GROUPOÏDES AUTOMORPHES PAR LE GROUPE CYCLIQUE

A. SADE

I. Introduction

1. *Définitions.* Nous appellerons *groupoïde* un ensemble non vide, G, muni d'une loi $(\times)$ faisant correspondre à tout couple ordonné $x, y \in G$, *au plus* un élément z de G, appelé produit de x par y, et satisfaisant à la loi d'homogénéité **(2)**. Si E est l'ensemble des z la loi $(\times)$ définit une *application de E sur G.* On dira que G est *incomplet* si $E \subset GG$ et *ordinaire* si $E = GG$.

Un *semi-groupe* **(5)** est un groupoïde associatif.

Un *quasigroupe*, ordinaire ou incomplet, est un groupoïde dont les éléments ont *au plus* un quotient à droite et un quotient à gauche. Le mot "diviseur" sera entendu au sens de "sous-quasigroupe".

Soit Q un groupe additif d'entiers, ou d'entiers mod. n, et T un sous-groupe de Q. Soit $(\times)$ une loi binaire des éléments de Q telle que:

(1) Q soit un groupoïde,

(2) l'application $x \to x + t$, $t \in T$, soit un automorphisme de Q. La structure ainsi définie est appelée un *groupoïde automorphe par le groupe cyclique T* et est désignée par $Q(\times)$. Si $Q = T$ on dira que $Q(\times)$ est *automorphe par le groupe cyclique.*

2. *Exemple* I. L'ensemble des nombres rationnels muni de la loi:

$$x \times y = \tfrac{1}{2}(x + y) + C$$

3. *Exemple* II. Le quasigroupe:

$$x \times y = -(x - y - 1)^4 + 4(x - y - 1) + y + 5 \pmod 7$$

4. *Un groupoïde $G(\times)$ automorphe par le groupe cyclique est entièrement défini par la fonction $f(x) = x \times 0$,* ou par l'application

$$S: \quad x \to xS = f(x),$$

d'un certain sous-ensemble de G, dans G; la fonction $f(x)$ étant définie pour tout élément de ce sous-ensemble.

5. La condition exprimant qu'un groupoïde, automorphe par le groupe cyclique, est un semi-groupe n'est pas simple. Bornons-nous à ce résultat: *Il n'existe aucun groupe automorphe par le groupe cyclique.*

Reçu le 7 avril, 1956.

6. *Pour qu'un groupoïde $G(\times)$, automorphe par le groupe cyclique, soit un quasigroupe il faut et il suffit que la fonction $x \times 0 = f(x)$ satisfasse aux deux conditions* :

$$(3) \qquad \begin{cases} \text{(i)} \ f(x) = f(y) \rightleftarrows x = y \\ \text{(ii)} \ x - f(x) = y - f(y) \rightleftarrows x = y \end{cases}$$

(mod. n si G est fini et d'ordre n.)

La première exprime la loi de cancellation à droite (N° 1) pour $y = 0$. Montrons qu'elle est obéie par deux facteurs quelconques. L'égalité:

$$x \times a = y \times a,$$

s'écrit, en vertu de l'automorphisme:

$$(x - a) \times 0 + a = (y - a) \times 0 + a$$
$$f(x - a) = f(y - a)$$

Donc (i) $$x = y.$$

(mod. n si G est fini.)

La seconde exprime la loi de cancellation à gauche.

Les réciproques sont immédiates.

7. Les quasigroupes infinis, automorphes par le groupe cyclique, ont peu de propriétés. Toute fonction $f(x)$ ayant une dérivée toujours négative, ou toujours plus grande que un, ou toujours comprise entre 0 et 1, fournit une solution.

8. *Tout quasigroupe ordinaire fini, automorphe par le groupe cyclique, est d'ordre impair.*

Le quasigroupe étant ordinaire, $f(x)$ décrit toutes les valeurs de x; donc, en désignant par n l'ordre du quasigroupe:

$$\Sigma f(x) = 0 + 1 + 2 + \ldots + (n - 1) = S \qquad \text{(mod. } n\text{)}.$$

D'après (ii), N° 6, la fonction $x - f(x)$ décrit ce même ensemble, donc:

$$\Sigma [x - f(x)] = S = S - S \qquad \text{(mod. } n\text{)},$$
$$S = n(n - 1)/2 \equiv 0 \qquad \text{(mod. } n\text{)}$$

$n = 2M + 1$.

Mais il existe des quasigroupes d'ordre pair *incomplets*, automorphes par le groupe cyclique.

