MATHÉMATIQUES ET SCIENCES HUMAINES

B. MONJARDET

II. Quasi-groupes finis, quasi-groupes orthogonaux, ensemble complet orthogonal

Mathématiques et sciences humaines, tome 19 (1967), p. 13-20

<http://www.numdam.org/item?id=MSH_1967__19__13_0>

B. MONJARDET

II

QUASI-GROUPES FINIS
QUASI - GROUPES ORTHOGONAUX
ENSEMBLE COMPLET ORTHOGONAL

3. 1. Définitions. Exemples

On appelle quasi-groupe un ensemble E muni d'une opération binaire $\perp$ telle que pour tout couple (a,b) d'éléments de E, les équations

$$x \perp a = b \qquad a \perp y = b$$

ont des solutions uniques; le quasi-groupe sera noté $(E, \perp)$. Le cardinal de E s'appelle l'ordre n du quasi-groupe. Nous ne considèrerons ici que des quasi-groupes d'ordre fini; un tel quasi-groupe peut être donné par la table de son opération. Si l'on considère une ligne de cette table, elle ne contiendra que des éléments distincts (Pourquoi ?) et donc tous les éléments de E; de même pour une colonne. Donc cette table constitue un tableau carré de n^2 éléments de E, tel que dans chaque ligne et chaque colonne figure une fois, et une seule, tout élément de E,: un tel tableau s'appelle un carré latin (de côté n).

Dans le cas particulier où la loi est associative, le quasi-groupe est alors un groupe (le montrer en exercice - cf. aussi à ce propos, la note de la page 62, Mathématiques et Sciences Humaines n° 17).

Donnons quelques exemples pour $n = 2, 3, 4$.

$n = 2$

	a	b
a	a	b
b	b	a

	a	b
a	b	a
b	a	b

Ce sont évidemment les deux seules tables possibles.

* $n = 3$

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

I

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

II

	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

III

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

IV

	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

V

la table I est celle du groupe cyclique d'ordre 3; les tables II et III sont celles de quasi-groupes non associatifs; par exemple, pour II (b b) a $\neq$ b (b a).

n = 4

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

A

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

B

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	a	b

C

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

D

	a	b	c	d
a	a	b	c	d
b	c	d	a	b
c	d	c	b	a
d	b	a	d	c

E

	a	b	c	d
a	a	b	c	d
b	d	c	b	a
c	b	a	d	c
d	c	d	a	b

F

On remarque que dans les 4 tables A, B, C, D, la lère ligne et la lère colonne reproduisent a, b, c, d, dans cet ordre; le carré latin correspondant est dit sous forme normale; on montrera aisément qu'il n'existe pas d'autre carré latin d'ordre 4 sous forme normale.

Les lois définies par les tables A et D sont bien connues. Quelles sont-elles ? (respectivement: groupe cyclique d'ordre 4, groupe de Klein).

Les lois correspondant aux tables B et C ne sont pas associatives, mais ont un élément neutre; ce sont des lois de boucles.

3. 2 Isomorphisme - Isotopie

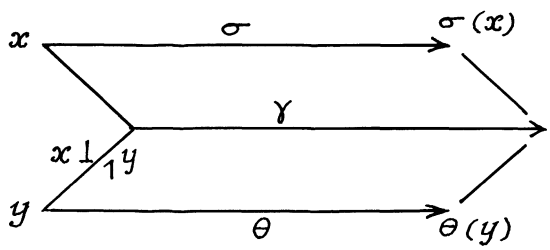
Deux quasi-groupes $(E, \perp_1)$, $(E, \perp_2)$ sont isomorphes s'il existe une permutation σ de E telle que:

$$\sigma\ (x \perp_1 y) = \sigma\ (x) \perp_2 \sigma\ (y), \qquad \forall\ (x, y) \in E^2$$

Par exemple les deux quasi-groupes d'ordre 3, I et V sont isomorphes (par quelle permutation ?); les carrés latins correspondants, définissent donc le même quasi-groupe.

Dans l'ensemble des carrés latins de format n, on pourra introduire l'équivalence: "définir deux quasi-groupes isomorphes". On utilise aussi une équivalence plus forte: deux carrés latins sont alors équivalents s'ils se déduisent l'un de l'autre par permutations de lignes, de colonnes ou d'éléments. Pour les quasi-groupes, ceci correspond à la relation d'isotopie: deux quasi-groupes $(E, \perp_1)$, $(E, \perp_2)$ sont isotopes, s'il existe trois permutations σ , θ , γ de E telles que:

$$\gamma\ (x \perp_1 y) = \sigma\ (x) \perp_2 \theta\ (y) \ ; \ \forall\ (x,y) \in E^2$$



$\gamma\ (x \perp_1 y) = \sigma\ (x) \perp_2 \theta\ (y)$

L'isomorphie est un cas particulier d'isotopie avec $\sigma = \gamma = \theta$

Un autre cas particulier, est celui où on opère uniquement une permutation des lignes de la table du quasi-groupe ($\gamma = \theta$ = permutation identique); les quasi-groupes correspondants sont dits isotopes - D_0 ; si seule γ est égale à la permutation identique, l'isotopie est dite principale.

