Groupes

La notion de groupe introduite par L.-A. Cauchy et E. Galois[1] apparaît au début du XIX^{ème} siècle ; cette notion était restée limitée aux groupes de permutations d'un ensemble fini d'objets. Les débuts de la cristallographie mathématique font apparaître d'autres groupes finis constitués de rotations et de symétries ayant un point invariant. C. Jordan, en 1868, aborde l'étude des groupes de déplacements (finis ou non) dans l'espace euclidien à 3 dimensions. S. Lie, dans la réalisation d'un travail dans le domaine des équations différentielles, introduit le concept de groupe continu de transformations[2]. En même temps, F. Klein est amené[3] à mettre la notion de groupe de transformations à la base de la géométrie[4] élémentaire.
Il faut attendre la fin du XIX^{ème} siècle pour que la structure de groupe soit enfin définie de façon intrinsèque et puisse être appliquée à d'autres ensembles que ceux constitués de transformations.

L'addition et la multiplication dans les réels ou les complexes, la composition d'applications de $\mathbb{R}$ dans $\mathbb{R}$ ou d'isométries du plan (affine euclidien) sont des lois (internes) qui possèdent en commun un ensemble de propriétés, telles que, par exemple, l'associativité[5]. La notion de groupe permet de donner un cadre commun à de tels ensembles munis de ces lois.

I.— Lois de composition interne

Définition 1.– E est un ensemble non vide.
Une **loi de composition interne** dans E est une application :

$$\begin{array}{rccc} * : & E\times E & \to & E \\ & (x,y) & \mapsto & *((x,y)) \overset{\text{noté}}{=} x*y \end{array}$$

L'élément $x*y$ de E est appelé composé de x et de y.

Exemple 1.– $\begin{array}{rccc} + : & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R} \\ & (x,y) & \mapsto & x+y \end{array}$ est l'addition dans $\mathbb{R}$.
L'image par $+$ du couple (x,y) est la somme de x et de y.

Exemple 2.– $\begin{array}{rccc} \circ : & T\times T & \to & T \\ & (t_{\vec{u}},t_{\vec{v}}) & \mapsto & t_{\vec{u}}\circ t_{\vec{v}} = t_{\vec{u}+\vec{v}} \end{array}$ est la composition des translations du plan

Définition 2.– E est muni de la loi de composition interne $*$.
1) La loi $*$ est **associative** si :

$$\forall\,(x,y,z)\in E\times E\times E,\ (x*y)*z = x*(y*z)\,.$$

On convient de noter $x*y*z$ un tel élément.
2) La loi $*$ est **commutative** si :

$$\forall\,(x,y)\in E\times E,\ x*y=y*x.$$

[1] Au cours de travaux sur la résolution des équations algébriques par radicaux, Galois obtient en considérant certains groupes (finis) de permutations des racines d'une équation algébrique des résultats décisifs sur la résolution par radicaux.
[2] Ce concept de groupe de Lie est au confluent de l'algèbre et de la géométrie différentielle et est d'une importance considérable dans de nombres domaines des Mathématiques et de la Physique théorique.
[3] Le programme d'Erlagen publié par F. Klein en 1872 *constitue une des principales étapes du renouvellement de la conception de la géométrie et de son intégration dans une vue unifiée des Mathématiques,* P. F. Russo, s.j.
[4] Une géométrie correspond à la donnée d'un espace et d'un groupe de transformations agissant sur cet espace. Le but étant l'étude des notions invariantes sous l'action de ce groupe.
[5] propriété que ne possède d'ailleurs pas une loi aussi simple que la soustraction dans $\mathbb{R}$.

3) Un élément e de E est dit **neutre** si :

$$\forall x \in E,\ x * e = e * x = x.$$

4) Si la loi $*$ possède un élément neutre e, on dit que l'élément x de E est symétrisable s'il existe un élément x' de E tel que :

$$x * x' = x' * x = e.$$

L'élément x' est appelé **symétrique** de x pour la loi $*$.