Exemples: $x = 0\ 1\ 2\ 3$; et $x = 0\ 1\ 2\ 3\ 4\ 5$
$f(x) = 2\ 0\ -\ 3$ $f(x) = 5\ 4\ 2\ -\ 0\ 3.$

Le quasigroupe incomplet du 6ième ordre: $x = 0\,1\,2\,3\,4\,5$; $x \times 0 = 3\,0\,1\,4\,2\,5$; $x \times 1 = 1\,5\,2\,-\,0\,-$; $x \times 2 = 4\,1\,5\,2\,3\,0$; $x \times 3 = 2\,-\,3\,1\,4\,-$; $x \times 4 = 5\,2\,0\,3\,1\,4$; $x \times 5 = 0\,-\,4\,-\,5\,3$, est automorphe par le sous-groupe du 3e ordre du groupe cyclique:

$$T = 024.135;\ T^2;\ T^3 = 1.$$

https://doi.org/10.4153/CJM-1957-039-3 Published online by Cambridge University Press

Il existe un quasigroupe ordinaire, automorphe par $x \to x + i$, $(i = 0, 3, 6)$ et défini par:

$$x = 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ ; \qquad x \times 1 = 2\ 6\ 1\ 7\ 3\ 0\ 4\ 8\ 5$$
$$f(x) = 6\ 1\ 5\ 3\ 2\ 7\ 0\ 4\ 8\ ; \qquad x \times 2 = 8\ 5\ 3\ 4\ 7\ 1\ 2\ 0\ 6.$$

II. Transformations préservant l'invariance par le groupe cyclique.

9. D'après le N° 4 on peut identifier tout quasigroupe automorphe par le groupe cyclique avec la fonction correspondante:

$$x \times 0 = f(x)$$

et parler du quasigroupe $f(x)$ mod. n. On peut même le représenter par la substitution $x \to f(x)$ mise sous la forme de produit de cycles.

10. *Si $f(x)$ définit un quasigroupe automorphe par le groupe cyclique, les fonctions*:

a:	$x - f(x)$,	
b:	$-f(-x)$,	
$ab = ba$:	$x + f(-x)$	(conjoint **(3** p. 60, N° 75**)**),
c:	$f^{-1}(x)$	(réciproque),
D_h:	$f(x + h)$,	
E_h:	$f(x) + h$,	

jouissent de la même propriété.

Soit $f(x)$ une fonction satisfaisant aux conditions (3) du N° 6. Alors,

$$(a) \qquad g(x) = x - f(x)$$

sera encore une solution, car

$$(i) \qquad g(x) = g(y) \rightleftarrows x - f(x) = y - f(x) \rightleftarrows x = y,$$

puisque $f(x)$ est une solution.

$$(ii) \qquad x - g(x) = f(x),$$

donc

$$x - g(x) = y - g(y) \rightleftarrows f(x) = f(y) \rightleftarrows x = y.$$

Les autres parties s'établissent de manière analogue.

Si $f(x)$ est d'ordre n, les n opérations E_h, $(h = 0, 1, \ldots, n - 1)$ forment un groupe cyclique car, si l'on désigne chaque opération par la valeur correspondante de h, ce groupe est isomorphe au groupe additif des restes, mod. n.

11. *Groupes formés par les opérations précédentes.* Considérons l'ensemble F de toutes les fonctions $f(x)$ solutions des conditions (3) pour une valeur donnée de n. Chacune de ces opérations a, b, c, D, E fait correspondre à chaque $f(x)$ une $f(x)$ et une seule et réciproquement. Ce sont des transformations de F. Elles forment un groupe, sous-groupe du groupe total **(8**, p. 3**)**.

https://doi.org/10.4153/CJM-1957-039-3 Published online by Cambridge University Press

Les opérations a, b et les opérations b, c engendrent deux *groupes carrés*. En effet, $ab = ba$ (N° 10), et $bc = cb$, car l'une comme l'autre transforme $x \to f(x)$ en $x \to -f^{-1}(-x)$.

L'opération $ca = (ac)^{-1}$ *est du* $6^{\text{ème}}$ *ordre et* $(ca)^3 = b$.
Les opérations a, b, c *engendrent un groupe diédral du* 12^{me} *ordre*, défini par:

$$ab = ba,\ bc = cb,\ a^2 = b^2 = c^2 = 1,\ (ac)^3 = (ca)^3 = b.$$

12. *Les opérations* E_h *et* D_h *sont transformées l'une de l'autre par* c.

$$c^{-1}E_h c = D_h.$$

13. *D et E sont des isotopies* **(1)**. Si $D_h = E_k$, en posant $f(x + h) = z$ et $f(x) = y$, on aura:

$$f(x + h)E_k = z + k$$

et

$$f(x + h)D_h = y,$$

d'où:

$$y = z + k,$$

ou:

$$f(x) = f(x + h) + k,$$

et enfin

$$f(x) = ax + b \quad (ah + k \equiv 0, \text{ mod. } n).$$

Pour que $f(x)$ et $x - f(x)$ décrivent toutes les valeurs de x il faut de plus que a et $a - 1$ soient premiers avec n. Ainsi:

Les quasigroupes $f(x)$ *pour lesquels toute opération D est aussi une opération E sont* $f(x) = ax + b$, *où a et* $a - 1$ *sont premiers avec n.*

Les opérations (a), (b), (c) du N° 10 laissent cette propriété invariante.
Si $a = (n + 1)/2$, on aura un quasigroupe abélien.