On montrera facilement qu'il existe 12 carrés latins de côté 3, correspondant à 4 quasi-groupes non isomorphes (I, II, III et IV), mais tous isotopes.

(Par exemple, I et III sont isotopes par permutations des colonnes a et c et des éléments b et c).

Pour n = 4, il existe 566 carrés latins dont 4 sont sous forme normale (566 = 4 x 4! x 3!); mais il n'existe que deux classes d'isotopies correspondants aux deux groupes d'ordre 4.

Pour n = 5, il existe 56 carrés latins sous forme normale et deux classes d'isotopie.

Pour n = 6, on a 9.408 carrés latins normaux, 17 classes d'isotopie (Résultat de Tarry - 1900).

Pour n = 7, 16.942.080 carrés latins normaux, 147 classes d'isotopie (Norton et Sade 1951).

Pour n > 7, ces nombres ne sont pas connus.

Nous verrons ultérieurement une représentation géométrique d'un quasi-groupe qui permettra d'interpréter l'isotopie comme une invariance de propriétés géométriques.

3. 3 Quasi-groupes orthogonaux

Soient $E\ (\perp_1)$ et $E\ (\perp_2)$, deux quasi-groupes d'ordre n définis sur le même ensemble E.

Considérons le système d'équations:

$$\begin{cases} x \perp_1 y = a \\ x \perp_2 y = b \end{cases}$$

Si pour tout couple (a, b) de E^2 ce système admet une solution unique, on dira que les deux quasi-groupes $E\ (\perp_1)$ et $E\ (\perp_2)$ sont orthogonaux.

Cette propriété peut s'interpréter ainsi: superposons les deux tables des quasi-groupes $E\ (\perp_1)$ et $E\ (\perp_2)$; dans la table ainsi obtenue, tous les couples d'éléments de E figurent une fois, et une seule. Le tableau correspondant est dit carré gréco-latin d'ordre n.

Par exemple, pour n = 3, les tables I et II précédentes nous donnent le carré gréco-latin suivant (on a remplacé les lettres de II par des lettres grecques):

a α	b β	c γ
b γ	c α	a β
c β	a γ	b α

La notion d'orthogonalité s'étend à plusieurs quasi-groupes. On dira que t quasi-groupes d'ordre n sont mutuellement orthogonaux, s'ils sont orthogonaux deux à deux; superposons les tables de ces t quasi-groupes; dans la table ainsi obtenue deux t-uplets d'éléments de E n'ont jamais deux mêmes composantes.

Le nombre t de quasi-groupes mutuellement orthogonaux (q.g.m.o.) d'ordre n, est limité.

Exercice 7

Montrer que $t \leqslant n - 1$

Un ensemble de n - 1 quasi-groupes orthogonaux d'ordre n est appellé un ensemble complet orthogonal d'ordre n.

Par exemple, pour n = 3, le carré gréco-latin précédent définit un ensemble complet. Pour n = 4, les quasi-groupes D, E, F du paragraphe précédent forment un ensemble complet.(le vérifier et montrer qu'il n'en est pas de même pour les quasi-groupes A,B, C).

Ces définitions posées, un certain nombre de problèmes se présentent. Posons $N(n)$ = nombre maximum de q.g.m.o. d'ordre n. On sait déjà que $N(n) \leqslant n - 1$.

On cherche à déterminer les valeurs de n pour lesquelles $N(n) = n - 1$; dans ce cas, il existe un ensemble complet orthogonal mais il faut se demander s'il en existe plusieurs non équivalents, de même ordre.

Plus généralement, on cherche des bornes inférieures ou supérieures pour $N(n)$. Ainsi, on peut se demander si $N(n) \geqslant 2$ pour tout n ; autrement dit s'il existe un carré gréco-latin pour toute valeur de n.

Cette dernière question a toute une histoire qui remonte à EULER. En 1780, celui-ci se pose le problème des 36 officiers:

Soit une assemblée de 36 officiers de 6 grades et de 6 régiments différents; peut-on les ranger dans un carré de telle sorte que dans chaque ligne et dans chaque colonne, les six officiers qui y sont rangés, soient de grades et de régiments différents ? ou encore existe-t-il un carré gréco-latin d'ordre 6 ?