Exemple 3.– L'addition dans $\mathbb{R}$ est associative, commutative, possède un (unique) élément neutre 0 ; de plus, tout réel x a un symétrique pour l'addition : c'est son opposé $-x$.

Exemple 4.– La composition des translations du plan est associative, commutative, possède un (unique) élément neutre Id qui est la translation de vecteur nul $t_{\overrightarrow{0}}$; de plus, toute translation $t_{\overrightarrow{u}}$ a un symétrique pour cette loi : c'est son application réciproque $(t_{\overrightarrow{u}})^{-1}$qui est bien une translation du plan puisque égale à $t_{-\overrightarrow{u}}$.

II.— Groupes

Définition 1.– Un couple $(G, *)$, où G est un ensemble et $*$ une loi de composition interne, est un **groupe** si la loi $*$ est associative, posséde un élément neutre, et est telle que tout élément de G admet un symétrique.

Le groupe est dit **abélien** si, de plus, la loi de composition interne est commutative.

Remarque 1.– Puisque qu'un groupe possède un élément neutre, il n'est jamais vide.

Exemple 1.– $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$ [1], $(\{-1, 1\}, \times)$ sont des groupes.

Exemple 2.– $(\mathcal{U}, \times)$, où $\mathcal{U}$ désigne l'ensemble des complexes de module 1 (complexes unimodulaires), est un groupe abélien (le symétrique de $e^{i\theta} \in \mathcal{U}$ est $e^{-i\theta} \in \mathcal{U}$).

Exemple 3.– ABC est un triangle équilatéral dont on note par O le centre du cercle circonscrit. Pour $k \in \{0, 1, 2\}$, on note par r_k la rotation du plan euclidien (rapporté à un repère orthonormé direct) de centre O et dont une mesure de l'angle est $\dfrac{2k\pi}{3}$ (r_0 est l'identité du plan $\mathcal{P}$, notée $Id_{\mathcal{P}}$). On désigne par A' (*resp.* B', C') le milieu de $[BC]$ (*resp.*$[AC]$, $[AB]$) et par $s_{(AA')}$ (*resp.* $s_{(BB')}, s_{(CC')}$) la réflexion d'axe (AA') (*resp.*(BB') , (CC')).
Soit l'ensemble $\mathcal{I}(ABC) = \left\{r_0, r_1, r_2, s_{(AA')}, s_{(BB')}, s_{(CC')}\right\}$ des isométries du plan conservant le triangle équilatéral ABC. $(\mathcal{I}(ABC), \circ)$ est un groupe appelé groupe des isométries du triangle équilatéral ABC.

Exemple 4.– Soit E un ensemble non vide. σ_E désigne l'ensemble des bijections de E sur lui-même. σ_E appelé ensemble des permutations de E a une structure de groupe pour la loi $\circ$.

Exercice 1.– Montrer qu'un groupe ne possède qu'un seul élément neutre.

Exercice 2.– Montrer que dans un groupe tout élément admet un seul symétrique.

Le symétrique de a sera noté a^{-1}.

Proposition 1.– Soit $(G, *)$ un groupe. L'équation $a * x = b$ a une unique solution $x = a^{-1} * b$.

Exercice 3.– $(G, *)$ est un groupe. Montrer que : $(x * y)^{-1} = y^{-1} * x^{-1}$.

[1] $(\mathbb{R}, \times)$ n'est pas un groupe car l'élément 0 n'a pas de symétrique pour la loi $\times$ (0 n'a pas d'inverse).

f

Exercice 4.– Soit $(G,*)$ un groupe de neutre e tel que : $\forall x \in G, x*x=e$. Montrer que G est abélien.

