GROUPES MONOGENES

Définition :

Certains groupes ont au moins un élément qui, composé plusieurs fois avec lui-même, engendre tous les autres y compris l'élément neutre. On les qualifie de *monogènes* et l'élément qui engendre tous les autres est nommé *générateur*.

Par exemple le petit groupe de 3 éléments {e, x, y} dont la table d'opération est :

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

a pour générateurs x et y. (On remarquera que x et y sont deux symétriques. Cela sera justifié par la suite.)

* Soit (G, .) un groupe monogène d'élément neutre « e » et tel que x lui soit un générateur. Démontrons que nx = y $\Rightarrow$ nx' = y' (x' et y' étant les symétriques respectifs de x et y, et n $\in$ N*)

$$nx.nx' = (x.x.....x.x).(x'.x'.....x'.x') = x.x\ .....x.x.\underbrace{x'.x'}_{e}.....x'.x' = e$$

$$\underbrace{\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad}_{e}$$

Cette composition se « vide » par son milieu puisque la loi de groupe est associative. Donc, si nx engendre tous les éléments du groupe, nx' engendre tous leurs symétriques, c'est-à-dire aussi tous les éléments du groupe puisque chaque élément est le symétrique de son symétrique. Par conséquent x' est aussi un générateur de (G, .). Le seul groupe monogène dont le symétrique du générateur est le générateur lui-même n'a que deux éléments. Au dessus de deux éléments il est impossible qu'un générateur soit égal à son symétrique car il n'engendrerait que l'élément neutre et lui-même. D'où :

Théorème : **Tout groupe monogène de plus de deux éléments a au moins deux générateurs distincts, symétriques l'un de l'autre**.

* Considérons un groupe monogène (G,.) dont un générateur est désigné par x. a = nx est élément de G, ainsi que b = n'x (n et n' $\in$ N*) ; donc a.b = nx.n'x $\in$ G car un groupe est stable pour sa loi de composition interne. Et cette loi est associative, aussi :

$$nx.n'x = \underbrace{(x.x...x)}_{n}.\underbrace{(x.x.....x)}_{n'} = \underbrace{(x.x.....x)}_{n'}.\underbrace{(x.x...x)}_{n} = n'x.nx$$

$$= b.a$$

c'est-à-dire : ab = ba. Donc cette loi de groupe est aussi commutative. Par conséquent :

Théorème : **Tout groupe monogène est commutatif**.

* L'ordre n d'un générateur x d'un groupe fini monogène de cardinal p doit être égal au cardinal de ce groupe sinon le composé nx, avec $n < p$ ($n \in N^*$) serait l'élément neutre e , puis $(n + 1)x = nxx = ex = x$, etc … et ainsi ne seraient engendrés par x, et par cycles successifs, que les éléments allant de x à nx et non tous les éléments du groupe. Donc l'ordre de $x = p$. Et alors $px = e$, puis $(p + 1)x = pxx = ex = x$ et ainsi de suite, engendrant à nouveau tous les éléments du groupe, par cycles successifs. On dit alors que ce groupe est *cyclique*.
D'où :

Théorème : **Tout groupe monogène fini est cyclique. L'ordre de ses générateurs est égal au cardinal de ce groupe.**

* La définition des groupes monogènes donnée en tête de ce texte exclut les groupes infinis. En effet, puisque le générateur doit aussi engendrer l'élément neutre, il ne peut, par ses compositions suivantes, qu'engendrer à nouveau les éléments qu'il avait déjà engendrés avant l'élément neutre et le groupe est donc fini et cyclique.

L'ensemble Z des entiers relatifs, muni de l'addition, est un groupe dont l'élément neutre est 0. Ce groupe (Z, +) est infini et la paire d'éléments {-1 ; 1} permet d'engendrer tous les autres éléments y compris le 0 (-1 + 1 = 0), le 1 engendrant par ses sommes tous les nombres positifs et le -1 tous les négatifs. Mais le 1 seul et le -1 seul ne permettent pas d'engendrer tous les éléments de (Z, +). Dans ce groupe il n'y a pas un générateur, mais la paire {-1 ; 1} génératrice.
Ce groupe (Z, +) a, à part cela, toutes les qualités des groupes monogènes finis, sauf le caractère cyclique. Il est commutatif et les éléments -1 et 1 qui constituent la paire génératrice sont symétriques. Aussi est-il considéré par extension comme un groupe monogène infini et il se démontre même que tout autre groupe monogène infini est isomorphe à (Z, +).

*

* *