14. Voici les lois de composition de tous les quasigroupes ordinaires, automorphes par le groupe cyclique, jusqu'à $n = 9$. a et $a - 1$ sont premiers avec n, b et c sont quelconques.
Pour toute valeur de n on a d'abord la solution:

$$x \times y = a(x - y) + y + b$$

Pour $n = 7$, on a, en plus:

$$x \times y = \pm(x - y + c)^4 + 4(x - y + c) + y + b.$$

Pour $n = 9$, on trouve 28 solutions, aux isotopies D et E près, dont

$$x \times y = 3(x - y)^2 + 2x - y$$

et

$$x \times 0 = 1 + 6\binom{x}{1} + 7\binom{x}{2} + 2\binom{x}{3} + 5\binom{x}{5} + 3\binom{x}{6} + 6\binom{x}{7}.$$

Quand n est pair, il faut avoir recours à des fonctions irrationnelles. Exemple, $n = 4$:

$$f(x) = x \times 0 = \sqrt{(17x^2 - 41x + 24)/6}$$

représente le quasigroupe du N° 8.

III. Composition des quasigroupes

15. *Si $f(x)$ est un quasigroupe d'ordre p automorphe par le groupe cyclique et si $\rho_x(y)$, $x = 0, 1, \ldots, p-1$, sont p quasigroupes d'ordre m encore automorphes par le groupe cyclique, alors:*

$$F(x + py) = f(x) + p\rho_x(y) \pmod{n}$$

est un quasigroupe d'ordre $n = mp$, automorphe par le groupe cyclique.

Exemple: $f = (01)\,(2)$; $\rho_0 = (0214)\,(3)$; $\rho_1 = (02)\,(34)\,(1)$; $\rho_2 = (0412)\,(3)$.

$X = x + 3y =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$F(X) =$			7	6	14	13	3	8	4	0	2	10	12	11	1	9	5

Quand x décrit le champ $(0, p-1)$ et y le champ $(0, m-1)$, la fonction $f(x)$ d'une part et chacune des fonctions $\rho_x(y)$ de l'autre décrivent respectivement les mêmes champs. Donc F prend toutes les valeurs de 0 à mp − 1 et il en est de même de $x - F(x)$.

16. *Dans les conditions du* N° 15, *il existe une partition régulière sur le quasigroupe $F(X)$. Les p cosets sont les ensembles $x + py$, où y décrit les m valeurs $0,1, \ldots, m-1$. A chaque valeur de x correspond un coset; le système des représentants est $x = 0,1, \ldots, p-1$. Le quasigroupe quotient est isomorphe au quasigroupe $f(x)$. Pour que la partition définisse un diviseur normal* **(4)** *il faut et il suffit que $f(x)$ soit idempotent; tous les cosets sont alors diviseurs normaux.*

Il est d'abord évident que les ensembles $x + py$ sont disjoints car si

$$a + py \equiv b + py' \pmod{mp},$$

on aura

$$a - b \equiv 0 \pmod{p},$$

donc

$$a = b,$$

puisque a et b sont plus petits que p.

Soient $a + py$ un élément du coset $x = a$ et $b + py'$ un élément du coset $x = b$. En notant $(\times)$, $(*)$ et $(\cdot)$ les opérations de f, ρ_{a-b} et $F = f + p\rho$, leur produit sera:

https://doi.org/10.4153/CJM-1957-039-3 Published online by Cambridge University Press

$$\begin{aligned} P = (a + py) \cdot (b + py') &= [a - b + p(y - y')] \cdot 0 + b + py' \\ &= F[a - b + p(y - y')] + b + py' \\ &= f(a - b) + p\rho_{a-b}(y - y') + b + py' \\ &= (a - b) \times 0 + b + p[(y - y') * 0 + y'] \\ P &= a \times b + p(y * y') = c + py''. \end{aligned}$$

Ainsi P appartient au coset représenté par $x = a \times b = c$.

La loi de composition des cosets est la même que celle de leurs représentants et il existe un homomorphisme canonique de F sur f.

Si f n'a aucun élément idempotent, aucun coset n'est fermé. Si un coset est diviseur normal, tous le seront, car si $a \times a = a$, tous les éléments de $f(x)$ seront idempotents, à cause de l'automorphisme $(a + 1) \times (a + 1) = a + 1$.

Exemple. Le quasigroupe examiné au N° 15 et représenté, avec la notation du N° 9, par:

$$F(x) = (0,7)\ (1, 6, 4, 3; 13, 9; 10, 12)\ (2, 14, 5, 8)\ (11)$$

a trois cosets

$$0; 3, 6, 9, 12; \quad 1, 4, 7, 10, 13; \quad \text{et} \quad 2, 5, 8, 11,14,$$

mais $f(x)$ n'ayant aucun élément idempotent, aucun coset n'est diviseur normal; il y a seulement partition régulière et homomorphisme naturel du quasigroupe F sur le quasigroupe quotient, isomorphe à f.

