DEUX STRUCTURES PARTICULIERES DANS UN GROUPE

Soit (G, .) un groupe et e son élément neutre. Nous désignerons par G* l'ensemble G – {e}.

Supposons qu'il existe une partie stable de (G*, .) et que nous désignerons par A (des exemples seront donnés plus loin montrant que ceci se rencontre).

Nous pouvons déjà affirmer qu'aucun élément de A n'est le symétrique d'un élément de A. En effet, supposons que a et b soient deux éléments symétriques l'un de l'autre et appartenant à A, alors a.b = e. Or $e \notin G^* \Rightarrow e \notin A$, ce qui contredirait l'hypothèse A est stable.

Proposition I :

Désignons par A' l'ensemble de tous les symétriques des éléments de A. **A' est une partie stable de (G*, .) et $A \cap A' = \emptyset$.**

Démonstration : Nous avons déjà démontré dans le texte « Groupes et propriétés » que si a.b = c alors c' = b'.a', c'est-à-dire : (a.b)' = b'.a'. Donc, quel que soit $\{x', y'\} \subset A'$, x'.y' = (y.x)'. Or $y.x \in A$ et son symétrique $(y.x)' \in A' \Rightarrow x'.y' \in A'$. Donc A' est stable. D'autre part $e \notin A'$ car, e étant son propre symétrique, s'il appartenait à A' il devrait aussi appartenir à A, or A est une partie de G*. Enfin, s'il existait un élément x commun à A et A', alors $x \in A'$ et serait donc le symétrique d'un élément « y » de A. Mais x appartiendrait aussi à A et on vient de démontrer qu'aucun élément de A n'est le symétrique d'un élément de A. Donc $A \cap A' = \emptyset$.

Proposition II :

Si A existe, elle ne peut être qu'infinie (donc A' et (G, .) aussi).

Démonstration : Soit « a » un élément de A. Il est possible de former a.a que nous désignerons par 2a. De même a.a.a = 3a, etc … d'où l'élément général x_n = na (n étant un naturel non nul). x_n appartient à A puisque A est une partie stable de G*, et $x_n \neq e$, puisque e n'appartient pas à G*. On peut alors engendrer ainsi une infinité d'éléments de A distincts deux à deux. En effet, considérons x_i et x_j tels que j > i . Ceci entraîne que $x_j = x_i.x_{j-i}$. Supposons alors que $x_j = x_i \Rightarrow x_{j-i} =$ e, ce qui serait contraire à l'hypothèse A ne contient pas e. **Donc la partie A est bien infinie,** et l'élément « a » est le générateur d'une infinité d'éléments de A.

A' étant l'ensemble des symétriques des éléments de A et deux éléments distincts d'un groupe ayant deux symétriques distincts, la relation de A vers A', qui fait correspondre à chaque élément de A son symétrique dans A', est une application injective. **Donc A' est infinie**. (Cette relation est aussi surjective car

les éléments de A' étant les symétriques de ceux de A, tous sont donc images dans cette relation. Par conséquent il y a bijection de A dans A').

Et nous pouvons affirmer *a contrario* que :

Théorème : **Dans tout groupe G fini il est impossible de trouver une partie stable de G***.
Corollaire : **S'il existe une partie stable dans un groupe fini, elle contient nécessairement l'élément neutre.**

Deux remarques :

* Même si le groupe (G, .) n'est pas commutatif, naa = ana et na'a' = a'na', $\forall n \in N^*$.

* Démontrons que si (na)' = na' $\Leftrightarrow$ na.na' = e, alors [(n+1) a]' = (n+1) a'. (n+1) a = naa et (n+1) a' = na'a' = a'na' $\Rightarrow$ naa.a'na' = na(aa')na' = naena' = na.na' = e par hypothèse. Or, pour n = 1, a' = a', évidence. Donc ceci est aussi vrai pour n = 2, 3 …etc, par récurrence et en général **(na)' = na'**.