EULER concluait, sans démonstration, à l'impossibilité de ce dispositif et il en tirait une conjecture: il est impossible de trouver un carré gréco-latin d'ordre $n = 4t + 2$ (pour tout $t \geqslant 1$).

La question fut reprise après EULER; on montra facilement que pour $n \neq 4t + 2$, il existe un carré gréco-latin; d'autre part en 1900, TARRY démontra l'impossibilité pour $n = 6$ par une méthode d'énumération complète;

On essaya alors de prouver la conjecture d'EULER et certains crurent même l'avoir démontrée. En fait, cette conjecture a été reconnue fausse récemment; en 1959-1960 BOSE, PARKER et SHRIKHANDE montraient au contraire que pour toute valeur de n de la forme $4t + 2$, $(t > 1)$. on peut construire un carré gréco-latin. Finalement pour toute valeur de n différente de 2 ou 6, il existe deux quasi-groupes orthogonaux.

Signalons encore un résultat récent sur $N(n)$ établi par CHOWLA, ERDOS et STRAUS en 1960: $N(n)$ augmente indéfiniment avec n : et renvoyons à la bibliographie pour une étude plus approfondie.

Dans le dernier paragraphe, nous allons montrer comment on peut construire certains ensembles complets de q.g.m.o. au moyen de structures algébriques introduites précédemment: corps de Galois, quasi-corps, presque-corps.

3.4. Construction d'ensembles complets de quasi-groupes mutuellement orthogonaux

Soit $(K, +, o)$ un corps, un quasi-corps ou un presque corps d'ordre n ; la loi $+$ est une loi de groupe abelien: la loi o est au moins une loi de boucle; K vérifie en particulier la propriété suivante:

Le système d'équations

$$(2) \quad \begin{cases} y = a_1 \; ox + b_1 & \text{avec} \quad a_1 \neq a_2 \\ y = a_2 \; ox + b_2 & \text{avec} \quad b_2 \neq b_2 \end{cases}$$

admet une solution et une seule (x, y).

On peut définir sur l'ensemble K, n - 1 opérations binaires ϕ_i de la façon suivante:

Soit x_i un élément de K différent de zéro, on pose

$$a \ \phi_i \ b = aox_i + b \qquad \forall a, b \in K$$

En particulier si x_1 est l'élément unité pour o de K, on a:

$$a \ \phi_1 \ b = a + b$$

et ϕ_1 est la loi $+$ de K.

D'autre part ϕ_i est une loi de quasi-groupe, quelque soit i; en effet, la loi o étant une loi de boucle, l'application $a \longrightarrow aox_i$ est une permutation σ_i de K; la table de ϕ_i est donc la table obtenue par la permutation σ_i des lignes de la table $+$; autrement dit (K, ϕ_i) est un quasi-groupe isotope D_o à $(K, +)$.

On obtient ainsi n - 1 quasi-groupes, isotopes - D_o; montrons qu'ils forment un ensemble complet orthogonal. Soient (K, ϕ_i) et (K, ϕ_j) deux tels quasi-groupes, il faut montrer qu'ils sont orthogonaux, c'est-à-dire que pour tout couple (y_1, y_2) de K^2 le système:

$$\begin{cases} a \ \phi_i b = aox_i + b = y_1 \\ a \ \phi_j b = aox_j + b = y_2 \end{cases}$$

admet une solution unique (a,b); ce résultat provient de la propriété (2) rappellée au début du paragraphe. On a donc la proposition suivante:

Proposition A tout corps, quasi-corps ou presque-corps d'ordre n, est associé un ensemble complet orthogonal d'ordre n.

On a vu que l'ordre n d'un corps, d'un presque-corps ou d'un quasi-corps est de la forme $n = p^r$; p premier, r quelconque. On peut donc construire des ensembles complets orthogonaux pour tous les nombres de cette forme; mais pour $n \neq p^r$ existe-t-il des ensembles complets orthogonaux ? Pour n = 6, puisqu'il n'existe pas de quasi-groupes orthogonaux, la réponse est négative; on connait d'autres valeurs de n pour lesquelles il n'existe pas d'ensemble complet orthogonal; mais pour une infinité de valeurs de n, commençant par n = 10, on ignore actuellement s'il existe ou non un ensemble complet orthogonal. Nous préciserons ces résultats dans un article ultérieur sur les géométries finies.