Soit au contraire le quasigroupe défini par:

$$p = 3; \mathrm{m} = 5; f(x) = (12)\ (0); \rho_0 = \rho_1 = \rho_2 = (0)\ (1243);$$

d'où:

$$F = (1,2)\ (3, 6, 12, 9)\ (4; 8, 13, 11)\ (5, 7, 14; 10)\ (0)$$

(Notation du N° 9).

Comme $f(x)$ est idempotent, tous les cosets sont diviseurs normaux.

17. *Si $\rho_x(y)$ ne dépend plus de x, et si l'on considère, pour l'ensemble de tous les nombres entiers $(p = 1,2,3, \ldots,)$ tous les quasigroupes $f(x)$ (mod. p) automorphes par le groupe cyclique d'ordre p, les fonctions f forment un semi-groupe* **(5)** *non commutatif, avec unité bilatère, par rapport à la loi de composition*

$$f*\rho = f + p\rho.$$

Cet ensemble est fermé d'après le N° 15. Il est associatif car, si f, ρ et ψ sont trois fonctions, mod. p, q et r respectivement, on a

$$\begin{aligned} (f*\rho)*\psi &= (f + p\rho)*\psi = f + p\rho + pq\psi \qquad (\text{mod. } pqr), \\ f*(\rho*\psi) &= f*(\rho + q\psi) = f + p\rho + pq\,\psi \qquad (\text{mod. } pqr). \end{aligned}$$

L'unité est la fonction $f = 0$, correspondant au quasigroupe du 1er ordre $0*0 = 0 = u$; elle est bilatère car $f*u = u*f = f$.

18. *Si $p,p',\ldots$ sont des entiers positifs quelconques et si $M = \{p,p',\ldots\}$ est le semi-groupe multiplicatif engendré par ces entiers, l'ensemble des fonctions $f(x)$* (mod. q), *$q \in M$, est un semi-groupe, diviseur du semi-groupe défini au N° précédent.*

Car il est fermé et contient l'unité; il est associatif. En particulier l'ensemble, au sens de la multiplication, $*$, définie au N° 17, des puissances d'une fonction unique $f(x)$, d'ordre q, est isomorphe au semi-groupe additif des entiers. Si l'on pose:

$$f^{*p} = 0 + f + qf + q^2 f + \ldots + q^{p-1} f,$$

alors,

$$f^{*p} * f^{*r} = f^{*(p+r)}.$$

IV. Recherches sur l'automorphe (8, p. 40) de f(x)

19. *Quand un quasigroupe $Q(\times)$, fini ou non, automorphe par toutes les transformations C; $x \to x + h$, est engendré par un de ses éléments, son automorphe se réduit au seul groupe cyclique C.*

Soit $Q = \{a\}$; à cause de l'automorphisme $x \to x - a$, Q est aussi engendré par l'élément zéro. Soit

$$\binom{x}{x'} = H$$

un automorphisme quelconque de Q, et v l'image de 0 par H. On montre par induction que, pour tout x dans Q, on aura: $xH = x' = x + v$.

Soient a et b deux élément de Q pour lesquels on suppose:

$$a' = a + v \text{ et } b' = b + v.$$

En vertu de l'automorphisme C:

$$a' \times b' = (a' - b') \times 0 + b' = (a - b) \times 0 + b + v,$$

et comme

$$a \times b = (a - b) \times 0 + b,$$
$$a' \times b' = a \times b + v.$$

La propriété étant vraie pour $a = b = 0$, et Q étant engendré par 0, la propriété est générale et $H \in C$.

20. En particulier, *si l'une des trois équations*: $0 \times 0 = x$; $x \times 0 = 0$; $0 \times x = 0$ *a pour solution un nombre premier avec n, le quasigroupe $Q(\times)$, d'ordre n, automorphe par le groupe cyclique C, admet C pour automorphe.*

https://doi.org/10.4153/CJM-1957-039-3 Published online by Cambridge University Press

21. *Si un quasigroupe $Q(\times)$ est automorphe par le groupe cyclique, si $0 \times 0 = a$ et si $x \to x'$ est un automorphisme quelconque de Q, on a, pour toute valeur de k;*

$$(ka + r)' = ka + r'.$$

La proposition est évidente si k est nul et on la généralise sans peine par induction.

22. *Si $Q(\times)$ est un quasigroupe d'ordre n, automorphe par le groupe cyclique $C = \{c\}$, $c = 0, 1, \ldots, n-1$, tout diviseur propre D de Q est composé des éléments de une ou plusieurs suites;*

$$i, i + p, i + 2p, \ldots, i + kp, \ldots, i + n - p,$$

où $p|n$ et $i < p$; la valeur de p restant la même pour toutes les suites de D. Il existe p telles suites, disjointes, correspondant aux p valeurs de $i (i = 0,1, \ldots, p-1)$. Enfin, D est automorphe par le diviseur $\{c^p\}$ du groupe cyclique C.

