JOUONS UN PEU AVEC CERTAINS GROUPES

Nous avons vu dans le texte précédent « Groupes et propriétés » qu'à la loi de composition interne (que nous avons symbolisée ainsi : &) correspond une loi de composition inverse (que nous avons symbolisée ainsi : §) telle que :

$$a\S b = c \Leftrightarrow c\&b = a$$

Demandons-nous alors si cette loi inverse peut être commutative et si oui quels genres de groupes en sont pourvus.

Tout d'abord, si cette loi inverse est commutative, cela signifie que : a§b = b§a = c. Or, a§b = a&b' et b§a = b&a' $\Rightarrow$ a&b' = b&a' = c. Mais b&a' = (a&b')' = c'. Donc c' = c. Il faut donc que c soit son propre symétrique et, comme c peut être n'importe quel élément du groupe, il faut donc que chaque élément soit son propre symétrique. Réciproquement, si c' = c, b&a' = a&b'= b§a = a§b, la loi inverse est commutative. Que chaque élément soit son propre symétrique est donc une condition nécessaire et suffisante pour que la loi inverse soit commutative.

Un tel groupe peut-il exister ? Oui, et nous en donnerons trois exemples. Mais remarquons d'abord que dans un tel groupe la loi inverse § donne les mêmes résultats que la loi directe &, car x§y = x&y' = x&y puisque y' = y. Donc cette loi est la même que la loi & ; c'est donc aussi une loi de groupe et comme elle est commutative, ceci implique évidemment que la loi & le soit aussi, donc que l'on ait à faire à un groupe commutatif, comme vont le montrer les trois exemples que voici :

1er exemple :

&	e	a
e	e	a
a	a	e

Il s'agit du plus petit groupe possible, à deux éléments.

Question 1 : Peut-on en trouver un de trois éléments (e, a, b) ?

&	e	a	b
e	e	a	b
a	a	e	
b	b		e

Dans cette grille il ne reste plus que deux cases à remplir et nous pouvons déjà remarquer que le petit groupe précédent à deux éléments est nécessairement inclus dans l'ensemble recherché, c'est-à-dire que s'il existait effectivement un tel groupe de trois éléments, le petit groupe de deux lui serait un sous-groupe. Or un théorème de Lagrange affirme que : *Le cardinal d'un sous-groupe d'un groupe fini est un diviseur du cardinal de ce groupe*. Mais 2 n'est pas un diviseur de 3. Donc un tel groupe de trois éléments n'existe pas.

Question 2 : Peut-on alors trouver un tel groupe de 4 éléments (e, a, b, c) ? La réponse est oui et voici sa table d'opération (dite aussi *table de Cayley*) :

2ème exemple :

	&	e	a	b	c
1	e	e	a	b	c
2	a	a	e	c	b
3	b	b	c	e	a
4	c	c	b	a	e

On y remarque que le petit groupe de deux éléments est un sous-groupe de celui-ci (il ne pourrait pas en être autrement). Et ceci fait que la construction de cette table montre qu'elle est unique. En effet, dès la deuxième ligne de résultats, nous n'avons pas de choix pour les deux cases hors du sous-groupe : il faut placer c et b dans cet ordre (sinon b et c seraient deux fois dans une même colonne), ce qui, par la commutativité de &, remplit également la deuxième colonne de résultats. Les deux dernières cases alors libres ne peuvent contenir que « a ». **Ce groupe est donc unique en son genre**. Et ici le théorème de Lagrange n'est pas bafoué puisque 2 est bien un diviseur de 4.

L'observation de cette table d'opération montre parfaitement que chaque élément est son propre symétrique, que la loi de composition interne est commutative (symétrie par rapport à la diagonale principale) et, d'autre part, qu'il n'y a pas deux fois le même élément dans une ligne ou une colonne, donc que tous les éléments sont réguliers. Mais, pour être sûr qu'il s'agisse vraiment d'une loi de groupe, il faut aussi vérifier qu'elle est associative. Ceci n'apparaît pas visuellement dans la grille, mais les seuls triplets à vérifier sont ceux contenant a, b et c (car la présence de « e » rend l'associativité évidente). Or, plutôt que de vérifier cela avec les triplets d'éléments, posons-nous la question suivante : Peut-on attribuer une représentation concrète, notamment géométrique, à nos deux premiers exemples ?

