times y'$.

Les groupoïdes quotients sont des quasigroupes car la congruence: $ax + by \equiv z \pmod{n}$, où a et b sont premiers avec n , détermine univoquement l'une quelconque des inconnues x, y, z en fonction des deux autres. Enfin, le système quotient (mod n) est encore orthogonal, car les conditions:

$$\begin{aligned} & \begin{cases} ax + by \equiv az + bt \\ cx + dy \equiv cz + dt \end{cases} \pmod{n} \\ \text{impliquent: } & \begin{cases} a(x - z) + b(y - t) \equiv 0 \\ c(x - z) + d(y - t) \equiv 0 \end{cases} \pmod{n} \\ & (ad - bc)(x - z) \equiv 0 \pmod{n} \end{aligned}$$

et puisque $(ad - bc, n) = 1$, $x - z \equiv 0$, $x \equiv z$, et de même $y \equiv t$.

En revanche, si $(ad - bc, n) = D \neq 1$, les mêmes conditions entraînent seulement $x = z + kn/D$, et le système quotient n'est plus orthogonal.

Bibliographie.

- [1] A. A. ALBERT, Non associative Algebras I. — Fundamental concepts and isotopy, *Annals of Math.* **43** (1942), 685–707.
- [2] C. JORDAN, Traité des substitutions, *Paris*, 1870.
- [3] O. ORE, Theory of equivalence relations, *Duke Math. J.* **9** (1942), 573–627.
- [4] A. SADE, Quasigroupes, *Marseille*, 1950.
- [5] J. B. SHAW, On parastrophic algebras, *Trans. Amer. Math. Soc* **16** (1915), 361–370.

(Reçu le 15 juin 1957.)