Exemples simples d'un groupe infini possédant A et A' :

Posons G = (Z, +), c'est-à-dire l'ensemble des entiers relatifs muni de l'addition. A peut être considérée comme Z*+ et A' comme Z*-, c'est-à-dire que A est l'ensemble des entiers strictement positifs et A' l'ensemble des entiers strictement négatifs.
Ou encore A peut être une partie de Z*+ comme $\{x \mid x \geq 3\}$, par exemple, et il s'ensuit que A' = $\{x \mid x \leq -3\}$. Mais dans ce choix tous les éléments de G* ne sont pas utilisés.

Relations d'ordre dans G* :

Maintenant, et afin de pouvoir utiliser la loi de composition inverse définie dans le texte « Groupes et propriétés », revenons aux symboles « & » pour la loi de groupe, « § » pour la loi inverse, et à leurs propriétés.

La loi de composition inverse permet de créer une relation d'ordre dans G*. En effet : posons a > b $\Leftrightarrow$ a§b $\in$ A et, *a contrario*, a < b $\Leftrightarrow$ a§b $\in$ A'.

* Cette relation n'est pas réflexive. En effet : a§a = a&a' = e $\notin$ G*. a n'est pas comparable à lui-même.

* Cette relation est antisymétrique. En effet : **a > b** $\Leftrightarrow$ a§b $\in$ A $\Leftrightarrow$ (a§b)' = b§a $\in$ A' $\Leftrightarrow$ **b < a**.

* Cette relation est transitive. En effet : posons **a > b** et **b > d**.

a > b $\Leftrightarrow$ a§b = a&b' $\in$ A ; b > d $\Leftrightarrow$ b§d = b&d' $\in$ A

(a&b')&(b&d') = a&(b&b')&d' = a&e&d' = a&d' = a§d. A étant stable pour la loi &, a§d ∈ A et donc **a > d**.

Cette relation est donc une relation d'ordre (strict) dans G*, et aussi dans A, et que nous énoncerons : « a est supérieur à b » De même on démontre aisément **que la relation a < b est aussi d'ordre strict dans G* et dans A** et que nous énoncerons : « a est inférieur à b » et, selon l'antisymétrie que nous venons de démontrer, nous pouvons énoncer aussi que si « a » est supérieur à b, inversement b est inférieur à « a ».

D'autre part, ∀ {x , y} ⊂ A, x&y ∈ A, car A est stable, ⇒ (x&y)' ∈ A'. Or, (x&y)' = y'&x' = y'§x. Donc y'§x ∈ A' ⇔ y' < x. Donc **tout élément de A' est inférieur à tout élément de A**. De même, **∀ a ∈ A**, a§e = a&e' = a&e = a ∈ A ⇔ **a > e**, **tout élément de A est supérieur à e**, et **∀ a' ∈ A'**, a'§e = a'&e' = a'&e = a' ∈ A' ⇔ **a' < e, tout élément de A' est inférieur à e**.

Pour en revenir au groupe additif (Z, +) on y retrouve la relation connue : tout nombre strictement négatif est inférieur à tout nombre positif au sens large.

Remarquons que, puisque **a > b** ⇔ a§b = a&b' ∈ A, si la loi de groupe est commutative b'&a ∈ A ⇔ (b'&a)' = a'&b ∈ A'. Or a'&b = a'§b' ⇒ **a' < b'**. **Si donc la loi de groupe est commutative, la relation d'ordre dans A' est inversée par rapport à celle de A**. Là encore, pour en revenir au groupe (Z, +), 3 > 2 et -3 < -2.

Proposition III :

Il est impossible de permuter des éléments entre A et A' sans détruire la stabilité de ces parties.

En effet, une question peut nous venir à l'esprit : Etant donné que si a' est le symétrique de a, réciproquement a est le symétrique de a', peut-on échanger ces éléments entre les deux parties A et A' sans modifier les propriétés de celles-ci ? Soit a ∈ A et donc a' ∈ A'. na ∈ A puisque A est stable et na'= (na)'∈ A'. Si l'on permute a et a' entre A et A', a'∈ A et si A reste stable pour la loi de groupe, na'∈ A. Or na'∈ A' ⇒ na'∈ A∩A'. Mais nous avons démontré que A∩A' = ∅. Donc il est impossible de permuter a et a' sans détruire la stabilité de A. De la même façon on peut démontrer que la stabilité de A' serait aussi détruite. Conclusion :

Les parties A et A' de G* étant définies comme initialement, il est impossible de permuter un seul élément de l'une avec son symétrique dans l'autre sans détruire la stabilité de ces parties.

