GROUPOÏDES AUTOMORPHES PAR LE GROUPE GÉOMÉTRIQUE ET QUASIGROUPES "ENDO"

A. SADE

ARGUMENT

L'ensemble des nombres $\in Z/n$, premiers avec l'entier n, forme un groupe (le groupe géométrique) G, par rapport à la multiplication. Etant donné un ensemble de nombres réels, M, un groupoïde Q, formé d'éléments quelconques, x, est automorphe par le groupe géométrique si (i) pour tout élément $x \in Q$ et tout nombre $m \in M$, la multiplication xm est définie; (ii) l'application $(x \rightarrow xm)$ est un automorphisme de Q.

Si M devient un semi-groupe, fini ou non, et l'application $(x \rightarrow xm)$ un endomorphisme, le groupoïde Q est dit "*endo.*"

La première partie expose les diverses généralisations ou restrictions de ces définitions: anneaux, clusters **(6)**, narings **(16)**, néofields **(10)**, keys **(19)**, groupes distributifs de Burstin-Mayer, en donne des illustrations et montre la corrélation de ces ensembles algébriques avec les groupoïdes automorphes par le groupe cyclique **(12)**.

La troisième partie est consacrée aux diviseurs des "endo." La quatrième concerne leur composition, leur décomposition en p-quasigroupes, leur structure. Les "endo" jouissent de propriétés élégantes qui s'abâtardissent en se transmettant aux groupoïdes qui sont seulement automorphes par le groupe géométrique. La deuxième partie, dont la lecture n'est pas indispensable à l'intelligence des autres, traite de ces derniers pour n fini et, avec une restriction sur la parité de k, des diviseurs formés par les multiples de k.

Dans la dernière section, la construction des p-quasigroupes est ramenée à celle des "endo" d'ordre premier.

I. GÉNÉRALITÉS

1. Notations et définitions. Nous utiliserons les symboles suivants: $a \Rightarrow b$, implication, a entraîne b. $a \leftrightarrows b$, a entraîne b et b entraîne a. $a \rightarrow b$, a est appliqué sur b. $\times$, $\cdot$, $*$, $\wedge$, $\ominus$, $\oplus$, $\circ$, $\odot$, signes d'opérations. Min (a, b), le plus petit des nombres a et b. $a \cong b$, a isomorphe à b. $a|b$, a divise b. $\{a\}$, groupoïde engendré par a. $\exists$, quantificateur existentiel. R, corps des nombres réels. Q, corps des fractions rationnelles. Z, anneau des entiers rationnels. Z/n, anneau des classes résiduelles modulo n.

DÉFINITION. *Un groupoïde* **(8)**, $G(\times)$ *est automorphe par le groupe géométrique s'il existe un ensemble de nombres réels, M, tel que, pour tout* $m \in M$ *et pour*

Reçu le 16 août 1956.

tout élément $x \in G$ (i) *la multiplication de cet élément par* m *soit définie* (ii) *l'application* $(x \to xm)$ *soit un automorphisme.*

L'ensemble de ces applications est donc un diviseur de l'automorphe $\mathbf{A}_G$ **(15,** *p.* 40**)** et par conséquent M est un groupe par rapport à la multiplication usuelle des nombres. Le vocable choisi tire son origine du fait que, si G est fini d'ordre n, l'ensemble M sera le groupe multiplicatif, modulo n, des $\phi(n)$ entiers inférieurs à n et premiers avec lui, auquel Cauchy **(4,** *p.* 233**)** a donné le nom de groupe géométrique.

Exemple I. Le groupe des translations, le groupe des homothéties dans l'espace usuel, sont automorphes par le groupe multiplicatif de **R.**

Exemple II. Le quasigroupe du $6^{\text{ème}}$ ordre $R = \{0, 1, \ldots, 5\}$ défini par les substitutions: $S_0 = (15)$, $S_1 = (05234)$, $S_2 = (0241)(35)$, $S_3 = (03)(12)(45)$, $S_4 = (0425)(13)$, $S_5 = (01432)$, où S_i détermine la translation $(x \to x \times i)$, est automorphe par $(x \to xm)$, $m = 1$ et 5.

Contre-exemple. L'ensemble $G(\wedge)$ des vecteurs libres dans l'espace à trois dimensions est un groupoïde par rapport au produit vectoriel. Mais G n'est automorphe par aucun groupe géométrique, car:

$$\mathbf{V}m \wedge \mathbf{V}'m = (\mathbf{V} \wedge \mathbf{V}')m^2$$

Exemple III. Un groupoïde peut être automorphe par une partie seulement du groupe géométrique. Ainsi le quasigroupe Q ($\times$), **(12,** N°1**)**, dont la loi de composition est, sur $Z/9$:

$$x \times y = 2x - y + 3, \text{ si } x - y - 2 \text{ est premier avec 3 et}$$
$$x \times y = 2x - y, \text{ dans le cas contraire,}$$

est automorphe par le sous-groupe $m = 1, 4, 7$ du groupe géométrique $\{x \to xm\}$, (m premier avec 3). Mais pour $m = 2, 5, 8$ il se projette sur un quasigroupe différent de Q. Pour $m = 3$ ou 6, l'image de Q est un quasigroupe du $3^{\text{ème}}$ ordre, qui n'est pas un diviseur de Q.

En général, si m n'est plus premier avec n, l'application $(x \to xm)$ projette le groupoïde G, d'ordre n, sur un système qui n'est plus un groupoïde. Ainsi, dans le quasigroupe R défini ci-dessus (II), $(x \to 2x)$ n'est pas un endomorphisme et projette R sur un ensemble algébrique qui ne satisfait plus à la loi d'unicité du produit: $(2 \times 2 = [2, 0, 4])$.

2. Groupoïdes "endo." *Un groupoïde* $G(\times)$ *admet les endomorphismes du semi-groupe* **(18)** *des homothéties, ou plus brièvement, est "endo," s'il existe un ensemble de nombres réels,* M, *tel que, pour tout* $m \in M$ *et tous* $x, y \in G$,

(i) *le produit* xm *soit défini,*

(ii) *l'application* $(x \to xm)$ *soit un endomorphisme:*

$$x \times y = z \Rightarrow (xm) \times (ym) = zm.$$

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

Si G est fini, d'ordre n, les homothéties $(x \to xm)$, $(m = [0, 1, \ldots, n-1])$ forment un semi-groupe isomorphe au semi-groupe multiplicatif de Z/n; il contient le groupe géométrique: $(m, n) = 1$.

Exemple I. Le groupe additif de Z/n est projeté par l'homothétie $(x \to xm)$, $(m, n) = k$, $n = kd$, sur son diviseur, le groupe cyclique d'ordre d:

$$(0, k, 2k, \ldots, n-k).$$

Exemple II. Soit G le groupe des translations engendré dans le plan par deux vecteurs non parallèles, $\mathbf{U}$ et $\mathbf{V}$, et dont les éléments sont de la forme:

$$\mathbf{W} = a\mathbf{U} + b\mathbf{V},$$

où a et b décrivent l'ensemble Z des entiers rationnels. Les éléments dont les coefficients a et b sont multiples d'un entier donné d, forment un diviseur D de G. Le groupe G se projette sur son diviseur D par l'endomorphisme $(x \to xd)$, car:

$$\mathbf{W} = a\mathbf{U} + b\mathbf{V} \rightleftarrows \mathbf{W}d = a\mathbf{U}d + b\mathbf{V}d.$$

Exemple III. On peut donner une définition plus générale encore et considérer des *ensembles munis de deux lois de composition* $(\times$ *et* $*)$, *telles que la seconde soit distributive à droite, à gauche, ou des deux côtés par rapport à la première:* $z * (x \times y) = (z * x) \times (z * y)$.

(a) Tel est l'ensemble dont les éléments sont les sous-ensembles d'un ensemble donné, si les lois de composition sont l'inter-section $\cap$ et la réunion $\cup$.

(b) Soit G l'ensemble des polynomes de degré $q-1$, $P = \Sigma a_i x^i$, $(i = 0, 1, \ldots, q-1)$, où p et q sont deux entiers naturels fixes et où les coefficients a_i sont définis sur Z/p (ce qui revient, pour $x = p$, à écrire les nombres $0, 1, \ldots, p^q - 1$ dans le système de base p). On définit un groupe Abélien $G(\times)$, d'ordre p^q, en prenant pour loi de composition $P \times P' = \Sigma (a_i + a_i')x^i$ (cela revient, si $x = p$, à l'addition sans retenues). Si m est un entier quelconque, appelons produit de P par m le polynome $P*m = \Sigma(a_i m)x^i$ où le coefficient ma_i est toujours calculé modulo p. Il est évident que l'application $P \to P*m$ est un endomorphisme de G. Si $x = p$, quand P et m décrivent l'ensemble $0, 1, \ldots, p^q - 1$, celui-ci est muni de deux opérations, la seconde étant distributive par rapport à la première.

(c) Tel est encore l'anneau Z, si la première loi est: $x \times y = 2x - y$ et la seconde: $x*y = x + y$.

(d) Si la première opération définit un groupe, on obtient un "*cluster*" **(6)**. Quand ce groupe est Abélien, le cluster devient un "*naring*" **(16)**. Si de plus la seconde opération est un semi-groupe, le naring est un anneau.

Tandis que le cluster est construit en se donnant le groupe $(\times)$ et en déterminant la seconde opération $(*)$ de manière qu'elle soit distributive par rapport à la première, dans le présent travail on se donne la multiplication $(*)$ et on construit la première loi $(\times)$ à partir de la seconde.

(e) Si la première opération définit un loop **(2)** et si les éléments non nuls forment un groupe par rapport à la seconde loi, on a affaire à un "*néofield*" **(10)**.

(f) Enfin, si les deux lois coïncident, on aboutit à la loi III des groupoïdes introduits sous le nom de "kēis" par Takasaki **(19)** et connus aussi sous celui de distributifs dans le cas des quasigroupes **(3)**. La première loi (c) en offre une illustration.

3. Définitions plus restreintes. Dans ce qui suit, nous nous en tiendrons aux définitions N° 1 et 2 restreintes à des ensembles de nombres de la façon suivante:

Un groupoïde G $(\times)$, *défini sur* Z/n, *est automorphe par le groupe géométrique si, pour tout entier* m, *premier avec* n, *et pour tous* $x,y,z \in G$, *on a:*

$$x \times y = z \Rightarrow (xm) \times (ym) = zm,$$

le produit xm *ayant la signification usuelle sur* Z/n.

Un groupoïde défini sur un ensemble de nombres réels, G, *est "endo" si la relation précédente a lieu quels que soient* $x,y,m \in G$.

4. Connexion avec Q_c. *Si* n *admet une racine primitive,* r, *tout groupoïde* $Q_g(\times)$ *d'ordre* n, *automorphe par le groupe géométrique, est (partiellement) isomorphe à un groupoïde* $Q_c(*)$, *automorphe par le groupe cyclique* **(12)**.