Exemple:

Le corps K_4 à 4 éléments $\{0, 1, 2, 3\}$ a les tables d'opérations suivantes:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

x	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

D'où deux autres quasi-groupes:

	ϕ_2	0	1	2	3
$0 \times 2 =$	0	0	1	2	3
$1 \times 2 =$	2	2	3	0	1
$2 \times 2 =$	3	3	2	1	0
$3 \times 2 =$	1	1	0	3	2

	ϕ_3	0	1	2	3
$0 \times 3 =$	0	0	1	2	3
$1 \times 3 =$	3	3	2	1	0
$2 \times 3 =$	1	1	0	3	2
$3 \times 3 =$	2	2	3	0	1

On obtient ainsi, l'ensemble complet orthogonal d'ordre 4 déjà cité en exemple (quasi-groupes D, E, F)

Exercices:

8. - Construire un ensemble complet orthogonal d'ordre 3, d'ordre 5.

9. - Construire deux ensembles complets orthogonaux non équivalents d'ordre 9 (on utilisera le corps K_9 et le quasi-corps à 9 éléments étudiés aux exercices 4 et 6 de l'article précédent).

NOTE BIBLIOGRAPHIQUE

III

QUASI-GROUPES FINIS, CARRES LATINS ENSEMBLES COMPLETS ORTHOGONAUX

Sur les quasi-groupes ou les boucles et leurs relations avec les configurations géométriques, il faut consulter:

R.H. BRUCK A survey of binary systems - Springer 1958.

R.H. BRUCK What is a loop ? dans Studies in Modern Algebra (A.A. Albert, Ed) The A.M.S. 1963, 59-100

Voir aussi la bibliographie du chapitre 1 de la thèse de R. GUERIN (cf. plus bas).

Sur les carrés latins, l'historique et l'état des problèmes en 1939, on peut se reporter à:

NORTON "The 7 × 7 Squares" Ann Eugenics London, vol 9 (1939) part III, p. 268-307.

Signalons que la démonstration de TARRY, de l'impossibilité du problème des 36 officiers, se trouve dans C.R. Ass. Fr. Avancement des Sciences, 1900, p. 122-123; 1901, p. 170-203.

On trouve des exposés récents, plus ou moins succincts dans différents livres ou articles sur les problèmes combinatoires:

A survey of combinatorial analysis - M. HALL J.R. dans Some aspects of analysis and Probability - New-York, John Wiley and Sons, 1958.

H.J. RYSER Combinatorial Mathematics, John Wiley and Sons, 1963 (voir particulièrement le chap. 7).

M. HALL Jr Block designs, chap. XIII de Applied Combinatorial Mathematics, John Wiley and Sons, 1964 (les diverses méthodes de constructions sont assez développées).

Un exposé de synthèse mais de caractère nettement plus algébrique se trouve dans l'article suivant:

J.R. BARRA Carrés latins et eulériens - Revue de l'Institut International de Statistique. Vol. 33 - 1 - 1965.

Enfin dans la thèse suivante, on trouvera une excellente synthèse de tous les travaux récents sur la question, avec la bibliographie correspondante.

R. GUERIN Existence et propriété des carrés latins orthogonaux. Publications Institut de Statistique Université de Paris (1966), p. 113-213.

Tous les aspects possibles sont abordés dans un langage algébrique clair. Nous donnons ici un bref résumé du 1er chapitre qui traite des "aspects algébriques et propriétés des carrés latins mutuellement orthogonaux". L'accent est mis sur l'étude d'ensembles complets de q.g.m.o. isotopes - D_o à un groupe abélien fini $(E, +)$; si l'on explicite les conditions d'isotopie D_o et d'orthogonalité, on aboutit naturellement à la notion d'orthomorphisme θ de E : θ est une permutation de E telle que l'application $\theta(x) - x$ soit aussi une permutation. On définit alors les notions d'orthomorphismes orthogonaux, d'ensembles complets d'orthomorphismes; il ne reste plus qu'à étudier les propriétés de tels orthomorphismes d'un groupe abélien et les conditions d'existence. On montre en particulier que l'existence d'un ensemble complet d'orthomorphismes orthogonaux du groupe abélien E (donc d'un ensemble complet de q.g.m.o. isotopes - D_o à E) est équivalente à la possibilité de définir dans E une deuxième opération o vérifiant certaines propriétés*, les orthomorphismes sont des automorphismes de $(E, +)$ si, et seulement si, o est distributive par rapport à +; les ensembles complets correspondants aux corps de Galois, aux quasi-corps ou aux presque-corps se déduisent immédiatement de ce résultat.

(A suivre)

* Cette seconde opération o est, en particulier, une loi de boucle.