De même il est impossible de permuter un seul élément de A' avec un de A qui ne soit pas son symétrique sans détruire la stabilité de A. En effet, si nous passions a' de A' à A sans retirer de A le symétrique a de a', et si A restait stable, nous aurions aa' ∈ A. Or aa' = e et e ∉ A, donc la stabilité de A serait dans ce cas une hypothèse absurde.

Mais une autre question se pose alors : et si l'on permutait, non seulement a et a' entre les deux parties A et A', mais aussi tous les éléments na et na', est-ce que les propriétés de A et A' seraient altérées ?

Dans l'exemple page 2 où G = (Z, +) et A = Z*+ et A' = Z*-, on peut former, à partir d'un nombre a $\in$ Z*+ une suite stable d'éléments de Z*+, les nombres na (n = 1, 2, 3, ….). a est le générateur de cette suite. Si a = 1, cette suite stable n'est autre que A tout entier, et le générateur de A' est a' = -1. Mais on peut aussi envisager les parties stables des nombres pairs (non nuls), à savoir dans A : 2, 4, 6, 8, ….. et dans A' : -2, -4, -6, -8, ……Ces deux suites ne contiennent pas tous les éléments de (Z, +). On peut alors considérer qu'elles forment deux « *fibres* » symétriques de (Z, +). De même on peut envisager les multiples non nuls de 3, par exemple, à savoir dans A : 3, 6, 9, 12, ….. et dans A' : -3, -6, -9, -12, …. Il s'agit de deux autres parties stables et l'on peut remarquer qu'entre les fibres de nombres pairs positifs et des multiples de 3 positifs, toutes dans A, il y a des éléments communs, par exemple 6, 12, 18, …. Ces fibres sont reliées un peu comme les fibres d'un élastomère en chimie. (Il existe même des fibres incluses dans d'autres. Ainsi la fibre des multiples de 6, par exemple, est incluse dans la fibre des multiples de 3).

La dernière question que nous nous sommes posée revient alors à celle-ci : Peut-on permuter deux fibres symétriques entre A et A' sans détruire les propriétés initiales de ces deux parties ?

Si ces fibres constituent chacune la totalité d'une des parties A et A', il est évident que oui, la permutation est possible ; elle ne consisterait en fait qu'à échanger les appellations des deux parties : A devenant A' et réciproquement. Par contre si ces fibres ne sont pas des parties pleines de A et A', on se trouve devant le cas suivant : supposons que nous ayons permuté les fibres a, 2a, 3a, … et a', 2a', 3a', … entre A et A' et donc que ces fibres ne soient pas des parties pleines de A et A', il y aurait dans A, par exemple, un élément « b » qui n'appartiendrait pas à la fibre mutée en A'.

Considérons donc la fibre « na » (n= 1, 2, 3, ……+∞) appartenant à A. Elle est telle que (n + 1)a > na. En effet : (n + 1)a = naa = ana $\Rightarrow$ ana§na = ana&na' = a(na&na'). Or, nous avons établi que na&na' = e $\Rightarrow$ a(na&na') = a $\in$ A. Les éléments de la fibre « na » sont donc d'ordre strictement croissant pour n croissant. Cette fibre est isomorphe à la fibre des nombres pairs positifs dans Z*+, laquelle tend vers l'infini. Il s'ensuit que $\forall$ b $\in$ A, il y aura au moins un naturel p tel que pa > b et alors pa§b $\in$ A $\Leftrightarrow$ (pa§b)' = b§pa = b&pa' $\in$ A'. Or b $\in$ A et pa' $\in$ A puisque permutation des fibres na et na' entre A et A'. Donc A n'est plus stable par cette permutation.