Preuve. Soit r une racine primitive de n. Les résidus (mod n) des puissances de r seront, à l'ordre près, les $\phi(n)$ nombres plus petits que n et premiers avec n. L'application $(r^i \rightarrow i)$ définit donc un système algébrique, $Q_c(*)$, automorphe par le groupe cyclique, et d'ordre $\phi(n)$. En effet, par hypothèse

$$x \times y = z \Rightarrow (xm) \times (ym) = zm, \qquad (\text{mod } n);$$

par suite $(\text{ind } x) * (\text{ind } y) = \text{ind } z$ entraîne

$$(\text{ind } m + \text{ind } x) * (\text{ind } m + \text{ind } y) = \text{ind } m + \text{ind } z,$$

c'est à dire, en changeant de notation

$$a * b = c \Rightarrow (a + h) * (b + h) = c + h \qquad (\text{mod } \phi(n)).$$

Mais l'isomorphisme n'est que partiel en ce sens que Q_c est incomplet **(12**, N°8**)**, le produit sur Q_c n'étant pas partout défini. De plus, si tout élément de Q_c a une préimage, tout élément de Q_g n'a pas une image dans Q_c.

Si r n'était plus racine primitive, l'ordre de Q_c serait un diviseur de $\phi(n)$ et $Q_c * Q_c$ pourrait même devenir vide.

Exemple I. Prenons pour Q_g le groupe additif de $Z/9$ et 2 pour racine primitive. Aux exposants $[1, 2, 3, 4, 5, 6]$ correspondent les restes $[2, 4, 8, 7, 5, 1]$. Si l'on remplace partout, dans Q_g, $[2, 4, 8, 7, 5, 1]$ par $[1, 2, 3, 4, 5, 0]$ on obtient

un quasigroupe incomplet du $6^{\text{ème}}$ ordre, où le produit n'est défini que si les facteurs ont même parité, et qui est automorphe par le groupe cyclique. Sa loi de composition est $x*y = 2x - y + 1 \pmod 6$, $x \equiv y \pmod 2$.

Si l'on prend $r = 4$, les exposants sont $[1, 2, 3]$, les restes $[4, 7, 1]$ et, en remplacant $[4, 7, 1]$ par $[1, 2, 0]$ dans Q_g, on obtient un groupoïde incomplet du $3^{\text{ème}}$ ordre, où aucun produit n'est défini.

Exemple II. Soit le quasigroupe "endo" du $7^{\text{ème}}$ ordre Q_g, défini par ses translations $S_i = (x \to x \times i)$; $S_0 = (132645)$, $S_1 = (034156)$, $S_2 = (061235)$, $S_3 = (025314)$, $S_4 = (052463)$, $S_5 = (016542)$, $S_6 = (043621)$; en prenant 3 comme racine primitive de 7, les exposants sont $[1, 2, 3, 4, 5, 6]$ et les restes $[3, 2, 6, 4, 5, 1]$. Supprimant l'ancien zéro et projetant chaque reste sur son indice, c.-à-d. $[1, 2, 3, 4, 5, 6]$ sur $[0, 2, 1, 4, 5, 3]$, on fait de Q_g un quasigroupe incomplet, du $6^{\text{ème}}$ ordre, automorphe par le groupe cyclique et défini **(12,** N° 4**)** par

$$S_0 = \begin{pmatrix} 012345 \\ 542\text{–}03 \end{pmatrix}.$$

Exemple III. Inversement, si n a une racine primitive, r, à tout groupoïde d'ordre $\phi(n)$, automorphe par le groupe cyclique, on pourra faire correspondre, par projection des indices sur les nombres, un groupoïde d'ordre n, automorphe par le groupe géométrique.

Ainsi, en prenant 2 comme racine primitive de 5, le quasigroupe incomplet Q, automorphe par le groupe cyclique, défini sur $Z/4$ par

$$S_0 = \begin{pmatrix} 0123 \\ 0\text{–}32 \end{pmatrix}$$

devient par la substitution

$$\begin{pmatrix} 0123 \\ 1243 \end{pmatrix}$$

un groupoïde dans lequel il suffit de remplacer les produits non définis par zéro, et de compléter en satisfaisant à la loi de cancellation, pour parvenir à un quasigroupe du $5^{\text{ème}}$ ordre, automorphe par le groupe géométrique, et ayant pour loi de composition $x \times y = 4x + 2y$, sur $Z/5$.

5. Non identité entre les propriétés des Q_c et des Q_g. La proposition 4 semble dénier tout intérêt à l'étude des groupoïdes "endo," Q_g. En réalité, presqu'aucune des propriétés des groupoïdes automorphes par le groupe cyclique ne se transmet aux "endo," car (i) ce parallélisme n'existe que si n a une racine primitive; (ii) Q_c est toujours incomplet et seulement d'ordre $(p - 1)p^q$, où p est premier impair (Si $n = 4$, Q_c est vide); (iii) alors que tout entier naturel, n, est de $n - 1$ manières la somme de deux autres, il n'est égal au produit de deux facteurs que dans la mesure où il est composé.

En fait, le domaine des Q_g est plus riche que celui des Q_c de tout l'apport fourni par la notion de divisibilité.

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

II. GROUPOIDES AUTOMORPHES PAR LE GROUPE GÉOMÉTRIQUE

6. Lemme. Tout groupoïde "endo" est automorphe par le groupe géométrique; mais la réciproque n'est pas vraie. Les "endo" jouissent de propriétés qui ne se retrouvent pas dans les groupoïdes automorphes par le groupe géométrique et non "endo." Nous allons d'abord étudier les propriétés appartenant à ces derniers.

Si $n = sk$, la suite $j, j + s, j + 2s, \ldots, j + (k - 1)s$, où j est premier avec s, contient $\phi(n)/\phi(s)$ termes premiers avec n. Ce nombre est toujours supérieur à un sauf si s est impair et k égal à deux.

Preuve. Soit $\bar{k}$ le plus grand diviseur de k qui soit premier avec s. En supposant k et s décomposés en produits de puissances de facteurs premiers inégaux, on voit facilement que la condition nécessaire et suffisante pour que x soit premier avec n est que x soit premier avec s et $\bar{k}$. La condition $(s,\bar{k}) = 1$ implique que les résidus de $i, i + s, i + 2s, \ldots, i + (k - 1)s$ forment $k/\bar{k}$ systèmes complets de restes modulo $\bar{k}$. Ainsi, chaque telle séquence a le même nombre de termes premiers avec $\bar{k}$. Pour que ces nombres soient premiers avec n il faut et il suffit que leur premier terme i soit premier avec s. Par suite les $\phi(s)$ séquences pour lesquelles $(i,s) = 1$ contiennent chacune le même nombre de termes premiers avec n, et en même temps elles contiennent la totalité des termes premiers avec n. D'où la relation de l'énoncé.

On vérifie sans peine qu'un nombre n, et son diviseur s, ont le même indicateur dans le seul cas où s est impair et moitié de n.

7. Relation entre les éléments. *Dans un groupoïde $G(\times)$, d'ordre n, automorphe par le groupe géométrique, si les PGCD de n avec deux éléments quelconques, a et a', sont $d = (n,a)$ et $d' = (n,a')$ et si $(d,d') = k$, alors les produits $a \times a'$ et $a' \times a$ sont multiples de k en général, et de $k/2$ si k est pair et n/k impair.*

Preuve. Soit $a \times a' = a''$ et p un nombre inférieur à n et premier avec n. En vertu de l'automorphisme $(ap \times (a'p) = a''p$. Mais

$$(1) \qquad (\exists p)\ ap \equiv a,\ a'p \equiv a' \pmod{n}.$$

En effet ces deux congruences s'écrivent

$$p \equiv 1 \pmod{n/d},\ p \equiv 1 \pmod{n/d'}.$$

Si $s = [n/d, n/d']$, les deux conditions simultanées équivalent à

$$(2) \qquad p \equiv 1 \pmod{s}.$$

Mais, en vertu d'une relation connue $n/s = (d,d')$, on aura $n = ks$ et il existera, d'après le lemme, $\phi(n)/\phi(s)$ valeurs de p satisfaisant à (2) et premières avec n.

Pour que le produit $a \times a'$ soit univoque il faut que, pour ces valeurs de p, on ait $a''p \equiv a'' \pmod{n}$ ou

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

$$a''(1 + sx) \equiv a'' \pmod{n}$$

et en divisant par s

$$a''x \equiv 0 \pmod{k}. \tag{3}$$

Soit $k = \prod A^\alpha$ (A premier). Si toutes les valeurs de x qui rendent $1 + sx$ premier avec n étaient divisibles par A, en posant $x = Ay$, la suite $1 + sx = 1 + sAy$ contiendrait $\phi(n)/\phi(sA)$ termes premiers avec n au lieu de $\phi(n)/\phi(s)$. Mais l'égalité $\phi(sA) = \phi(s)$ n'est possible que si $A = 1$ ou 2. Si $A \neq 2$, il y a au moins une valeur de x qui n'est pas divisible par A. Pour cette valeur de x, la condition (3) entraîne $a'' \equiv 0 \pmod{A^\alpha}$.

Ainsi a'' est divisible par A^α et, le même raisonnement pouvant être fait pour tous les facteurs premiers impairs de k, si k est impair, a'' est divisible par k.

Si k est pair, le raisonnement subsiste pour tous les facteurs de k, sauf pour $A = 2$ et $\phi(sA) = \phi(s)$, ce qui suppose s impair. Soit alors $k = 2^\alpha k'$, $n = 2^\alpha k's$, k' et s impairs. Considérons de nouveau la suite $1, 1 + s, \ldots, 1 + (k - 1)s$; les valeurs impaires de x fournissent des termes $1 + sx$ pairs. Donc les termes de cette suite qui sont premiers avec n sont tout contenus dans la suivante: $1, 1 + 2s, 1 + 4s, \ldots, 1 + 2ys, \ldots, 1 + (k-2)s$, et leur nombre est $\phi(n)/\phi(2s) = \phi(n)/\phi(s)$.

Parmi les valeurs de y qui rendent $1 + 2ys$ premier avec n, il y en a au moins une qui est première avec 2 car, si toutes ces valeurs étaient paires, les termes $1 + xs$ premiers avec n seraient tous compris dans la suite $1 + 4ts$ ou, en posant $4s = s'$, dans la suite $1 + ts'$. Or cette dernière contient seulement $\phi(n)/\phi(4s) = \phi(n)/2\phi(s)$ termes premiers avec n, puisque s est impair; ce nombre n'est pas égal à $\phi(n)/\phi(s)$. Soit donc $y = 2z + 1$ la (ou une) valeur impaire de y qui rend $1 + xs$ premier avec n; on a

$$x = 2y = 2(2z + 1)$$

et la condition (3) devient

$$2(2z + 1)a'' \equiv 0 \pmod{2^\alpha k'}$$

ou

$$a'' \equiv 0 \pmod{2^{\alpha-1}};$$

ainsi a'' est divisible par $k/2$.