Puisque C opère transitivement sur Q, tout élément de C ne peut pas être un automorphisme de D. Comme les conditions $c^\alpha D = D$ $c^\beta D = D$ impliquent que $c^{\alpha-\beta}D = D$, le sous-ensemble des éléments de C, qui sont des automorphismes de D, forme un sous-groupe. C étant cyclique, ce sous-groupe est de la forme $\{c^p\}$, où $p|n$ et est le plus petit entier satisfaisant à $c^p D = D$

Si D contient l'élément i, il contiendra les $n/p = m$ éléments distincts:

$$i, i + p, i + 2p, \ldots, i + kp, \ldots, i + n - p. \tag{4}$$

L'automorphisme $x \to x + r$, $(r < p)$ transformera D en un diviseur D', pouvant coincïder avec D, qui contiendra les éléments:

$$i + r, p + i + r, \ldots, kp + i + r, \ldots, n - p + i + r. \tag{5}$$

On voit immédiatement que les suites (5) correspondant à des valeurs distinctes de r sont disjointes. Elles réalisent une partition des n éléments de Q, épuisant l'ensemble de ces éléments, puisqu'elles sont disjointes, au nombre de p, et composées de n/p éléments chacune.

23. *Si un quasigroupe $Q(\times)$ d'ordre n, automorphe par le groupe cyclique, $x \to x + h$, n'est engendré par aucun de ses éléments.*

(1) *Chaque élément de Q engendre un diviseur d'ordre constant m $(mp = n)$.*

(2) *Le nombre des diviseurs distincts ainsi définis est p et chacun d'eux est engendré par n'importe quel de ses éléments.*

(3) *Ces p diviseurs sont disjoints, isomorphes entre eux et l'on passe de l'un à tous les autres par les transformations*:

$$x \to x + h \ (h = 0,1,2, \ldots, p-1).$$

(4) *Le diviseur engendré par l'élément* 0 *est*: $D = 0, p, 2p, 3p, \ldots, n - p$, *et on l'obtient en multipliant par* p, *sans changer la loi de composition, un quasi-groupe quelconque d'ordre* m, *automorphe par le seul groupe cyclique d'ordre* m, *c'est-à-dire engendré par un seul de ses éléments.*

(5) *Tous ces diviseurs ont le même automorphe, à savoir le groupe cyclique d'ordre* m:

$$x \to x + kp,\ k = 0,1,2, \ldots, m - 1.$$

Preuve. Soit un quasigroupe $Q(\times)$ d'ordre n, non monogène, et automorphe par le groupe cyclique C: $x \to x + h$; $h = 0,1,2, \ldots, n - 1$. Soit D le sous-quasigroupe propre engendré par l'élément zéro: $\{0\} = D \subset Q$. Si l'on fait subir à D toutes les transformations C, à chaque valeur i de h correspondra un diviseur D_i, isomorphe à D:

$$D_i = D\begin{pmatrix} x \\ x + i \end{pmatrix},$$

et D_i sera engendré par l'élément i de la même manière que D l'était par l'élément 0. On obtiendra ainsi n diviseurs.

Soit a un élément non nul de D, $D_a = \{a\}$. Comme $a \in D$, $D_a \subset D$. Mais $D_a \cong D$, donc $D_a = D$. Ainsi chacun des n diviseurs D_i est engendré par n'importe quel de ses éléments.

Soit p le plus petit élément non nul de $D = \{0\}$. Donc

$$D_p = \{p\} = D = D\begin{pmatrix} x \\ x + p \end{pmatrix}$$

Par suite D contient, outre l'élément zéro, les éléments $p,2p,3p, \ldots, kp; \ldots$ (mod. n), dont le plus petit (mod. n) est p par hypothèse. On voit facilement que $p|n$ et $kp < n$; on peut poser $mp = n$; $k < m$. Supposons alors que D, en plus de $0,p,2p, \ldots, (m - 1)p$, contienne un autre élément q, non multiple de p, par exemple:

$$kp < q < kp + p \leqslant n,$$

l'égalité correspondant au cas où $k = m - 1$.

S'il en était ainsi, le diviseur:

$$D' = D\begin{pmatrix} x \\ x - kp \end{pmatrix}$$

contiendrait l'élément zéro et coïnciderait avec D. D'autre part, il contiendrait l'élément $q - kp$. Or

$$0 < q - kp < p$$

et, contrairement à l'hypothèse, p ne serait pas le plus petit élément non nul de D. Ainsi, $D = 0, p, 2p, \ldots, kp, \ldots, (m - 1)p$.

Chaque diviseur D_i est d'ordre m et le nombre des D_i distincts est p.

D'après le N° précédent ces diviseurs sont disjoints. Si l'on remplace dans D tous les éléments $0,p,2p,\ldots,n-p$ par leurs quotients par p:

$$0,1,2,\ldots,m-1,$$

en respectant la loi de composition de Q, on obtient évidemment un quasi-groupe isomorphe à D par $x \to (x/p)$, dont l'automorphe se réduit (N° 19) au groupe cyclique d'ordre m: $x \to x+k$, $(k = 0, 1,2,\ldots,m-1)$ puisqu'il est engendré par l'un quelconque de ses éléments.