- En ce qui concerne le premier, une représentation satisfaisante est, pour « a », la rotation d'angle π autour d'un axe donné. Elle est involutive donc a&a = e (e = rotation d'angle nul).

- En ce qui concerne le deuxième exemple (4 éléments), une représentation satisfaisante est les rotations, là encore d'angle π (ou nul pour « e ») mais chacune autour de l'un de 3 axes deux à deux orthogonaux dans l'espace vectoriel euclidien à 3 dimensions. En effet : on peut considérer ces 3 axes comme ceux d'un repère cartésien orthonormé dont nous désignerons les vecteurs de base par **i**, **j**, **k**.

La rotation R_i d'angle π autour de l'axe support de **i** a pour matrice associée, selon la base (**i**, **j**, **k**) :

$$MR_i = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

La rotation R_j d'angle π autour de l'axe support de **j** a pour matrice associée :

$$MR_j = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Et enfin la rotation R_k d'angle π autour de l'axe support de **k** a pour matrice associée :

$$MR_k = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Chacune de ces matrices est diagonale, et orthogonale (isométries vectorielles). Sa transposée, qui est donc son inverse, est elle-même. Ces trois rotations sont donc involutives, chacune est sa propre symétrique (comme cela était d'ailleurs évident sans considérer les matrices).

Observons maintenant les produits de ces rotations :

$$MR_j\, MR_i = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = MR_k$$

$$MR_k MR_i = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = MR_j$$

$$MR_k\,MR_j = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = MR_i$$

Ces produits sont commutatifs car le produit de matrices diagonales de même ordre l'est toujours. L'ensemble de ces trois rotations et de la rotation nulle forme un groupe multiplicatif car chaque rotation a une symétrique (elle-même), il existe un élément neutre (rotation nulle) et le produit est associatif car les rotations sont des transformations et les produits de transformations sont toujours associatifs. Cet ensemble est donc bien un groupe, qui plus est commutatif, et sa table d'opération est :

&	e	R_i	R_j	R_k
e	e	R_i	R_j	R_k
R_i	R_i	e	R_k	R_j
R_j	R_j	R_k	e	R_i
R_k	R_k	R_j	R_i	e

On retrouve ici la table d'opération du deuxième exemple où $R_i = a$; $R_j = b$ et $R_k = c$ et on peut constater qu'elle reste inchangée si l'on affecte à ces rotations les lettres a, b, c dans un autre ordre, ce qui confirme l'unicité de la table précédente avec ces lettres.

Question 3 : Peut-on trouver de tels groupes de 5, 6 ou 7 éléments ?

La réponse est évidemment non en ce qui concerne les groupes de 5 et 7 éléments car, le petit groupe de 2 (e et a) étant incontournable, doit en être un sous-groupe, or 5 et 7 ne sont pas des multiples de 2.

En ce qui concerne un groupe éventuel de 6 éléments (ayant les propriétés imposées), là encore c'est impossible car un théorème affirme que *tout groupe fini commutatif de cardinal non premier admet au moins un sous-groupe ayant pour cardinal un diviseur arbitraire de son cardinal*. Or, le groupe de 6 éléments devant être commutatif, devrait admettre un sous-groupe de 3 éléments et nous venons d'établir qu'un tel groupe est impossible selon les propriétés imposées.

Question 4 : Peut-on alors trouver un tel groupe de 8 éléments, ce qui ne contredirait pas le théorème de Lagrange puisque 4 est diviseur de 8 ?

La réponse est oui. Et, comme pour le groupe précédent à 4 éléments, cherchons quelles transformations géométriques peuvent correspondre à ces éléments. En ce qui concerne les quatre premiers (e, a, b, c), nous pouvons reprendre les rotations précédentes (rotation nulle, et rotations R_i, R_j et R_k). Pour les quatre suivants (que je désignerai par d, f, g, h), après plusieurs tâtonnements, j'ai adopté ceci : Considérons le repère cartésien orthonormé (O, **i**, **j**, **k**), les symétries par rapport aux trois plans du trièdre et la symétrie par rapport à O :

S_1 = Sym (i, j) dont la matrice associée est : $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

S_2 = Sym (i, k) dont la matrice associée est : $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

S_3 = Sym (j, k) dont la matrice associée est : $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

S_4 = Sym (O) dont la matrice associée est : $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

L'ensemble des rotations et de ces symétries se révèle stable pour le produit.
Quelques exemples : $MR_iMS_1 = (1, -1, -1)(1, 1 –1) = (1, -1, 1) = MS_2$

$MR_iMS_2 = (1, -1, -1)(1, -1, 1) = (1, 1 –1) = MS_1$

$MR_jMS_4 = (-1, 1 –1)(-1, -1, -1) = (1, -1, 1) = MS_2$

(N'ont été écrites dans ces exemples que les diagonales des matrices concernées puisque elles seules interviennent). Tous les autres produits confirment cette stabilité et sont évidemment commutatifs puisque concernant des matrices diagonales.