8. Autre relation. *Dans un quasigroupe $Q(\times)$, d'ordre n, automorphe par le groupe géométrique, si $a \times a' = a''$, (a, a' impairs $\in Q$), alors les PGCD, $(a,n) = d$, $(a',n) = d'$, $(a'',n) = d''$ satisfont à la relation $(d,d') = (d',d'') = (d'',d)$ et l'on a $d'' = (d,d')h$, où les facteurs premiers de n qui divisent h sont premiers avec d et d', ou bien figurent dans les décompositions, de d et de d', avec le même exposant. La proposition est vraie quels que soient a et a' si n est impair.*

Preuve. A cause de la loi du quotient, deux des congruences

$$pa \equiv a,\ pa' \equiv a',\ pa'' \equiv a'' \pmod{n}, \qquad (p, n) = 1,$$

doivent entraîner la troisième. D'après le N° précédent, a'' est divisible par (d,d'), autrement dit, (d,d') divise a'' et n, donc aussi (a'',n) ou d''; ainsi

$$(d, d')\,|\,d'', \qquad (d', d'')\,|\,d, \qquad (d'', d)\,|\,d',$$

et le *PGCD* de d, d', d'' est à la fois (d, d'), (d', d'') et (d'', d). On aura donc $d'' = h(d, d')$.

Désignons par A les facteurs premiers de n et soit

$$d = \prod A^{\alpha},\ d' = \prod A^{\alpha'},\ d'' = \prod A^{\alpha''},$$

on aura

$$(d, d') = \prod A^{\mathrm{Min}(\alpha,\alpha')}$$
$$(d', d'') = \prod A^{\mathrm{Min}(\alpha',\alpha'')}$$
$$(d'', d) = \prod A^{\mathrm{Min}(\alpha'',\alpha)}.$$

Donc, pour tout facteur premier de n,

$$\mathrm{Min}(\alpha,\alpha') = \mathrm{Min}(\alpha',\alpha'') = \mathrm{Min}(\alpha''\alpha).$$

En vertu de l'égalité $d'' = h(d,d')$ le facteur A ne peut diviser h que si $\alpha'' > \mathrm{Min}(\alpha,\alpha')$, ce qui exige $\alpha = \alpha'$.

9. Diviseurs. *Si $Q(\times)$ est un quasigroupe d'ordre n, automorphe par le groupe géométrique, et k un diviseur impair de n, les multiples de k forment un sous-quasigroupe D, de Q, d'ordre n/k, isomorphe par $(x \to x/k)$ à un quasigroupe $E(.)$ qui est lui-même automorphe par le groupe géométrique d'ordre $\phi(n/k)$.*

Preuve. Soit $(n,a) = d$ et $(n,a') = d'$. Alors

$$k|n,\ k|a \text{ et } k|a' \Rightarrow k|(d,d'),$$

donc (N° 7) $a \times a'$ est multiple de (d,d') et par conséquent de k. Ainsi l'ensemble des multiples de k est fermé et forme un sous-quasigroupe de Q. Si dans celui-ci on divise tous les éléments par k, on trouve un quasigroupe, $E(.)$, d'ordre n/k, composé des éléments $[0, 1, 2, \ldots, n/k - 1]$ et où nous définissons la composition $(\cdot)$ par

$$a \times a' = a'' \Rightarrow (a/k).(a'/k) = a''/k$$

donc $D \cong E$. Mais, à cause de l'automorphisme

$$a \times a' = a'' \Rightarrow (ap) \times (a'p) = a''p, \qquad (p,n) = 1,\ p<n.$$

Donc $(a/k).(a'/k) = a''/k \Rightarrow (ap/k).(a'p/k) = a''p/k$.

L'ensemble des valeurs de p parcourt (mod n/k) tous les nombres premiers avec n/k. En effet, d'après le lemme, si l'on remplace les $\phi(n)$ nombres plus

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

petits que n et premiers avec $n = ks$ par leurs résidus (mod s), on obtient les $\phi(s)$ nombres plus petits que s et premiers avec s, chacun le même nombre de fois. En faisant $n/k = s$, on voit que la condition

$$(a/k).(a'/k) = a''/k \Rightarrow (ap/k).(a'p/k) = a''p/k \qquad (\text{mod } n/k)$$

est vérifiée pour toute valeur de p première avec n/k; ainsi le quasigroupe $E(.)$ est bien automorphe par le groupe géométrique $(x \to px)$, $(p,n/k) = 1$.

Quand Q est "endo" la proposition est vraie même sans la restriction sur la parité de k, et la preuve est immédiate. Mais elle n'est pas valable si Q n'est pas "endo."

10. Corrélation avec Q_c. Avant de passer a l'étude des "endo," observons que, en vertu du N° 4, les propositions 10 et suivantes de **(12)** ont ici leurs corrélatives:

Si Q ($\times$) est un quasigroupe d'ordre n automorphe par le groupe géométrique, $(x \times y = z)$, son conjoint $(y.x = z)$, son réciproque $(z \ominus y = x)$, le quasigroupe R ($\odot$) défini par $x \odot y = az$, $(a,n) = 1$, le quasigroupe S $(*)$ défini par $ax*ay = z$ et le quasigroupe T ($\wedge$), image de Q par la transformation $x \to x^a$, $(a,\phi(n)) = 1$, avec la définition $x^a \wedge y^a = z^a$, sont encore automorphes par le groupe géométrique.

La vérification est immédiate pour les quatre premiers cas. Dans le dernier, observons que le groupe géométrique est invariant par $(x \to x^a)$ si a est premier avec l'ordre $\phi(n)$ de ce groupe. Alors, si $x \times y = z$ et par suite $xm \times ym = zm$, $(m,n) = 1$, *on aura*

$$x^a \wedge y^a = z^a \Rightarrow (xm)^a \wedge (ym)^a = (zm)^a \Rightarrow m^a x^a \wedge m^a y^a = m^a z^a$$

et comme m^a décrit les mêmes valeurs (mod n) que m,

$$mx^a \wedge my^a = mz^a.$$

Exemple. Soit A le quasigroupe du $9^{\text{ème}}$ ordre $[0, 1, 2, \ldots, 8]$, automorphe par le groupe géométrique et défini par $1 \times 0 = 1$, $1 \times 3 = 2$, $2 \times 3 = 1$, $A \times 1 = [8, 0, 6, 4, 5, 3, 7, 1, 2]$, et où le diviseur $D = [0, 3, 6]$ a pour loi de composition, sur $Z/9$, $x \times y = x + 2y$. Si l'on fait subir à A l'isomorphisme $(2, 5)(4, 7)$, qui laisse invariant le groupe géométrique d'ordre $\phi(9)$, on obtient un nouveau quasigroupe qui est encore automorphe par le groupe géométrique. (Il suffit de le vérifier en prenant pour m une racine primitive $\rho = 2$.)

Plus généralement, *si Q($\times$) est un quasigroupe automorphe par le groupe géométrique G, et si R (.) est isomorphe à Q par T: $(x \to x')$, une condition suffisante pour que R soit automorphe par G est que T laisse G invariant.*

Car $mx \times my = mz \leftrightarrows (mx)'.(my)' = (mz)'$, mais puisque $T \in A_G$, $(mx)' = m'x' = \mu x'$, donc $\mu x'.\mu y' = \mu z'$, *avec* $\mu \in G$.

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

11. Tables. Pour $n = 1, 2, 3$ on obtient seulement la solution ordinaire

$$x \times y = ax + by \pmod{n}, \qquad (a, b \text{ premiers avec } n)$$

qui est toujours "endo." Toutefois, pour $n = 2$, on a la solution exceptionnelle: $x \times y = x + y + 1$.

Pour $n = 4$ on trouve le groupe carré de *K*lein, son produit par l'isotopie **(1)**

$$\xi = 1, \qquad \eta = 0.13.2, \qquad \zeta = 1,$$

et le conjoint de ce dernier.

Pour $n = 5$, une prospection exhaustive donne 32 solutions, 16 ordinaires et 16 définies par les produits $Q \times a = [1, 0, 2, 4, 3]$, $[1, 2, 3, 0, 4]$, $[1, 3, 4, 2, 0]$, $[1, 4, 0, 3, 2]$, $(a = 1, 2, 3, 4)$, en complétant de manière à respecter la loi du quotient.

12. Isomérie. *Si, dans un quasigroupe $Q(\times)$, d'ordre n, automorphe par le groupe géométrique, $(x \to xm)$, $(m,n) = 1$, on remplace par isomérie* **(11**, pp. 8-10**)** *l'ensemble produit $D \times D$ induit par Q sur le sous-quasigroupe D de Q composé des multiples de k, $(k|n)$, par l'ensemble produit $D'*D'$, où D' est un quasigroupe automorphe par $(x \to xm)$, et composé des mêmes éléments que D, alors on obtient un nouveau quasigroupe Q' qui est encore automorphe par le groupe géométrique.*

Ainsi, si Q et R sont deux quasigroupes du même ordre n, automorphes par le groupe géométrique, on obtiendra deux nouveaux quasigroupes, automorphes par le groupe géométrique, en échangeant par isomérie le diviseur $D = 0,d,2d, \ldots, n-d$, avec $(n,d) = d$ du premier contre le diviseur $D' = 0,d,2d,\ldots$ du second.

D'un quasigroupe "endo" on pourra déduire par isomérie une série de quasigroupes automorphes par le groupe géométrique; toutefois toutes les solutions ne seront pas atteintes de cette façon, car on peut construire des quasigroupes automorphes par le groupe géométrique et dont le diviseur $D = 0,d,2d,\ldots$ n'est pas normal, (N° 14). Ainsi, dans l'exemple du N° 10, le diviseur $D = [0, 3, 6]$ n'est pas normal.

Néanmoins la remarque précédente, d'une part met en lumière l'importance de la notion d'*isomérie*, introduite en 1950 **(11)** et que l'on rencontre d'une façon toute naturelle et presque obligatoire dans l'étude des quasigroupes, dont elle est une propriété caractéristique; d'autre part, elle nous mène à l'étude des quasigroupes "endo."

III. QUASIGROUPES "ENDO"

13. "Endo" usuels. Avant d'aborder l'étude des "endo," signalons quelques quasigroupes susceptibles de servir d'illustration aux propriétés que nous rencontrerons plus loin.

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

(a) Sur Z/n la loi

$$x \times y = ax + by \qquad (a, b, \text{ premiers avec } n)$$

définit un quasigroupe "endo."

(i) L'équation à gauche $x \times c = d$, ou $ax + bc = d$, a une solution unique $x = (d-bc)a'$, où a' est l'associé de a, $(aa' = 1)$. Il en est de même pour l'équation à droite $c \times y = d$. Donc $A(\times)$ est un quasigroupe.

(ii) A est "endo" car

$$xm \times ym = amx + bmy = m(ax + by) = (x \times y)m.$$

(b) Sur le corps Q des fractions rationnelles, la loi

$$x \times y = ax + by, \qquad (a, b \neq 0 \text{ dans } Q)$$

définit un quasigroupe "endo," car

(i) $$(\exists x)\, x \times c = d$$

puisque $ax + bc = d$ a une solution unique $x = (d-bc)/a$, a n'étant pas nul; et de même $(\exists y)\, c \times y = d$. Donc B est un quasigroupe.