Tout ceci démontre dans le cas le plus général la proposition III.

Structures arithmétiques d'un groupe infini:

Dans le cas où l'on choisit dans Z, A= Z*+ et A' = Z*-, ce groupe se trouve donc fractionné selon la partition A, {e}, A'. En considérant maintenant

les deux parties B = A ∪ {e} et B' = A' ∪ {e}, lesquelles sont tout simplement Z+ et Z-, nous voyons apparaître l'arithmétique positive que nous noterons (B, +) et sa symétrique l'arithmétique négative (B', +).

En généralisant ceci nous dirons que lorsqu'un groupe (G, .) est sécable en deux parties stables de (G*, .), disjointes, A et A', contenant à elles deux tous les éléments du groupe sauf son élément neutre e, ce groupe est « *arithmétisable* » et les parties (B, .) = (A ∪ {e}, .) et (B', .) = (A' ∪ {e}, .) seront nommées *arithmétiques* du groupe, l'une étant désignée par commodité comme positive et l'autre négative.

Bien des groupes sont arithmétisables. Ainsi (R, +) dans lequel nous avons B = (R^+, +) et B' = (R^-, +)

Le groupe des vecteurs d'un espace vectoriel à une dimension est aussi arithmétisable relativement à l'addition. Chaque arithmétique correspond à l'un des deux sens possibles.

De même le groupe des vecteurs d'un espace vectoriel à deux dimensions est arithmétisable relativement à l'addition : une arithmétique correspond par exemple à l'ensemble des vecteurs dont le couple des coordonnées (x, y) ⊂ R^+xR et sa symétrique à (x', y') ⊂ R^-xR.

Retour sur la loi de composition inverse :

En utilisant une fois de plus & comme symbole de la loi de groupe et § comme symbole de la loi inverse (rappel : a&b = c ⇔ c§b = a), nous pouvons remarquer le fait suivant :

Si & est commutative : a&b = c ⇔ **c§b = a** et b&a = c ⇔ **c§a = b**. Nous constatons que a et b ont commuté « à travers » le signe « = » dans la loi inverse. Dans mes élucubrations d'étudiant j'ai traduit cela en disant que la loi inverse est alors « *transmutative* » (« trans » pour « à travers », sous entendu le signe « = ». Attention que cette transmutativité consiste en la permutation du deuxième opérande et du résultat de l'opération). Exemple simple : - est l'opération inverse de + en arithmétique élémentaire et 5 – 3 = 2 ⇔ 5 – 2 = 3.

Réciproquement : si la loi inverse § est transmutative, qu'en est-il de la loi directe ? a§b = c ⇔ **c&b = a** et a§c = b ⇔ **b&c = a**. La loi directe est commutative. D'où :

Théorème : **Pour qu'une loi inverse soit transmutative, il est nécessaire et suffisant que la loi directe soit commutative**.

Cette transmutativité n'est pas simplement une curiosité ou le plaisir d'augmenter le vocabulaire déjà volumineux des mathématiques, mais peut être intéressante dans certains groupes. Ainsi, dans le texte « jouons avec certains groupes » nous avons eu affaire à des groupes dont chaque élément est son propre symétrique et nous avons établi que dans ce cas la loi de composition

inverse est identique à la loi de groupe qui doit nécessairement être commutative. Par conséquent, dans ce cas, la loi de groupe est elle-même transmutative et ceci peut nettement simplifier l'établissement de sa table d'opération. Ainsi dans le troisième exemple du texte précité : à df = a correspond da = f ; à fg = c correspond fc = g, etc …(dans ce cas particulier la transmutativité est même valide non seulement avec le deuxième opérande mais aussi avec le premier puisque la loi inverse est commutative).

Après toutes ces considérations sur la loi de composition inverse, nous constatons donc qu'elle a un rôle important.

