GROUPES ET PROPRIETES

(*La notion de groupe est la première structure algébrique qui a été pressentie (notamment par les jeunes prodiges Abel et Galois) puis définie, et la première étudiée aujourd'hui par les étudiants en math. Cependant il arrive souvent qu'on néglige les bénéfices qu'on peut tirer de ses propriétés*.)

Soit un ensemble G d'éléments, ensemble fini ou non, muni d'une loi de composition interne que nous noterons « & ».
(*Rappel : Une loi de composition interne dans G est une application de GxG dans G, donc tout couple d'éléments de G a une image unique ; cette loi est donc partout définie dans G et univoque).*
Remarquons à ce sujet que dans un groupe de cardinal n les couples d'éléments sont au nombre de n^2. On en déduit donc qu'il existe des éléments qui sont individuellement les composés de plusieurs couples différents.

Définition :

G, muni de &, qu'on note (G, &), est un *groupe* si et seulement si ces trois axiomes sont vérifiés quels que soient les éléments mis en jeu :

* & est associative $\Leftrightarrow$ (a&b)&c = a&(b&c)
* & admet un élément neutre (e) tel que a&e = e&a = a
* Chaque élément « a » admet un symétrique a' tel que a&a' = a'&a = e

Montrons tout d'abord que ces axiomes constitutifs peuvent être ramenés à ces axiomes plus courts :

* & est associative
* & admet un élément neutre (e) à droite $\Leftrightarrow$ a&e = a
* Chaque élément de G admet un symétrique à droite $\Leftrightarrow$ a&a' = e

Propriété I : **Tout élément de (G, &) est régulier à droite**.
En effet : si b&a = c&a $\Rightarrow$ (b&a)&a' = (c&a)&a' = b&(a&a') = c&(a&a') = b&e = c&e = **b = c**.

Propriété II : **e est aussi élément neutre à gauche**.
En effet : Soit e&a = c $\Rightarrow$ (e&a)&a' = c&a'. Or (e&a)&a' = e&(a&a') = e&e = e
Donc c&a' = e. Or a&a' = e. Donc, en vertu de la propriété I, c = a $\Rightarrow$ **e&a = a**.

Propriété III : **Tout symétrique à droite est aussi symétrique à gauche**.
En effet : Soit a'&a = d, puisque a&a' = e $\Rightarrow$ a'&(a&a') = a'&e = e&a' (d'après la propriété II). Or a'&(a&a') = (a'&a)&a' = d&a'. Donc : e&a' = d&a' $\Rightarrow$ d = e, d'après la propriété I, $\Rightarrow$ **a'&a = e**.

Propriété IV : **Tout élément de (G, &) est régulier à gauche**.
En effet : Si a&b = a&c $\Rightarrow$ a'&(a&b) = a'&(a&c) = (a'&a)&b = (a'&a)&c = e&b = e&c = **b = c**.

Les propriétés II et III, que nous venons de démontrer, nous permettent d'affirmer que les axiomes définissant la notion de groupe se résument en fait à ces trois-là :

* La loi de composition interne est associative.
* Il existe un élément neutre à droite.
* Tout élément admet un symétrique à droite.

(Il est clair que, par le même type de raisonnements, on peut aussi démontrer que **ce système d'axiomes est également constitutif à gauche**).

Quant aux propriétés I et IV, elles signifient que tout élément du groupe est régulier pour la loi de composition interne, ce que nous résumerons en disant que *cette loi est régulière*.
Ceci a pour conséquence que **l'élément neutre est unique**, même accidentellement : Si l'on en envisageait un autre (e') n'agissant, par exemple, que sur l'élément a, nous aurions a = a&e = a&e' $\Rightarrow$ e = e', puisque la loi est régulière.

Quelques autres conséquences de ces propriétés :

* **Chaque élément d'un groupe possède un unique symétrique** :

En effet : Supposons que a&a' = e = a&b. Par la régularité de la loi de composition interne, **a' = b**.

* Il s'ensuit que **si a' est le symétrique de a, réciproquement a est le symétrique de a'**.

* **Deux éléments distincts ont deux symétriques distincts.**

* **L'élément neutre est son propre symétrique**.

En effet : Si e&x = e. Etant donné que e&x = x, nous en déduisons que x = e.

* Si a&b = c, alors b'&a' = c'. En effet :

(a&b)&(b'&a') = a&(b&b')&a' = (a&e)&a' = a&a' = e.

Donc b'&a' = c'

Le symétrique du composé de 2 éléments est égal au composé des symétriques du 2ème élément et du premier.