(ii) On voit comme pour A que B est "endo."

(c) Le quasigroupe B reste évidemment "endo" si l'on suppose a et b entiers.

(d) Sur le corps R des nombres réels, la loi

$$x \times y = ax + by, \ (a, b \text{ quelconques} \neq 0)$$

définit un quasigroupe "endo." Si a et b sont rationnels, B est un diviseur de D.

(e) Si a et b sont entiers, D est un "endo" dont C est diviseur.

14. Diviseur. (i) *Si a est un nombre réel quelconque, convenons d'appeler multiples de a les produits de a par les entiers rationnels $Z = [0, \pm 1, \pm 2, \ldots]$. Deux nombres sont congrus par rapport à a si leur différence est multiple de a.* (ii) *La condition nécessaire et suffisante pour que, dans un quasigroupe "endo," $Q(\times)$, les multiples d'un élément quelconque, a, forment un diviseur D_a est que les éléments entiers de Q forment eux-mêmes un sous-quasigroupe de Q. Si Q est fini, d'ordre n, $D_a = [0, d, 2d, \ldots, n-d]$, $d = (n,a)$ et D_a est d'ordre n/d.* (iii) *Si $Q(\times)$ est construit dans le corps R des nombres réels, ou dans celui, Q, des fractions rationnelles tout nombre $a \neq 0$ dans Q $(\times)$ définit une partition des éléments de Q où deux éléments appartiennent ou non au même bloc suivant qu'ils sont, ou non, congrus par rapport à a. La condition nécessaire et suffisante pour que cette partition soit régulière est que la partition définie par $a = 1$ le soit. D_a est alors normal dans Q. Le système des représentants est l'ensemble des éléments de Q qui ne sont pas congrus les uns des autres par rapport à a. Le quasigroupe quotient Q/D_a a même puissance que l'ensemble des éléments de Q compris entre 0 et a.*

Preuve. (ii) La condition est nécessaire car, en faisant $a = 1$, les multiples de 1, c'est-à-dire les éléments entiers de Q, forment un diviseur.

Elle est suffisante car si

$$x, y \in Z \Rightarrow x \times y \in Z,$$

soient ax et ay deux multiples de a. Leur produit sera, en tenant compte de l'endomorphisme,

$$ax \times ay = a(x \times y),$$

ce qui est un multiple de a puisque $x \times y$ est entier par hypothèse. Donc le complexe des multiples de a est fermé par rapport à $(\times)$. Les équations $q \times x = b$ et $x \times q = b$ ont une solution unique dans ce complexe, donc **(8**,p. 986**)** celui-ci est un quasigroupe.

Si Q est fini d'ordre n, le diviseur existera toujours et sera $D = [0,d,2d, \ldots,n-d]$ (mod n), d'ordre n/d, car les multiples de a s'indentifient avec ceux de $d = (a,n)$.

Exemple I. Dans le quasigroupe A (N° 13) défini par

$$x \times y = 2x + 8y \pmod{15},$$

les quatre diviseurs sont [0], [0, 5, 10], [0, 3, 6, 9, 12] et [A] lui-même.

Exemple II. Dans le groupe additif des fractions rationnelles (C, N° 13, avec $a = b = 1$), le complexe des entiers relatifs forme un diviseur, et il est isomorphe au diviseur $[0, \pm p/q, \pm 2p/q, \ldots]$, formé par les multiples de la fraction fixe arbitraire $p/q \neq 0$.

(iii) Si i et i' sont deux éléments de Q, non congrus par rapport à a, ils représentent deux classes disjointes

$$\Sigma\, az + i \quad \text{et} \quad \Sigma\, az + i', \quad z \in Z,$$

de la partition déterminée par a sur Q. Le produit $(\times)$ de deux éléments $az + i$ et $az' + i'$ peut se mettre sous la forme $az'' + i''$, où i'' est bien déterminé, à une congruence près par rapport à a:

$$(az + i) \times (az' + i') = az'' + i''. \tag{1}$$

Si cette partition est régulière, i'' ne doit dépendre que de i et de i' (par rapport à a). En vertu de l'endomorphisme, si l'on multiplie les trois éléments de (1) par $1/a$, on aura;

$$(z + i/a) \times (z' + i'/a) = z'' + i''/a. \tag{2}$$

Mais si deux nombres i et j sont congrus (ou non) par rapport à a, les quotients i/a et j/a seront en même temps congrus (ou non) par rapport à 1 et vice-versa, car

$$a|(i-j), \text{ ou } i-j = ka \leftrightarrows i/a - j/a = k,$$

où k est entier, c'est-à-dire multiple de 1.

Les égalités (1) et (2) expriment que les partitions définies sur Q par a et par 1 sont régulières en même temps.

Si D_1 est le diviseur de Q formé de ses éléments entiers et D_a celui qui est formé par les multiples de a, D_1 et D_a sont alors normaux. D'ailleurs ils sont isomorphes car, à cause de l'endomorphisme

$$D_1 \cong D_a = D_1(x \to xa)$$

Le quasigroupe quotient Q/D_a est formé des cosets $az + i$, $az + i', \ldots,$ $z \in Z$, $(i-i')/a$ non entier.

On peut ramener tous les i entre 0 et a; le système des représentants est formé de tous les éléments de Q compris entre 0 et a.

Exemple. (N° 13,*C*), $x \times y = ax + by$. La fraction 3/4 définit une partition régulière dont le diviseur normal est formé des multiples de 3/4 et dont les cosets sont $\Sigma\ 3z/4 + p/q$, où p/q n'est pas multiple de 3/4; on a

$$(3z/4 + p/q) \times (3z'/4 + p'/q') = 3(az + bz')/4 + ap/q + bp'/q'.$$

Le représentant $ap/q + ap'/q'$ ne dépend que des représentants p/q et p'/q'. A chaque fraction comprise entre 0 et 3/4 correspond un coset. Le quasigroupe quotient est isomorphe au quasigroupe défini par la même loi que C, sur l'intervalle (0, 3/4), modulo 3/4.

15. Diviseur Normal. *Si $Q(\times)$ est un quasigroupe "endo" d'ordre n, si f est un élément quelconque de Q et si $(f,n) = d$, $(n = kd)$,* (i) *l'endomorphisme $(x \to xf)$ projette Q sur son diviseur $D = [0, d, 2d, \ldots, n-d]$.* (ii) *Celui-ci est toujours normal, les cosets sont $\Sigma\ ud + i$, $(u = 0, 1, \ldots, k-1)$.* (iii) *Le quasigroupe quotient Q/D est isomorphe au diviseur $[0, k, 2k, \ldots, n-k]$.* (iv) *Si E est un ensemble quelconque d'éléments $\in Q$, en nombre k, respectivement congrus* (mod k) *à $[0, 1, 2, \ldots, k-1]$. l'ensemble produit $E.E = E \times E$* (mod k) *est isomorphe à D par $(x \to xd)$.* (v) *Enfin E (.) est "endo"* (mod k).

Preuve. (i) Dans l'application T $(x \to xf)$, tous les éléments $x, x + k, x + 2k,$ $\ldots, x + n-k$ ont la même image xf. Ainsi, T projette homomorphiquement Q sur celui de ses diviseurs, D, qui est composé des multiples de f, c'est-à-dire de d.

(ii) La partition modulo d est régulière car, quels que soient u et v, on a par $(x \to xk)$

$$du + i \to ki \quad (i < d)$$
$$dv + j \to kj \quad (j < d)$$
$$(ud + i) \times (vd + j) \to ki \times kj = k(i \times j).$$

Mais les éléments qui se projettent sur $k(i \times j)$ sont

$$i \times j,\ i \times j + d,\ i \times j + 2d,\ \ldots,\ i \times j + n - d,$$

donc $(ud + i) \times (vd + j) = wd + (i \times j)$;
par suite les cosets $\Sigma_u\ ud + i$ et $\Sigma_v\ vd + j$ ont pour produit ($\times$) le coset $\Sigma_w\ wd + (i \times j)$.

(iii) Le système des représentants est $0, 1, 2, \ldots, i, \ldots, j, \ldots, d-1$. Le quasigroupe quotient Q/D est isomorphe au diviseur $0, k, 2k, \ldots, n-k$, puisque

$$i \times j = r \leftrightarrows (ki) \times (kj) = kr.$$

(iv) Soit E un système quelconque de k éléments respectivement congrus à $0, 1, 2, \ldots, k-1 \pmod k$. L'application $T = (x \to xf)$ les projette sur

$$0, f, 2f, 3f, \ldots, n-f \qquad (\text{car } kf = 0, \bmod n)$$

c'est-à-dire univoquement sur les éléments de D.

Soient $x, y \in E$ et $x \times y = z$. En tenant compte de l'endomorphisme de Q, on a

$$(fx) \times (fy) = fz \pmod n$$

Mais cette égalité a lieu aussi modulo n/d. L'ensemble produit $E \times E$ est composé d'éléments qui, ramenés au dessous du module k, forment un quasigroupe $E(.)$ isomorphe à D par T.

(v) Reste à montrer que $E(.)$ est "endo" (mod k). Par hypothèse, Q admet les endomorphismes $(x \to xm)$, $(m < n)$. Toute application $(x \to xm)$ projette D sur un de ses diviseurs, pouvant coïncider avec D. Cela signifie que

$$(ad) \times (bd) = cd \Rightarrow (mad) \times (mbd) = mcd \pmod n.$$

Mais puisque $D(\ \times\ ) \cong E(.)$ par T,

$$a.b = c \Rightarrow (ma).(mb) = mc \pmod k.$$

Exemple. Soit le quasigroupe "endo" du $15^{\text{ème}}$ ordre $Q = [0, 1, 2, \ldots, 14]$ défini par les produits:

$$Q \times 1 = [11, 4, 0, 8, 7, 6, 14, 10, 3, 2, 1, 9, 5, 13, 12];$$
$$1 \times Q = [2, 4, 6, 5, 13, 12, 14, 1, 0, 8, 7, 9, 11, 10, 3].$$

Prenons $f = 10$. Par $(x \to 10x)$ on le projette sur son diviseur $D_5 = [0, 5, 10]$.

Pour $d = 3$, on a la partition $D_3 = [0, 3, 6, 9, 12]$; $C = [1, 4, 7, 10, 13]$; $C' = [2, 5, 8, 11, 14]$. Le quasigroupe quotient Q/D_3 est isomorphe à $D_5 = [0, 5, 10]$.

Pour $d = 5$, on a le diviseur normal $D_5 = [0, 5, 10]$ et les cosets $C = [1, 6, 11]$; $C' = [2, 7, 12]$; $C'' = [3, 8, 13]$; $C''' = [4, 9, 14]$. Le quasigroupe quotient est isomorphe à D_3.