Si maintenant on désigne les rotations par les lettres e, a, b, c comme dans l'exemple à 4 éléments et S_1, S_2, S_3, et S_4 respectivement par les lettres d, f, g, h, on obtient la table d'opération suivante qui est notre :

3ème exemple :

&	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	e	a	g	h	d	f
c	c	b	a	e	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

Cette table montre bien que :

- Chaque élément est son propre symétrique (e sur toute la diagonale principale).
- La loi & (et donc aussi §) est commutative (symétrie par rapport à la diagonale principale)
- Chaque élément est régulier car chaque colonne et chaque ligne de résultats ne présente jamais deux fois le même élément.
- D'autre part, l'associativité est assurée par le fait que les éléments de cet exemple sont des transformations. **Cet ensemble, muni de sa loi de composition « & » est donc un groupe**.

Mais il s'avère qu'il n'est pas le seul groupe possible des huit éléments précités et avec toutes les propriétés énoncées. On peut aussi former un groupe de ce genre en désignant par exemple S_3 par f et S_2 par g. Voici sa table d'opération :

&	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	g	h	d	f
b	b	c	e	a	f	d	h	g
c	c	b	a	e	h	g	f	d
d	d	g	f	h	e	b	a	c
f	f	h	d	g	b	e	c	a
g	g	d	h	f	a	c	e	b
h	h	f	g	d	c	a	b	e

Le groupe précédent que nous avons trouvé n'est donc pas unique en son genre avec les éléments e, a, b, c, d, f, g, h. Et on peut vérifier qu'il y en a d'autres !

Dernière question : Peut-on trouver des groupes finis d'un cardinal encore plus grand et ayant les propriétés imposées ?

S’il en existe, nous pouvons déjà prévoir que leurs cardinaux sont pairs car le petit groupe des 2 éléments « e » et « a » est incontournable et donc nécessairement un de leurs sous-groupes comme nous l’avons vu jusqu’ici.
D’autre part, les cardinaux pairs, n’étant évidemment pas premiers, peuvent être décomposés en produits de facteurs premiers, et il existe au moins un sous-groupe ayant pour cardinal chacun de ces facteurs premiers, en vertu du deuxième théorème cité dans ce texte (*tout groupe fini commutatif de cardinal non premier admet au moins un sous-groupe ayant pour cardinal un diviseur arbitraire de son cardinal*). Or, si l’un de ces facteurs premiers est différent de 2, par exemple 3, 5, 7, 11, etc…, le sous-groupe qui l’aurait pour cardinal répondrait au théorème que voici : *Tout groupe de cardinal premier est cyclique*. Un groupe fini cyclique est dit aussi *monogène*, c’est-à-dire qu’un seul élément particulier permet, par la loi de composition interne, d’engendrer tous les autres (y compris l’élément neutre). Le petit sous-groupe de cardinal 2 ({e, a}, &) que nous avons déjà signalé comme incontournable est cyclique : son élément générique est « a » (a&a=e et a&e=e&a=a). Mais pour un cardinal supérieur à 2 il est impossible de trouver un élément générique puisque, d’après les conditions initiales, chaque élément doit être son propre symétrique.
On en déduit donc que, si des groupes de cardinaux supérieurs à 8 satisfont aux propriétés imposées, leurs cardinaux sont nécessairement des puissances de 2. D’ailleurs, les trois exemples que nous venons d’étudier ont pour cardinaux $2 = 2^1$; $4 = 2^2$ et $8 = 2^3$. Les nouveaux groupes à envisager doivent alors avoir pour cardinaux $2^4 = 16$; $2^5 = 32$; etc. Existe-t-il des transformations connues qui correspondraient à leurs éléments ?

C’est une affaire à suivre et peut-être qu’un lecteur intéressé et créatif saura la faire progresser et m’en faire part ?