* On peut envisager la loi de « composition inverse » de la loi de groupe &, définie de la façon suivante (et symbolisée par §) :

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

$$\text{Si } c\&b = a \Rightarrow (c\&b)\&b' = \underline{a\&b'} = c\&(b\&b') = c\&e = \underline{c}.$$

D'où : c = a&b' c'est-à-dire : **a§b = a&b'**

Il s'ensuit que a§a = a&a' = e.

Par exemple, dans l'ensemble Z des entiers relatifs, qui forme un groupe relativement à l'addition, retrancher un nombre consiste à ajouter son opposé et faire la différence entre deux nombres égaux donne l'élément neutre 0.

Cette loi de « composition inverse » se révèle donc partout définie dans (G, &) et univoque. **Il s'agit donc d'une loi de composition interne dans G**. Et elle est régulière. En effet : a§b = a§d = a&b' = a&d' $\Rightarrow$ b' = d' (car & est régulière) $\Leftrightarrow$ b = d, et a§b = c§b = a&b' = c&b' $\Rightarrow$ a = c. Mais généralement cette loi de composition inverse n'est pas associative, donc pas une loi de groupe, ce qui fait qu'il n'y a pas une vraie symétrie entre ces deux lois de composition interne. D'ailleurs : $\underline{(a\S b)'}$ = (a&b')' = b&a' = $\underline{b\S a}$. **Le symétrique du composé inverse de 2 éléments est égal au composé inverse du deuxième élément et du premier**, ce qui diffère du symétrique du composé direct tel qu'énoncé dans la règle précédente.

Les propriétés I, II, III, IV et leurs conséquences, étant établies, s'appliquent à toutes sortes d'ensembles formant des groupes relativement à une loi de composition interne et permettent alors d'éviter des démonstrations particulières. Ainsi, par exemple :

Considérons l'ensemble F des matrices carrées inversibles d'un ordre n fini et donné, muni du produit matriciel :

- Ce produit, comme on le sait, est associatif.

- Il existe une matrice unité (dite aussi matrice identité, matrice diagonale dont tous les éléments de sa diagonale principale sont 1). Le produit de cette matrice unité et d'une matrice de F redonne cette dernière. Donc la matrice unité est l'élément neutre à gauche du produit.

- Toute matrice de F, étant inversible, a une matrice inverse et le produit de l'inverse d'une matrice de F et de cette matrice donne la matrice unité.

Donc F, muni du produit matriciel, est un groupe (Ici les trois axiomes sont constitutifs à gauche).

Ceci étant établi, on peut alors affirmer, sans faire de démonstrations sur les matrices elles-mêmes, que :

* La matrice unité est unique (pour chaque ordre n donné).
* Chaque matrice de F n'a qu'une unique inverse, commutable avec elle.
* Si M' est l'inverse de M, réciproquement M est l'inverse de M'.
* Deux matrices de F distinctes ont deux inverses distinctes.

* L'inverse du produit de matrices M_1M_2 est égale à $M_2'M_1'$ (ce qui dispense de la démonstration du théorème X du texte « Théorèmes sur les matrices … »).

* On peut aussi envisager un quotient de matrices (opération inverse du produit) défini ainsi : $M_1/M_2 = M_3 \Leftrightarrow M_3.M_2 = M_1$, ce qui entraîne $M_1/M_2 = M_1.M_2'$.

Propriétés V et VI : Soient deux éléments quelconques a et c de (G, &), il est toujours possible de trouver x appartenant à G tel que x&c = a.
En effet : x&c = a $\Leftrightarrow$ a§c = x. Or, nous venons de voir que cette « loi de composition inverse (§) » est une loi de composition interne dans G. **On en déduit que tout élément « a » de G peut être considéré comme le composé, selon la loi &, de deux éléments de G autres que « a »**, (ce qu'on pourrait résumer en disant qu'aucun élément d'un groupe n'est « premier » selon la loi de composition interne de ce groupe), et que **toute équation du type x&c = a admet une solution unique dans (G, &), cette solution étant x = a&c'**.
Remarquons aussi que x&c = a $\Leftrightarrow$ c'&x' = a'. Or, dans un groupe, tout élément admet un symétrique, et est lui-même le symétrique de son symétrique. Ainsi c' et a' peuvent être deux éléments quelconques du groupe G, ce qui entraîne que **toute équation du type c&x = a admet une solution unique dans (G, &)**, cette solution n'étant pas nécessairement la même que la précédente, à moins que (G, &) soit commutatif.

Détaillons : x_1&c = a $\Leftrightarrow \underline{x_1}$ = a§c = $\underline{a\&c'}$

c&x_2= a $\Leftrightarrow$ x'_2&c' = a' $\Leftrightarrow$ x'_2 = a'§c' = a'&c $\Leftrightarrow \underline{x_2 = c'\&a}$

Pour que $x_2 = x_1$ il est nécessaire et suffisant que la loi de groupe & soit commutative.

*

* *