Si l'on prend $E = [2, 3, 5, 11, 14] \equiv [2, 3, 0, 1, 4] \pmod 5$ et si l'on remplace tous les éléments de E et de $E \times E$ par leur reste (mod 5) on obtient $E(.) \cong D_3 \cong Q/D_5$.

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

IV. COMPOSITION DES "ENDO"

16. Lemme. Si deux quasigroupes K et S, d'ordres k et s, sont "endo", leur produit direct **(9)** sera encore un quasigroupe Q et, d'après ce que l'on sait du produit direct, en regardant l'endomorphisme $(x \to xm)$ comme une opération externe, distributive, Q admettra encore cette opération distributive. Mais pareille affirmation a une signification illusoire, car les éléments de Q ne sont plus des nombres, mais des êtres complexes (x,y), $x \in K$, $y \in S$. Les démonstrations suivantes sont donc nécessaires. Nous utiliserons le lemme connu **(7**, Théorème 59**)**:

Si $n = sk$, $(s, k) = 1$, tout nombre (mod n) *peut se mettre, d'une manière et une seule, sous la forme $kx + sy$, $x < s$, $y < k$.*

17. Produit direct. *Le produit direct de deux "endo" est "endo,"* ou plus précisément: *Si $(s,k) = 1$ et si $K\ (\times) = [0,1, \ldots ,y, \ldots ,k-1]$ et $S(.) = [0, 1, \ldots , x , \ldots , s-1]$ sont deux "endo" (ou deux quasigroupes automorphes par le groupe géométrique), le groupoïde $G(*)$défini par*

$$G = \sum (kx + sy),\ (xk + sy) * (kx' + sy') \equiv k(x.x') + s(y \times y'), \quad (\text{mod } ks),$$

est un quasigroupe "endo" (ou un quasigroupe automorphe par le groupe géométrique).

Preuve. A tout couple ordonné $kx + sy$, $kx' + sy'$ correspond un produit et un seul; donc G est un groupoïde.

Supposons que

$$(kx + sy)*(kx' + sy') \equiv (xk + sy)*(kx'' + sy'') \qquad (\text{mod } n)$$

donc $x.x' - x.x'' \equiv 0$ (mod s) et $x' = x''$; pareillement $y' = y''$. Le calcul est le même à droite. Ainsi $Q(*)$ est un quasigroupe.

Pour que Q soit "endo" (automorphe par le groupe géométrique) il faut qu'il satisfasse, pour tout facteur f (mod n), (pour tout facteur f premier avec n) à

$$[f(kx + sy)]*[f(kx' + sy')] \equiv fk(x.x') + fs(y \times y') \qquad (\text{mod } n).$$

Si l'on cherche les coefficients de u et v, de k et de s, lorsqu'on met le nombre $f(kx + sy)$ sous la forme $ku + sv$ (mod n), $u < s$, $v < k$, on trouve que u et v sont uniques et bien déterminés. Si l'on appelle u' et v' les quantités analogues à u et v, relativement à x' et y', la condition devient

$$(ku + sv)*(ku' + sv') \equiv fk(x.x') + fs(y \times y') \qquad (\text{mod } n),$$

ou finalement

$$k(u.u') + s(v \times v') \equiv k(u.u') + s(v \times v') \qquad (\text{mod } n),$$

où $u.u'$ est défini (mod s) et $v \times v'$ (mod k), ce qui est une identité. Dans le cas des "endo" elle est vérifiée quel que soit f. Si les quasigroupes sont auto-

morphes par le groupe géométrique, elle est satisfaite pour tout nombre f, premier avec k et s, c'est-à-dire avec n.

Exemple I.

$$k = 2\ ,\ s = 3;\ K(\times) = 0, 1,\ x \times y = x + y \pmod 2;$$
$$S(.) = [0, 1, 2];\ x.y = 2(x + y) \pmod 3;$$
$$Q(*) = [0, 1, 2, 3, 4, 5];\ x*y = 5(x + y) \pmod 6.$$

Exemple II. $k = 5$; $s = 3$. Prenons pour $K(\times)$ le quasigroupe défini par $S_0 = (1\,2\,4\,3)$, $S_1 = (0\,1\,4\,2)$, $S_2 = (0\,2\,3\,4)$, $S_3 = (0\,3\,2\,1)$, $S_4 = (0\,4\,1\,3)$, où S_i est la translation $(x \to x \times i)$. Comme quasigroupe $S(.)$, gardons le même $x.y = 2(x + y) \pmod 3$ que dans l'exemple précédent.

Alors $Q(*)$ a pour loi de composition

$$(5x + 3y)*(5x' + 3y') \equiv 5(x.x') + 3(y \times y') \pmod{15}.$$

Il coïncide avec le quasigroupe donné en exemple au N° 15.

Les composants S et K ne sont autre chose que les quasigroupes $E(.)$ définis au N° 15 et relatifs aux modules s et k (*cf.* l'exemple du N° 15).

18. Réciproque. *Tout "endo" d'ordre ks, $(k, s) = 1$, est le produit direct de deux "endo" d'ordres k et s;* ou, plus précisément: *Si Q $(*)$ est un quasigroupe "endo," d'ordre $n = sk$, $(k, s) = 1$, alors $\exists$ deux "endo" $K(\times)$ d'ordre k et S $(.)$ d'ordre s, respectivement isomorphes à $D_s = [0, s, 2s, \ldots, n-s]$ par $(x \to xs)$ et à $D_k = [0, k, 2k, \ldots, n-k]$ par $(x \to xk)$, tels que, pour tous $a = kx + sy$, $a' = kx' + sy'$; $x, x' < s$; $y, y' < k$, on ait*

$$a*a' \equiv k(x.x') + s(y \times y') \pmod n.$$

Preuve. Soit $Q(*)$ un quasigroupe "endo" d'ordre $n = ks$, $(k, s) = 1$. Si a et a' sont deux éléments quelconques de Q, chacun d'eux peut, d'une seule manière, être mis sous la forme

$$a = kx + sy,\ a' = kx' + sy'$$

avec $x, x' < s$; $y, y' < k$; et $a, a' \in Q$.

On a vu (N° 15, (ii)) que si

$$a \equiv i,\quad a' \equiv i' \pmod s,$$

alors

$$a*a' \equiv i*i' \pmod s,$$

or on a

$$a \equiv kx,\quad a' \equiv kx' \pmod s.$$

Donc

$$a*a' \equiv (kx)*(kx') \equiv k(x*x') \pmod s.$$

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

Considérons le quasigroupe $S(.) = [0, 1, 2, \ldots, s-1]$, induit par $(*)$ de la manière suivante. Soit l'ensemble produit $E*E$, où $E = [0, 1, 2, \ldots, s-1]$. Remplaçons tous les éléments de $E*E$ par leur reste (mod s). Nous obtenons un quasigroupe $S(.)$ qui (N° 15, (iv) et (v)) est "endo" et isomorphe au diviseur $D_k = [0, k, 2k, \ldots, n-k]$ par $(x \to xk)$. Ainsi on a

$$x*x' \equiv x.x' \pmod{s},$$

d'où

$$a*a' \equiv k(x.x') \pmod{s}.$$

On trouve pareillement

$$a*a' \equiv s(y \times y') \pmod{k},$$

où $K(\times)$ est induit par $(*)$ sur l'ensemble $F*F$, $(F = [0, 1, 2, \ldots, k-1])$, pris modulo k, et est isomorphe au diviseur $D_s = [0, s, 2s, \ldots, n-s]$ par $(x \to xs)$.

On a donc

$$a*a' \equiv k(x.x') + s(y \times y') \pmod{s \text{ et mod } k}$$

et comme s et k sont premiers entre eux, la congruence est vérifiée modulo n.

La réciproque n'est pas vraie, en général, pour les quasigroupes automorphes par le groupe géométrique (voir N° 1, exemple II).

19. Lemme. Citons la proposition connue **(5, II**, p. 64**) (17**, p. 130**)**.

Si $n = a^\alpha b^\beta c^\gamma \ldots$, $(a,b,c, \ldots$ *premiers inégaux*), *tout entier* A (mod n) *peut être décomposé d'une manière et une seule en une somme*

$$A = (n/a^\alpha)x + (n/b^\beta)y + (n/c^\gamma)z + \ldots, 0 \leqslant x < a^\alpha, 0 \leqslant y < b^\beta, \ldots.$$

20. Généralisation. *Tout "endo" fini est le produit direct d'"endo" ayant pour ordres des puissances de nombres premiers,* ou plus précisément: *Si* $n = a^\alpha b^\beta c^\gamma \ldots$ $(a,b,c \ldots$ *premiers inégaux*), *tout quasigroupe "endo,"* $Q(*)$, *d'ordre* n, *a pour loi de composition*

$$A * A' = \sum{}_a (n/a^\alpha)(x \times x')_a, \text{ où } A = \sum{}_a (n/a^\alpha)x \in Q,$$

$A' = \Sigma_a (n/a^\alpha)x' \in Q$; $0 \leqslant x,x' < a^\alpha$ *et où* $K(\times)_a$ *est le quasigroupe "endo" d'ordre* a^α, *induit par* $x*x' \equiv (x \times x')_a$ (mod a^α), *isomorphe au diviseur de* Q: $[0, (n/a^\alpha), (2n/a^\alpha), \ldots, (n - n/a^\alpha)]$ *par* $(x \to (nx)/a^\alpha)$.

Preuve. On sait (N° 15, (ii)) que

$$A \equiv i, A' \equiv i' \pmod{s}, \qquad (s,n) \equiv s \Rightarrow A*A' \equiv i*i' \pmod{s}.$$

Or

$$A \equiv (n/a^\alpha)x, \qquad A' \equiv (n/a^\alpha)x' \pmod{a^\alpha},$$

donc

$$A*A' \equiv (nx/a^\alpha)*(nx'/a^\alpha) \pmod{a^\alpha}.$$

A cause de l'endomorphisme

$$(nx/a^\alpha)*(nx'/a^\alpha) \equiv (n/a^\alpha)(x*x') \pmod{n}.$$

Donc

$$A*A' \equiv (n/a^\alpha)(x \times x')_a \pmod{a^\alpha}.$$

Considérons la somme

$$\sum{}_a (n/a^\alpha)(x \times x')_a.$$

Tous ses termes, sauf le premier, ont des coefficients divisibles par a^α, et comme le premier est congru à $A*A'$ (mod a^α), on a

$$A * A' \equiv \sum{}_a (n/a^\alpha)(x \times x')_a \pmod{a^\alpha}.$$

La même chose peut être répétée pour toutes les puissances $b^\beta, c^\gamma, \ldots$. Finalement

$$A * A' \equiv \sum{}_a (n/a^\alpha)(x \times x')_a \pmod{a^\alpha, b^\beta, c^\gamma, \ldots},$$

donc aussi (mod n).