- Tout d'abord nous avons établi qu'elle est une loi de composition interne dans un groupe.
- Ensuite nous avons montré qu'elle permet de définir des relations d'ordre dans un groupe infini arithmétisable et dans ce que nous avons nommé ses « arithmétiques ».
- Une autre propriété est la suivante : Si les arithmétiques d'un groupe infini sont dénombrables (donc n'ont pas la puissance du continu), on peut classer ses éléments, discrets, par ordres strictement croissant (ou décroissant) et ainsi faire apparaître une autre loi de composition interne : Considérons un groupe dénombrable (infini), arithmétisable, dont la loi de composition interne est notée additive et les éléments de son arithmétique positive rangés par ordre croissant et désignés ainsi : a_1, a_2, a_3,….,a_n ($n \rightarrow \infty$). Soit « x » un élément de cette arithmétique positive et soit la composition x + x + x, pour laquelle nous faisons correspondre a_1 au 1^{er} x, a_2 au $2^{ème}$ et a_3 au $3^{ème}$ (il s'agit donc d'utiliser les a_1, a_2, et a_3 comme comptage des x). Nous pouvons alors écrire x + x + x = a_3.x, en adoptant la notation multiplicative symbolisée ici par un point. Il s'agit d'une nouvelle loi de composition interne que j'ai qualifiée, toujours dans mes élucubrations d'étudiant, de loi « *sommative* » déduite de la loi additive. Cette loi a la propriété suivante : soient x et y deux éléments de l'arithmétique concernée et (x + y) + (x + y) + (x + y) = a_3.(x + y). Si la loi additive est commutative, en outre d'être associative : (x + y) + (x + y) + (x + y) = (x + x + x) + (y + y + y) = (a_3.x) + (a_3.y). Par conséquent **a_3.(x + y) = (a_3.x) + (a_3.y)**. Le multiplicateur a_3 s'est donc « distribué » sur les éléments x et y de la composition additive. D'où :

Théorème : **Une loi sommative déduite d'une loi associative et commutative est distributive sur cette loi**.

Ceci n'est pas vraiment nouveau et n'est en fait que la généralisation abstraite de cette propriété qu'a la multiplication, en algèbre, d'être distributive sur l'addition (je dis « sur » l'addition plutôt que « par rapport » à l'addition car cela me paraît moins lourd et répondant mieux à l'image de cartes distribuées sur une table de jeu devant chaque joueur). La multiplication, en arithmétique et en algèbre, est donc une loi sommative selon ma terminologie. Elle n'est pas la

seule. L'opération « puissance » l'est aussi, mais sur la multiplication. En effet : $(x.y)^a = x^a .y^a$.

D'autre part, si la loi sommative est distributive sur une loi commutative et associative, elle l'est aussi sur sa loi de composition inverse. En effet : a.(x§y) = a.(x&y') = (a.x)&(a.y') = (a.x)§(a.y). Ainsi, en algèbre classique a.(x – y) = (a.x) – (a.y) et $(x/y)^a = x^a/y^a$.

J'avais développé ces notions en pensant au « grand théorème de Fermat » qui n'avait pas encore été démontré de façon générale lorsque j'étais étudiant (début des années 1960). Je m'étais alors posé la question suivante : ce théorème est-il vraiment démontrable ou ne serait-il qu'un axiome à ajouter, comme le postulat d'Euclide en géométrie, à ceux de Peano définissant les entiers naturels et aux lois de composition dans cet ensemble ? S'il n'était qu'un axiome, il devrait être alors possible d'envisager une arithmétique « non-fermatienne » comme il y a des géométries non-euclidiennes ? En utilisant ces notions d'arithmétiques de groupes, de lois inverses et de lois sommatives, j'ai donc essayé de constituer une arithmétique « non-fermatienne » répondant à toutes les propriétés de base de l'arithmétique classique. Mais j'ai bien vite constaté que mon arithmétique abstraite était en fait isomorphe à l'arithmétique classique, et que donc, si le théorème de Fermat était un axiome de l'arithmétique classique, il se retrouvait aussi être nécessairement de mon arithmétique abstraite, donc lié aux précédentes propriétés.

Aujourd'hui le fameux « grand théorème de Fermat » est démontré dans le cas général, depuis plus de 20 ans par le mathématicien britannique Andew Whiles et sa question est donc close.

*

* *