24. *Si un quasigroupe $Q(\times)$ est automorphe par le groupe cyclique et si $D_0, D_1, D_2, \ldots, D_{p-1}$ sont les diviseurs d'ordre $m = n/p$ engendrés par les divers éléments de Q, tout automorphisme T de Q projette chaque diviseur D_i sur un diviseur D_j, l'isomorphisme induit par T entre D_i et D_j étant:*

$$x \to x + j - i \quad (iT = j)$$

L'automorphe de Q induit sur l'ensemble des indices $0,1,2\ldots,p-1$ un groupe de transformations.

Preuve. Soit T un automorphisme de Q et soit a l'image de zéro.

$$0T = a.$$

Alors tous les produits engendrés par 0 se projettent sur les produits engendrés de la même manière par a et tous les éléments de D_0 ont des images bien déterminées et définies par la seule donnée de l'image de 0.

Si $0 \times 0 = kp$, d'après l'automorphisme,

$$a \times a = kp + a,$$

de sorte que;

$$D_0T = D_a.$$

Plus généralement si i a pour image j, l'image de $\{i\}$ sera évidenment $\{j\}$; car si

$$iT = j = i + h,$$

d'après le N° 21

$$(kp + i)T = kp + iT = kp + i + h, \quad D_iT = D_{i+h} = D_i.$$

Tout automorphisme T de Q induit donc sur l'ensemble des diviseurs D_0; $D_1, D_2, \ldots, D_{p-1}$ une transformation t des indices $0,1,2,3,\ldots,p-1$. L'automorphe de Q induit sur l'ensemble $0,1,2,\ldots,p-1$ un groupe de substitutions.

25. *Dans les conditions du N° 24, si g est l'ordre du système minimal de générateurs de Q, l'ordre de l'automorphe de Q est un diviseur de $m^g p!/(p-g)!$.*

https://doi.org/10.4153/CJM-1957-039-3 Published online by Cambridge University Press

Si l'on choisit un élément quelconque dans chaque diviseur: $a_0 \in D_0$, $a_1 \in D_1, \ldots, a_i \in D_i, \ldots$ d'après le N° 24, tout automorphisme T de Q sera entièrement défini si l'on connaît les images:

$$a'_0 = a_0 T, \ldots, a'_i = a_i T, \ldots .$$

Mais ces images ne sont pas indépendantes enaénéral.

Soit $a_i, a_j, \ldots, a_k$ un système minimal de générateurs indépendants de Q (c'est-à-dire comprenant le plus petit nombre possible de générateurs tels que, par la suppression d'un de ces générateurs, les éléments restants engendrent seulement une partie propre de Q). Alors si les images des générateurs sont connues, il est clair que l'image d'un élément quelconque de Q sera définie. Le nombre des éléments de Q dont on peut se donner arbitrairement l'image est donc égal au nombre minimum des générateurs; soit g ce nombre.

On observera encore que ces g générateurs appartiennent nécessairement à g diviseurs distincts parmi les diviseurs $D_0, D_1, \ldots, D_{p-1}$ Car si deux d'entre eux appartenaient au même diviseur, D, on aurait évidemment un système de générateurs plus court en supprimant l'un d'eux.

Il y a
$$m^g \binom{p}{g} g! = m^g \, p!/(p-g)! = q$$
manières de choisir les images des g générateurs. Les substitutions ainsi obtenues forment un groupe d'ordre q, dont l'automorphe de Q est un diviseur, toutes ces substitutions n'étant pas nécessairement des automorphismes de Q.

Si $p = 1$, alors $g = 1$, $m = n = q$ et l'automorphe de Q est d'ordre n; conformément à la conclusion du N° 19.

26: *Le diviseur D_0 n'est pas nécessairement normal.*

Exemple.

Le quasigroupe:

$$S: F(x) = (0, 10)\ (1, 3, 11, 14, 8, 9, 7, 13, 12, 4)\ (2, 6)\ (5)$$

automorphe par le groupe cyclique du 15° ordre, a pour diviseurs

$$D_i = i, 5 + i, 10 + i \quad (i = 0, 1, 2, 3, 4).$$

Mais aucun de ces diviseurs n'est normal.

27: *Si Q est un quasigroupe d'ordre $n = mp$, automorphe par le groupe cyclique C_n, si $D_0, D_1, \ldots, D_{p-1}$ sont les p diviseurs d'ordre m engendrés par les divers éléments de Q, pour que D_0 (et par conséquent tout D_i) soit normal dans Q il faut et il suffit que Q soit défini par une fonction $F(i + py) = f(i) + p\,\rho_i y$ où $j = f(i)$ est un quasigroupe idempotent d'ordre p, automorphe par le groupe*

cyclique C_p et où $\rho_i(y)$, $(y = 0,1,2 \ldots, m-1)$ définit pour chaque valeur de i $(i = 0, 1, \ldots, p-1)$ un quasigroupe d'ordre m, automorphe par le groupe cyclique C_m.