21. Semi-groupes des "endo". *L'ensemble des quasigroupes "endo" finis est, par rapport à l'opération de composition des "endo"* (N° 17) *un semi-groupe incomplet et commutatif, homomorphe à celui des entiers naturels, où la multiplication (usuelle) n'est supposée être définie que si les facteurs sont premiers entre eux, l'image de tout "endo" d'ordre n étant le nombre n.*

Preuve. L'opération de composition entre deux "endo" dont les ordres k et s sont premiers entre eux, définie au N° 17, est associative et commutative; car, si k, s, t sont trois nombres premiers entre eux deux à deux, et si $n = kst$, soient K,S,T trois "endo" d'ordres respectifs k, s, t. Si l'on compose K et S, et le résultat avec T, ou S et T, puis K avec ce produit, on obtiendra un "endo" d'ordre n, dont la loi de composition, d'après le N° 20, sera dans les deux cas

$$A * A' \equiv \sum{}_a (n/a^\alpha)(x \times x')_a \pmod{n}.$$

On peut d'ailleurs le vérifier par un calcul facile. Soient $K(*)$, $S(\times)$ *et* $T(.)$ les trois "endo" d'ordres respectifs k,s,t. Composons K et S; la loi de multiplication du résultat sera $(\oplus)$.

$$X \oplus X' \equiv (sx + ky) \oplus (sx' + ky') \equiv s(x*x') + k(y \times y') \pmod{ks}.$$

Composons ce quasigroupe avec T; le quasigroupe résultant sera $Q(\circ)$

$$A \circ A' = (tX + ksz) \circ (tX' + ksz') \equiv t(X \oplus X') + ks(z.z') \pmod{n}$$
$$\textit{ou}\ A \circ A' = st(x*x') + tk(y \times y') + ks(z.z') \pmod{n}.$$

Cette expression est indépendante de l'ordre des trois composants K, S, T. Le produit est donc associatif.

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

Ainsi, si l'on considère l'ensemble de tous les "endo" d'ordre fini, l'opération de composition organise cet ensemble en un semi-groupe commutatif incomplet, où la composition n'est définie que si les deux "endo" composants ont des ordres premiers entre eux. L'"endo" unité est le quasigroupe du premier ordre $0 \times 0 = 0$. Un "endo" n'a pas d'inverse; mais la loi d'existence du quotient est satisfaite toutes les fois que l'ordre de l'"endo" dividende, n, est un multiple de l'ordre, k, de l'"endo" diviseur, avec $n = ks$ et $(k,s) = 1$. Quand le quotient existe il est unique. Ce semi-groupe incomplet est homomorphe au semi-groupe multiplicatif des entiers naturels, dans lequel la multiplication est supposée n'être définie que si les deux facteurs sont premiers entre eux. Tous les "endo" d'un ordre déterminé, n, se projettent sur l'élément n.

22. Lemme. *Si* $d = a^{\alpha'}b^{\beta'}c^{\gamma'} \ldots$ *est un diviseur de* $n = a^{\alpha}b^{\beta}c^{\gamma} \ldots$ ($a, b, c \ldots$ *premiers inégaux*), *alors tout multiple de* d, *inférieur à* n, *a pour décomposition suivant le* N° 19

$$B = (n/a^{\alpha})a^{\alpha'}u + (n/b^{\beta})b^{\beta'}v + \ldots \pmod{n}$$

où u *est défini modulo*

$$a^{\alpha-\alpha'},$$

v *modulo*

$$b^{\beta-\beta'}, \ldots ;$$

et tout nombre ayant une telle décomposition est multiple de d.

On vérifie aisément que B est multiple de toutes les

$$a^{\alpha'}.$$

23. Diviseur engendré par deux autres. *Le sous-quasigroupe engendré dans un "endo"* $Q(*)$, *d'ordre* n, *par les diviseurs* $D_d = [0, d, 2d, \ldots, n-d]$ *et* $D_{d'} = [0, d', 2d', \ldots n-d']$, $(d|n, d'|n)$, *est le diviseur* $D_{d''} = [0, d'', 2d'', \ldots n-d'']$, *où* $d'' = (d, d')$.

Preuve. Soit

$$d' = a^{\alpha''}b^{\beta''}c^{\gamma''} \ldots$$

et P le produit, dans $Q(*)$, d'un multiple de d par un multiple de d',

$$P = [\sum (n/a^{\alpha})a^{\alpha'}u) * (\sum (n/a^{\alpha})a^{\alpha''}u'] \equiv \sum (n/a^{\alpha})(a^{\alpha'}u \times a^{\alpha''}u')_a;$$

$$P = \sum (n/a^{\alpha})a^{\min(\alpha',\alpha'')}(\omega \times \omega')_a \pmod{n},$$

où

$$\omega = u, \omega' = a^{\alpha''-\alpha'}u' \text{ si } \alpha'' \geqslant \alpha'$$

et

$$\omega' = u', \omega = a^{\alpha'-\alpha''}u \text{ si } \alpha'' \leqslant \alpha'.$$

Cela montre que P est multiple de

$$\prod a^{\min(\alpha',\alpha'')} = d'', \qquad (\text{N}^\circ 7)$$

De plus, u décrit toutes les valeurs

$$0, 1, \ldots, a^{\alpha-\alpha'} - 1,$$

et u' toutes les valeurs

$$0, 1, \ldots, a^{\alpha-\alpha''} - 1.$$

Si $\alpha'' \geqslant \alpha'$, ω décrit toutes les valeurs de u et, dans le quasigroupe $(\times)_a$, le produit $(\omega \times \omega')_a$ les parcourt aussi.

Si $\alpha'' \leqslant \alpha'$, ω' décrit les

$$a^{\alpha-\alpha'}$$

valeurs de u' et il en est de même de $(\omega \times \omega')_a$. Donc, dans les deux cas, ce produit prend

$$a^{\alpha-\min(\alpha',\alpha'')}$$

valeurs distinctes. Le nombre des valeurs parcourues par l'élément P, c'est-à-dire l'ordre de

$$\{D_d, D_{d'}\}$$

est

$$\prod \frac{a^\alpha}{a^{\min(\alpha',\alpha'')}} = \frac{n}{d''}.$$

Ce nombre est celui des multiples de d'' dans Q. Ainsi

$$\{D_d, D_{d'}\} = D_{d''}.$$

24. Diviseurs admissibles. Treillis. (i) *Tout diviseur admissible d'un quasigroupe "endo," $Q(*)$, d'ordre n, est composé des multiples d'un entier d, $(d|n)$. On peut dire que ces sous-quasigroupes admissibles sont les idéaux* **(16**, p. 94**)** *de l'"endo."* (ii) *Sur un quasigroupe "endo" d'ordre n, le treillis* (lattice) *des sous-quasigroupes D_d, $(d|n)$, est isomorphe au treillis formé par les sous-groupes du groupe cyclique C_n.*

Preuve. (i) Soit $D = [a, b, c, \ldots]$ un diviseur admissible (au sens de "zulässig", **(14)**). Les endomorphismes de Q projettent D sur l'ensemble des éléments $am, bm, cm, \ldots$ quel que soit $m \in Q$. Donc D contient, en même temps que a, tous les nombres $[a, 2a, 3a, \ldots, (n-1)a, 0]$, autrement dit $Dx \subseteq D$ pour tout $x \in Q$.

Soit $(a,n) = d$. Cette suite contient seulement n/d termes distincts (mod n), à savoir $[0, d, 2d, \ldots, n-d]$, à l'ordre près. Donc D contient le diviseur D_d formé par les multiples de d.

Si cet ensemble n'épuise pas tous les éléments de D, soit $b \in D$ et non multiple de d. Désignons par d' le $PGCD$ de b et de n, $(b,n) = d'$. Alors D

https://doi.org/10.4153/CJM-1958-032-8 Published online by Cambridge University Press

contiendra à la fois tous les multiples de d et, pour la même raison, tous les multiples de d', et par conséquent le sous-quasigroupe engendré par les multiples de d et de d', lequel est formé (N° 23) par l'ensemble des multiples de (d,d'). En répétant ce raisonnement jusqu'à ce que tous les éléments de D soient épuisés, on voit que D est le sous-quasigroupe composé des multiples d'un diviseur de n. (ii) Il est clair, d'autre part, que

$$D_d \cap D_{d'} = D_\Delta,$$

où Δ est le $PPCM$ de d et d'.

25. Décomposition en p-quasigroupes. *Dans tout quasigroupe $Q(*)$ "endo" d'ordre n $(n = a^\alpha b^\beta c^\gamma \dots)$, le sous-quasigroupe $\{A\}$, engendré par l'élément $A = \Sigma_a(n/a^\alpha)x$, est le produit direct des diviseurs engendrés par les éléments x, respectivement dans chaque quasigroupe $(x \times x')_a$, d'ordre a^α.*

Preuve. Pour construire $\{A\}$ il faut former les puissances de A, puis les produits de ces puissances deux à deux, et ainsi de suite, jusqu'à fermeture. Or

$$A * A = (n/a^\alpha)(x \times x)_a + (n/b^\beta)(y \times y)_b + \dots .$$

Pendant ces opérations successives, l'élément x, dans le quasigroupe "endo" $(x \times x')_a$ d'ordre a^α, engendre un diviseur d'ordre a'. De même $\{y\}$, dans $(y \times y')_b$ est un diviseur d'ordre b', etc. Donc $\{A\}$ sera le produit direct, d'ordre $a'b'c' \dots$, de ces divers quasigroupes; symboliquement

$$\{A\} = \Sigma(n/a^\alpha)\{x\}.$$

Ainsi les problèmes de construire un "endo" d'ordre donné et de trouver ses diviseurs monogènes, sont ramenés aux problèmes analogues pour les quasigroupes "endo" dont l'ordre est une puissance d'un nombre premier, ou *p-quasigroupes.*

V. P-QUASIGROUPES "ENDO"

26. Isotopie. Soit $Q(\times)$ un "endo" d'ordre $n = p^\alpha$ où p est premier. On a vu (N° 15) que, pour toute valeur β $(0 \leqslant \beta < \alpha)$ le diviseur $D_\beta = [0, p^\beta, 2p^\beta, \dots, n-p^\beta]$ est normal; les cosets sont

$$C_{\beta,i} = [i, i + p^\beta, i + 2p^\beta, \dots, i + n - p^\beta] \qquad (i = [0, 1, \dots, p^\beta - 1]).$$

et l'on a

$$C_{\beta,i} \times C_{\beta,j} = C_{\beta,i\times j}.$$

Le quasigroupe quotient est isomorphe au diviseur $D_{\alpha-\beta}$ et aussi à l'ensemble produit $R_\beta \times R_\beta (\mathrm{mod}\ p^\beta)$, où R_β est l'ensemble des restes $[0, 1, \dots, p^\beta - 1]$. (On le voit en intervertissant k et d dans le N° 15 (iv).) Enfin, $D_{\alpha-\beta} = [0, p^{\alpha-\beta}, 2p^{\alpha-\beta}, \dots, (p^\beta - 1)p^{\alpha-\beta}]$ se projette par $(x \to x/p^{\alpha-\beta})$ sur un quasigroupe d'ordre p^β, "endo."

Exemple. Soit le quasigroupe "endo" $Q = [0, 1, 2, \ldots, 8]$ défini par $1 \times Q = [2, 1, 3, 5, 7, 6, 8, 4, 0]$; $Q \times 1 = [5, 1, 3, 8, 7, 6, 2, 4, 0]$. $D_1 = [0, 3, 6]$. L'ensemble produit $[0, 1, 2] \times [0, 1, 2]$ est isomorphe (mod 3) à D_1: $R \times R = D_1(3x \to x)$. En posant $C_0 = [0, 3, 6]$; $C_1 = [1, 4, 7]$; $C_2 = [2, 5, 8]$, le quasigroupe quotient est $(C_0, C_1, C_2) \cong D_1$.

THÉORÈME. *Si $Q(\times)$ est un quasigroupe "endo" d'ordre $n = p^\alpha$, (p premier)* (i) *par l'application $(x \to k)$, où k est le quotient entier $[x/p^\beta]$ de x par p^β, l'ensemble produit des cosets $C_{\beta,i} \times C_{\beta,j} = C_{\beta,r}$, où $r = i \times j$ et $i, j, r \neq 0$, $C_{\beta,i} = [i,\ i + p^\beta,\ i + 2p^\beta, \ldots, i + kp^\beta, \ldots, i + n - p^\beta]$, se projette sur un quasigroupe $G_{i,j}(.)$ d'ordre $p^{\alpha-\beta}$. Si $\alpha \geqslant 2\beta$, G est invariant par l'autotopie* **(1)**

$$A\left\{\xi = \begin{pmatrix} x \\ x + hi \end{pmatrix}, \eta = \begin{pmatrix} y \\ y + hj \end{pmatrix}, \zeta = \begin{pmatrix} z \\ z + hr \end{pmatrix}\right\}$$

où $h = p^{\alpha-2\beta}$.

(ii) *Si $\beta = \alpha - 1$ et $D = [0, p^{\alpha-1}, 2p^{\alpha-1}, \ldots, kp^{\alpha-1}, \ldots, (p-1)p^{\alpha-1}]$, le quasigroupe quotient Q/D est isomorphe à $D_1 = [0, p, 2p, \ldots, n-p]$ et se projette par $(x \to x/p)$ sur un quasigroupe "endo" d'ordre $p^{\alpha-1}$. Si $i, j, r \neq 0$, $G_{i,j}(.)$ est isotope par*

$$T\left\{\xi = \begin{pmatrix} x \\ xi' \end{pmatrix},\ \eta = \begin{pmatrix} y \\ yj' \end{pmatrix},\ \zeta = \begin{pmatrix} z \\ zr' \end{pmatrix}\right\}$$
$$ii' \equiv jj' \equiv rr' \equiv 1 \pmod{p}$$

à un quasigroupe automorphe par le groupe cyclique **(12)**

(iii) *Si $j = 0$, et $i, r \neq 0$, $G_{i,0}(.)$ est isotope par*

$$T'\left\{\xi' = \begin{pmatrix} x \\ xi' \end{pmatrix}, \eta' = \begin{pmatrix} y \\ 0.y \end{pmatrix}\zeta', \zeta' = \begin{pmatrix} z \\ zr' \end{pmatrix}\right\}$$

au groupe cyclique $x \wedge y = x + y \pmod{p}$. On a un résultat symétrique si $i = 0$, au lieu de j.

(iv) *Si $r = 0$ et $i, j \neq 0$, $G_{i,j}(.)$ est isotope au même groupe cyclique par*

$$T''\left\{\xi'' = \begin{pmatrix} x \\ xi' \end{pmatrix}, \eta'' = \begin{pmatrix} y \\ - yj' \end{pmatrix}, \zeta'' = \begin{pmatrix} z.0 \\ zi' \end{pmatrix}\right\}$$

(v) *Si $r = j = i = 0$, $G_{0,0}(.) \cong D$ par $(x \to x/p^{\alpha-1})$*

Preuve. (i) Considérons l'ensemble produit

$$C_{\beta,i} \times C_{\beta,j} = C_{\beta,r}, \qquad r = i \times j,$$

dans la partition régulière définie par D_β. On a

$$(i + kp^\beta) \times (j + k'p^\beta) \equiv r + k''p^\beta \pmod{p^\beta}.$$

Appliquons l'endomorphisme et multiplions par $(p^{\alpha-\beta} + 1)$:

$$(i + kp^\beta)(p^{\alpha-\beta} + 1) \equiv i + ip^{\alpha-\beta} + kp^\beta \equiv i + (k + ip^{\alpha-2\beta})p^\beta \pmod{p^\alpha}$$
$$[i + (k + ip^{\alpha-2\beta})p^\beta] \times [j + (k' + jp^{\alpha-2\beta})p^\beta) = r + (k'' + rp^{\alpha-2\beta})p^\beta$$

Ainsi le quasigroupe $G_{i,j}(.)$ obtenu en retranchant i à tous les éléments du multiplicande, j à tous ceux du multiplicateur, r à tous les produits, puis en divisant les restes par p^β, $G = [0, 1, 2, \ldots, p^{\alpha-\beta} - 1]$, satisfait à la relation

$$k.k' = k'' \Rightarrow (k + ih).(k' + jh) = k'' + rh \qquad (\text{mod } p^{\alpha-\beta})$$

où $h = p^{\alpha-2\beta}$. Il coïncide avec lui-même par une isotopie dont les trois composantes sont des substitutions régulières **(4**, p. 162.**)**:

$$A\left\{\xi = \begin{pmatrix} x \\ x + hi \end{pmatrix}; \eta = \begin{pmatrix} y \\ y + hj \end{pmatrix}; \zeta = \begin{pmatrix} z \\ z + hr \end{pmatrix}\right\} \qquad (\text{mod } p^{\alpha-\beta})$$

En particulier, si $i = j = r$, l'autotopie devient un automorphisme par un diviseur du groupe cyclique.

(ii) Soit $\beta = \alpha - 1$ et appelons D le diviseur d'ordre p

$$D = [0, p^{\alpha-1}, 2p^{\alpha-1}, 3p^{\alpha-1}, \ldots, kp^{\alpha-1}, \ldots, (p-1)p^{\alpha-1}].$$

Il définit une partition régulière; les cosets sont

$$C_{\alpha-1,i} = [i, i + p^{\alpha-1}, i + 2p^{\alpha-1}, \ldots, i + p^{\alpha-1}k, \ldots, i + (p-1)p^{\alpha-1}].$$

Considérons l'ensemble produit

$$(1) \qquad C_{\alpha-1,i} \times C_{\alpha-1,j} = C_{\alpha-1,r}; \quad i \times j = r \qquad (\text{mod } p^{\alpha-1}).$$

On a

$$(kp^{\alpha-1} + i) \times (k'p^{\alpha-1} + j) = k''p^{\alpha-1} + r \qquad (\text{mod. } p^\alpha)$$

Multiplions les trois éléments par $1 + p^{\alpha-1}$

$$(kp^{\alpha-1} + i)\,(1 + p^{\alpha-1}) \equiv i + p^{\alpha-1}(k + i) \qquad (\text{mod } p^\alpha)$$

car $p^{2\alpha-2} \equiv 0 \pmod{p^\alpha}$ puisque $\alpha > 1$.

Donc, en appliquant l'endomorphisme

$$(2) \qquad [p^{\alpha-1}(k + i) + i] \times [p^{\alpha-1}(k' + j) + j] \equiv p^{\alpha-1}(k'' + r) + r \pmod{p^\alpha}$$

Formons le quasigroupe $G(.)$ d'ordre p, $(G = [0, 1, 2, \ldots, p-1])$ déduit de $C_i \times C_j$ par $x \to [x/p^{\alpha-1}]$

$$G = (C_i \times C_j)\begin{pmatrix} x \\ k \end{pmatrix};$$

d'après (2), G jouit de la propriété

$$(3) \qquad k.k' = k'' \Rightarrow (k + i).(k' + j) = k'' + r \qquad (\text{mod } p)$$

Il coïncide avec lui-même par l'isotopie **(1)** dont les composantes sont trois substitutions circulaires

$$A\left\{\xi = \begin{pmatrix} x \\ x + i \end{pmatrix}; \eta = \begin{pmatrix} y \\ y + j \end{pmatrix}; \zeta = \begin{pmatrix} z \\ z + r \end{pmatrix}\right\} \qquad (\text{mod } p)$$

Si $i = j = r$, l'autotopie A devient un automorphisme par le groupe cyclique.

Supposons $i, j, r \neq 0$ et faisons subir à $G(.)$ l'isotopie

$$T\left\{\xi = \begin{pmatrix} x \\ xi' \end{pmatrix} ; \eta = \begin{pmatrix} y \\ yj' \end{pmatrix} ; \zeta = \begin{pmatrix} z \\ zr' \end{pmatrix}\right\} \qquad (\text{mod } p)$$

où i', j', r' sont les associés de i, j, r: $ii' \equiv jj' \equiv rr' \equiv 1 \pmod{p}$. Soit $\Gamma\ (*)$ l'image de G par T: $\Gamma = G_T$.

Dans l'autotopie A, l'image de x est $x + i$, dans Γ l'image de xi' est $(x + i)$ $i' = xi' + 1$. Donc Γ est invariant par l'autotopie

$$\left\{\begin{pmatrix} x \\ x+1 \end{pmatrix}, \begin{pmatrix} y \\ y+1 \end{pmatrix}, \begin{pmatrix} z \\ z+1 \end{pmatrix}\right\}$$

c'est-à-dire qu'il est automorphe par le groupe cyclique.

(iii) Supposons une des trois quantitités i, j, r, et une seule, par exemple j, nulle. $G_{i,0}$ est toujours automorphe par:

$$A\left\{\xi = \begin{pmatrix} x \\ x+i \end{pmatrix}, \eta = \begin{pmatrix} y \\ y \end{pmatrix}, \zeta = \begin{pmatrix} z \\ z+r \end{pmatrix}\right\}.$$

Faisons l'isotopie:

$$T_1\left\{\xi_1 = \begin{pmatrix} x \\ xi' \end{pmatrix}, \eta_1 = \begin{pmatrix} y \\ y \end{pmatrix}, \zeta_1 = \begin{pmatrix} z \\ zr' \end{pmatrix}\right\};$$

nous obtenons un quasigroupe $\Gamma_1(*) = GT_1$, qui est cette fois invariant par l'autotopie

$$\left\{\begin{pmatrix} x \\ x+1 \end{pmatrix}, \begin{pmatrix} y \\ y \end{pmatrix}, \begin{pmatrix} z \\ z+1 \end{pmatrix}\right\}$$

car la relation $x.y = z \Rightarrow (x + i).y = z + r$, devient par T_1 $xi'*y = zr' \Rightarrow$ $(xi' + 1)*y = zr' + 1$. Donc $x*y = z \Rightarrow (x + 1)*y = z + 1$.

Exemple. Γ_1: $x*y \equiv x + 3y + 3 \pmod 5$.