On a alors $D_i \times D_0 = D_j$ et le quasigroupe quotient Q/D est isomorphe à $f(i)$ par $D_i \to i$.

Preuve. Si D est normal, tout D_i est normal et il est évident que, pour toute valeur de i, les produits de tous les éléments de D_i par 0 doivent appartenir à un seul diviseur, par exemple D_j. Réciproquement, si cela a lieu, il est facile de montrer que tous les D_i sont normaux. En effet, par définition (23), on a:

$$D_i = D_0\begin{pmatrix} x \\ x+i \end{pmatrix}.$$

Supposons: $D_i \times 0 = D_j$, alors, à cause de l'automorphisme

$$D_{i+kp} \times kp = D_{j+kp}.$$

Mais $D_{i+kp} = D_i$, puisque

$$D_{i+kp} = D_i\begin{pmatrix} x \\ x+kp \end{pmatrix}$$

et que $D_i = i, i+p, \ldots,$ donc

$$D_i \times kp = D_j,$$

quelque soit k, ce qui signifie

$$D_i \times D_0 = D_j,$$

et par suite

$$D_{i+h} \times D_h = D_{j+h}.$$

Donc D_0 sera bien normal si, pour toute valeur de i $(i = 0, 1,2, \ldots, p-1)$ on a

$$D_i \times 0 = D_j.$$

Cette relation établit une correspondance biunivoque entre chaque élément de D_i: $i + kp \in D_i$ et un élément: $j + z_k p$ de D_j. Reste à exprimer que cette transformation satisfait pour tout $x \in Q$, à la condition:

$$x - x \times 0 = y - y \times 0 \rightleftarrows x = y \pmod{n}$$

(On observera que D est toujours normal si $m = n/p = 3$.)

En s'occupant d'abord des $x \in D_i$, on aura:

$$\begin{array}{llllll} x = i, & i+p, & i+2p, \ldots, & i+kp, \ldots, & i+mp-p. \\ F = j+z_0p, & j+z_1p, & j+z_2p, \ldots, & j+z_kp, \ldots, & j+z_{m-1}p. \end{array}$$

$$x - F = i - j - z_0p, i - j - (z_1 - 1)p, i - j - (z_2 - 2)p, \ldots,$$
$$i - j - (z_k - k)p, \ldots, i - j - (z_{m-1} - m + 1)p.$$

Pour que ces différences soient toutes distinctes deux à deux, il faut que, en posant:

$$y = 0, 1, 2, 3, \ldots, k, \ldots, m - 1.$$

et

$$\rho_i(y) = z_0, z_1, z_2, z_3 \ldots, z_k \ldots, z_{m-1},$$

la fonction $\rho_i(y)$ satisfasse à la condition:

$$y - \rho_i(y) = y' - \rho_i(y') \rightleftarrows y = y' \qquad \text{(mod. } m\text{)}$$

Cela exprime que ρ définit un quasigroupe d'ordre m, automorphe par le groupe cyclique C_m et d'ailleurs quelconque.

Si toutes les différences $i - j + (k - z_k)p$ sont distinctes elles seront, à l'ordre près, égales à:

$$(6) \qquad i - j, i - j + p, i - j + 2p, \ldots, i - j + (m - 1)p.$$

En considérant maintenant toutes les valeurs de x, il faut exprimer que la suite (6) n'a aucun terme commun avec chacune des suites analogues:

$$(7) \qquad i' - j', i' - j' + p, i' - j' + 2p, \ldots, i' - j' + (m - 1)p,$$

où $i, j, i', j' < p$.

Or il est facile de voir que, pour que (6) et (7) n'aient aucun terme commun il faut et il suffit que:

$$i - j \neq i' - j',$$

car: [1], si $i - j = i' - j'$, alors les suites (6) et (7) ont tous leurs termes deux à deux égaux et par conséquent ne sont pas distinctes; [2], si (6) et (7) ont un terme commun, par exemple:

$$i - j + kp \equiv i' - j' + k'p \qquad \text{(mod. } n\text{)},$$

on en déduira

$$(i - j) - (i' - j') \equiv (k' - k)p \qquad \text{(mod. } mp\text{)}$$

ce qui exige

$$i - j \equiv i' - j' \qquad \text{(mod. } p\text{)}$$

et comme i et j sont plus petits que p,

$$i - j = i' - j'.$$

Finalement il faut que la transformation $i \rightarrow j$ satisfasse à

$$i - j \neq i' - j', \qquad i \neq i',$$

ou, en posant $j = f(i)$,

$$i - f(i) \neq i' - f(i'), \qquad i \neq i'.$$

Donc la fonction $f(i)$ définit encore un quasigroupe, d'ordre p, automorphe par le groupe cyclique C_p. D'ailleurs ce quasigroupe est idempotent car $D_i \times D_i = D_i$.

La réciproque résulte du N° 15 et la dernière partie du N° 16.

28. *Dans les conditions du N° 27, si P est l'ordre de l'automorphe de $f(i)$, le nombre des automorphismes de Q est un diviseur de Pm^g où g désigne comme au N° 25 le nombre minimum de générateurs indépendants de Q.*

Tout automorphisme de Q est défini par un ensemble de p substitutions

$$s_i : x \to x + kp + j - i \qquad (k = 0, 1, 2, \ldots, m - 1)$$

où $i \to j$ est un automorphisme de $f(i)$ et où la substitution s_i opère sur un seul diviseur D_i.

D'autre part, d'après le N° 24, tout automorphisme T de Q projette un D_i sur un D_j, c'est-à-dire permute les D_i entre eux. D étant normal, T induit sur le quasigroupe quotient $f(i)$ d'ordre p un automorphisme t. Et, si $iT = j$, l'automorphisme T induit un isomorphisme de D_i sur D_j.

Le nombre des automorphismes t est au plus égal à celui des automorphismes du quasigroupe $f(i)$, soit P.

Comme tous les D sont monogènes, chacun a pour automorphe le seul groupe cyclique d'ordre m.

$$x \to x + kp \qquad (k = 0, 1, \ldots, m - 1).$$

Si R est un isomorphisme de D_i avec D_j,

$$D_i R = D_j,$$

comme on a:

$$D_i \begin{pmatrix} x \\ x + kp \end{pmatrix} = D_i$$

et par conséquent

$$D_i \begin{pmatrix} x \\ x + kp \end{pmatrix} R = D_j,$$

tous les autres automorphismes seront compris dans la formule:

$$\begin{pmatrix} x \\ x + kp \end{pmatrix} R.$$

Or D_j est isomorphe de D_i par $x + i \to x + j$, c'est-à-dire:

$$\begin{pmatrix} x \\ x + j - i \end{pmatrix}.$$

Donc tous les isomorphismes de D_i avec D_j sont exprimés par les transformations:

$$S = \begin{pmatrix} x \\ x + kp \end{pmatrix}\begin{pmatrix} x \\ x + j - i \end{pmatrix} = \begin{pmatrix} x \\ x + kp + j - i \end{pmatrix}$$

i, j fixes; $k = 0, 1, \ldots, m - 1$.

Pour chaque D_i il existe donc m substitutions, correspondant aux m valeurs de k et projetant D_i sur D_j.

L'automorphisme T de Q induit un isomorphisme de D_i avec D_j compris dans les m substitutions S ci-dessus. Cela peut être répété pour les p diviseurs D_i, mais si Q a g générateurs, le choix de k n'est libre que pour ces g générateurs et finalement le nombre total des automorphismes de Q est un diviseur de Pm^g, ordre du groupe défini par les t et par les S.

Exemple I.

$$F = (0, 3)\ (1, 5)\ (2, 4)\ (6)\ (7, 8)$$
$$p = m = 3;\ D_0 = 0, 3, 6;\ D_1 = 1, 4, 7;\ D_2 = 2, 5, 8$$
$$S_0 = \begin{pmatrix} x \\ x \end{pmatrix};\qquad S_1 = \begin{pmatrix} x \\ x + 3 \end{pmatrix};\qquad S_2 = \begin{pmatrix} x \\ x + 6 \end{pmatrix}$$
$$T = (0)\ (3)\ (6) \cdot (147) \cdot (285)$$

Exemple II.

$$f = (0)\ (1243);\ \rho_0 = \rho_2 = \rho_3 = (02)\ (1);\ \rho_1 = (01)\ (2)$$
$$F = (0, 10)\ (1, 7, 9, 13)\ (2, 14, 8, 6)\ (3, 11, 12, 4)\ (5) = f + 5\ \rho_i(y).$$

Ce quasigroupe est engendré par (0, 1). Tout automorphisme est défini par les images de 0 et de 1. L'automorphe de Q est donc d'ordre $9.\ 5!/3! = 180$ ou un diviseur de 180.

En écrivant i pour D_i, le quasigroupe quotient devient $f(i)$ lui-même. Son automorphe est du $20^{\text{ème}}$ ordre; il contient C_5 et le sousgroupe du $4^{\text{ème}}$ ordre $\{(1243)\}$.

Citations

1. A. A. Albert, *Non associative Algebras*, Ann. Math. (2), *43* (1942), 696.
2. B. A. Haussmann, O. Ore, *Theory of Quasigroups*. Amer. J. Math., *59* (1937), 983.
3. C. Jordan, *Traité des substitutions* (Paris, 1870).
4. F. Kiokemeister, *A theory of normality for quasi-groups*, Amer. J. Math., *70* (1948), 100–102.
5. D. Rees, *On semi-groups*, Proceed. Camb. Phil. Soc., *36* (1940), 387.
6. A. Sade, *Quasigroupes* (Marseille, 1950).
7. ———, *Contribution à la théorie des quasigroupes*, CR Acad. Sci. Paris, *237* (1953), 420–422.
8. G. Scorza, *Gruppi Astratti* (Roma, 1942).

Lycée Perier, Marseille