Or si $0*y = a$, on aura: $x*y = a + x$, donc si l'on applique à Γ_1 l'isotopie.

$$T_2\left\{\begin{pmatrix} x \\ x \end{pmatrix}, \begin{pmatrix} y \\ a \end{pmatrix}, \begin{pmatrix} z \\ z \end{pmatrix}\right\},$$

on aboutira à un quasigroupe $\Gamma\ (\wedge)$ tel que: $x \wedge a = x + a$,
ce qui est le groupe cyclique d'ordre p. Or

$$\begin{pmatrix} y \\ a \end{pmatrix} \to \begin{pmatrix} y \\ 0*y \end{pmatrix} = \begin{pmatrix} y \\ 0.y \end{pmatrix} \zeta'$$

donc enfin

$$\Gamma = GT_1T_2,\ T_1T_2 = T' : \left\{\xi' = \begin{pmatrix} x \\ xi' \end{pmatrix}, \eta' = \begin{pmatrix} y \\ 0.y \end{pmatrix}\zeta', \zeta' = \begin{pmatrix} z \\ zr' \end{pmatrix}\right\}$$

Si l'élément nul est i à la place de j on arrive à une conclusion symétrique.

Exemple. $n = 25$; $C_0 = [0, 5, 10, 15, 20]$; $C_2 = [2, 7, 12, 17, 22]$; $C_2 \times 0 = [14, 24, 9, 19, 4]$; $C_2 \times 5 = [24, 9, 19, 4, 14]$; $C_2 \times 10 = [9, 19, 4, 14, 24]$; $C_2 \times 15 = [4, 14, 24, 9, 19]$; $C_2 \times 20 = [19, 4, 14, 24, 9]$; $i = 2, j = 0, r = 4$. Le quasigroupe $G_{2,0}(.)$ est $G = [0, 1, 2, 3, 4]$; $G.0 = [2, 4, 1, 3, 0]$; $G.1 = [4, 1, 3, 0, 2]$; $G.2 = [1, 3, 0, 2, 4]$; $G.3 = [0, 2, 4, 1, 3]$; $G.4 = [3, 0, 2, 4, 1]$;

$$T'\left\{\xi' = \begin{pmatrix} 0\,1\,2\,3\,4 \\ 0\,3\,1\,4\,2 \end{pmatrix}, \eta' = \begin{pmatrix} 0\,1\,2\,3\,4 \\ 3\,1\,4\,0\,2 \end{pmatrix}, \zeta' = \begin{pmatrix} 0\,1\,2\,3\,4 \\ 0\,4\,3\,2\,1 \end{pmatrix}\right\}$$

$\Gamma = G_T$, est le groupe cyclique additif de $Z/5$.

(iv) Si $i, j \neq 0$ et $r = 0$, $G(.)$ est invariant par l'autotopie

$$A\left\{\xi = \begin{pmatrix} x \\ x + i \end{pmatrix}, \eta = \begin{pmatrix} y \\ y + j \end{pmatrix}, \zeta = \begin{pmatrix} z \\ z \end{pmatrix}\right\}.$$

Faisons l'isotopie

$$R_1\left\{\xi_1 = \begin{pmatrix} x \\ xi' \end{pmatrix}, \eta_1 = \begin{pmatrix} y \\ yj' \end{pmatrix}, \zeta_1 = \begin{pmatrix} z \\ z \end{pmatrix}\right\},$$

nous obtenons le quasigroupe $\Omega\ (*) = G_{R1}$. La condition

$$(x + i) \cdot (y + j) = x.y$$

devient par R_1 $(x + 1)*(y + 1) = x*y$.

Si l'on fait subir à Ω une nouvelle isotopie

$$R_2\left\{\xi_2 = 1, \eta_2 = \begin{pmatrix} y \\ -\,y \end{pmatrix}, \zeta_2 = \begin{pmatrix} z*0 \\ z \end{pmatrix}\right\}$$

on obtiendra le groupe cyclique $\Gamma : x \wedge y = x + y \pmod{p}$. Finalement, $G(.)$, multiplié par l'isotopie $R_1R_2 = T''$

$$T''\left\{\xi'' = \begin{pmatrix} x \\ xi' \end{pmatrix}, \eta'' = \begin{pmatrix} y \\ -\,yj' \end{pmatrix}, \zeta'' = \begin{pmatrix} z.0 \\ zi' \end{pmatrix}\right\}$$

devient le groupe cyclique.

Exemple. Soit le quasigroupe "endo" d'ordre 25, défini par $[0, 5, 10, 15, 20] \times 1 = [16, 1, 6, 21, 11]$; $1 \times [0, 5, 10, 15, 20] = [7, 17, 22, 12, 2]$; $[1, 6, 11, 16, 21] \times 1 = [9, 14, 19, 24, 4]$; $[2, 7, 12, 17, 22] \times 1 = [10, 0, 15, 5, 20]$; $[3, 8, 13, 18, 23] \times 1 = [18, 8, 23, 13, 3]$, et $[4, 9, 14, 19, 24] \times 1 = [17, 22, 2, 7, 12]$. On a $G_{4,2} = [0, 1, 2, 3, 4]$; $G.0. = [4, 2, 0, 3, 1]$; $G.1 = [3, 1, 4, 2, 0]$; $G.2 = [2, 0, 3, 1, 4]$; $G.3 = [1, 4, 2, 0, 3]$; $G.4 = [0, 3, 1, 4, 2]$. On en tire $\Omega = [0, 1, 2, 3, 4]$; $\Omega *0 = [4, 1, 3, 0, 2]$; $\Omega *1 = [2, 4, 1, 3, 0,]$; $\Omega *2 = [0, 2, 4, 1, 3]$; $\Omega *3 = [3, 0, 2, 4, 1]$; $\Omega *4 = [1, 3, 0, 2, 4]$. Et Ω_{R2} est le groupe cyclique d'ordre 5.

(v) Si enfin deux nombres sont nuls, le troisième l'est aussi et $i = j = r = 0$. $G_{0,0}$ coïncide avec l' "endo" d'ordre p isomorphe à D par $(x \to x/p^{\alpha-1})$.

Ce théorème permet de construire par récurrence les "endo" d'ordre p^2, p^3, ... à partir des "endo" d'ordre p. La construction des "endo" d'ordre premier résulte de la proposition suivante.

27. Cas où n est premier. *Pour qu'un groupoïde $G(\times)$, d'ordre premier, p, automorphe par le groupe géométrique (et par conséquent "endo") soit un quasigroupe, il faut et il suffit que les fonctions*

$$x \times 1 = f(x) \text{ et } x'f(x),\ xx' \equiv 1 \pmod{p},$$

définissent deux substitutions $(x \to f(x))$et $(x \to x'f(x))$, où la valeur de $x'f(x)$ correspondant à $x = 0$ est conventionnellement prise égale à celui des nombres $0, 1, 2, \ldots, p-1$ qui ne figure pas parmi les $p-1$ valeurs de $x'f(x)$. Le quasigroupe est alors entièrement déterminé par la fonction $f(x)$.

Exemple.

$$\begin{aligned} x &= [0, 1, 2, 3, 4, 5, 6] \pmod 7. \\ f(x) &= (3, 5, 2, 4, 1, 6, 0] \\ x' &= [-, 1, 4, 5, 2, 3, 6] \\ x'f(x) &= [-, 5, 1, 6, 2, 4, 0];\ x'f\ (0) = 3 \end{aligned}$$

(*cf.* N° 4, Exemple II).

La démonstration directe de cette proposition est facile, mais lourde; la propriété résulte d'ailleurs immédiatement, par le N° 4, de l'énoncé corrélatif dans le cas des groupoïdes automorphes par le groupe cyclique **(12**, N° 6**)**.

Si un quasigroupe d'ordre premier est monogène, il est clair que son automorphe se réduit au seul groupe géométrique. Mais cette condition n'est pas nécessaire et l'on peut construire des quasigroupes d'ordre premier, possédant des diviseurs, et dont le groupe d'automorphisme se réduise néanmoins au groupe géométrique. Ainsi le quasigroupe "endo" du $19^{\text{ème}}$ ordre défini par la substitution

$$(x \to x \times 1) = (0, 18, 13, 17, 2, 10, 6, 16, 15, 3, 5, 12, 9)(1, 7)(4, 8, 14)(11),$$

écrite sous forme de produit de cycles, admet six diviseurs monogènes isomorphes du $3^{\text{ème}}$ ordre: [1, 7, 11] et ses produits par 2, 4, 5, 8 et 10: [2, 14, 3], [4, 9, 6], [5, 16, 17], [8, 18, 12], et [10, 13, 15]. Son automorphe se réduit aux 18 transformations $(x \to mx)$, $(m = [1, 2, 3, \ldots, 18])$. En effet, parmi les séries des multiplications à droite **(13**, N° 7-8**)**, une seule est d'ordre 18; elle est formée par les puissances de 2 (mod 19). Comme elle doit se projeter sur elle-même par tout automorphisme, A_Q est d'ordre 18.

Citations

1. A. A. Albert, *Non-associative algebras I.* Ann. Math., *43* (1942), 696.
2. ———, *Quasigroups*, Trans. Amer. Math. Soc., *54* (1943), 510.
3. C. Burstin, W. Mayer, *Distributive Gruppen von endlicher Ordnung*, J. reine ang. Math., *160* (1929), 111–130.
4. A. Cauchy, *Exercices d'Analyse et de Phys. Math.* III (Paris, 1844).
5. L. E. Dickson, *History of the Theory of Numbers*, II (New York, 1952).
6. R. A. Good, *On the theory of clusters*, Trans. Amer. Math. Soc., *63* (1948), 482–513.
7. G. H. Hardy and E. M. Wright, *Number theory* (Oxford, 2ème édit., 1953).
8. B. A. Hausmann, O. Ore, *Theory of quasigroups*, Amer. J. Math., *59* (1937), 983–1004.
9. D. C. Murdoch, *Structure of Abelian quasigroups*, Trans. Amer. Math. Soc., *49* (1941), 395.
10. L. J. Paige, *Neofields*, Duke Math. J., *16* (1949), 39–60.
11. A. Sade, *Quasigroupes* (Marseille, 1950).
12. ———, *Groupoïdes automorphes par le groupe cyclique*, Can. J. Math., *9* (1957), 321–335.
13. ———, *Quelques remarques sur l'isomorphisme et l'automorphisme des quasigroupes.* Abh. Math. Sem. Univ. Hamburg (1958).
14. O. Schmidt. Math. Z., *29* (1929), 34–41.
15. G. Scorza. *Gruppi Astratti* (Roma, 1942).
16. M. F. Smiley. *Application of a radical of Brown, McCoy to non-associative rings*, Amer. J. Math., *72* (1950), 93–100.
17. B. M. Stewart, *Theory of Numbers.*
18. A. Suschkewitsch, *Ueber die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit*, Math. Ann., *99* (1928), 33.
19. M. Takasaki, *Abstraction of symmetric transformations*, Tôhoku Math. J., *49* (1943), 145–207.

Lycee Perier, Marseille