Exercice 5.– Soit G l'ensemble des applications

$$\varphi : z \mapsto \frac{az+b}{cz+d} \quad \text{où } a,b,c \text{ et } d \text{ sont des réels tels que : } ad-bc=1$$

de l'ensemble $\mathcal{P}$ des complexes de partie imaginaire strictement positive dans lui-même.
Montrer que $(G,\circ)$ est un groupe.

III.— Sous-groupes

Soit $(G,*)$ un groupe et G' une partie non vide de G.
On dit que G' est **stable** pour la loi $*$ si :

$$\forall (x',y') \in G' \times G',\ x' * y' \in G'.$$

Définition 1.– On appelle **sous-groupe** d'un groupe $(G,*)$ toute partie G' de G stable pour la loi $*$ et telle que la loi $*'$ définie sur G' par $\forall (x',y') \in G' \times G',\ x' *' y' = x' * y'$ soit une loi de groupe.
La loi $*'$ est appelée **loi induite** sur G' par la loi $*$.

On convient de noter $*'$ par $*$.

Le théorème suivant dont la démonstration est immédiate est une caractérisation d'un sous-groupe très utilisée.

Théorème 1.– Soit $(G,*)$ un groupe de neutre e et G' une partie de G.
Pour que G' soit un sous-groupe de G, il faut et il suffit que l'on ait :
- $[SG_1]$ $e \in G'$
- $[SG_2]$ G' est stable pour $*$
- $[SG_3]$ le symétrique de tout élément de G' appartient encore à G'.

Pratiquement, on peut remplacer les conditions $[SG_2]$ et $[SG_3]$ par la seule condition :
$[SG_4]$ $\forall (x',y') \in G' \times G',\ x' * y'^{-1} \in G'$
où y'^{-1} est le symétrique de y'.

Exemple 1.– $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

Exemple 2.– Soit $(G,*)$ un groupe de neutre e. Les ensembles $\{e\}$ et G lui-même sont des sous-groupes de G.

Exemple 3.– $\mathcal{I}^+(ABC) = \{r_0, r_1, r_2\}$ est un sous-groupe du groupe des isométries du triangle équilatéral $(\mathcal{I}(ABC), \circ)$ dit sous-groupe des déplacements du triangle équilatéral.

Exemple 4.– $\mathcal{U}_n$ ensemble des racines $n^{ièmes}$ de l'unité est un sous-groupe de $\mathcal{U}$.

Exercice 1.– Soit a un entier fixé et soit $a\mathbb{Z}$ l'ensemble des entiers de la forme $a.n$ où $n \in \mathbb{Z}$.

1. Montrer que $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
2. Réciproquement, établir que tout sous-groupe H de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ (où $a \in \mathbb{N}$).
[on pourra, pour $H \neq \{0\}$,désigner par a le plus petit élément strictement positif de H puis effectuer pour tout m de H, la division euclidienne[1] dans $\mathbb{Z}$ de m par a]

Proposition 1.– L'intersection de deux sous-groupes de G est un sous-groupe de G.

Démonstration. Considérons un groupe G et soient G'et G" deux sous-groupes de G. Etablissons que $G' \cap G$" est encore un sous-groupe de G en utilisant les propriétés $[SG_1]$ et $[SG_4]$.

[1] $m = aq + r,\ 0 \le r < a,\ q \in \mathbb{Z}$

Puisque e, neutre du groupe appartient à chaque sous-groupe, il appartient à $G' \cap G$"; $[SG_1]$ est alors vérifiée.

Soient x et y deux éléments de $G' \cap G$" ; puisque x et y appartiennent tous deux à G', d'après $[SG_4]$,l'élément $x * y^{-1}$ appartient aussi à G'. De manière analogue, on obtient $x * y^{-1} \in G$". Et ainsi $x * y^{-1} \in G' \cap G$". $[SG_4]$ est donc vérifiée et le résultat en découle.

IV.— Homomorphismes de groupes

Définition 1.– $(G, *)$ et $(G', *')$ sont deux groupes .
1) On dit qu'une application $f : G \to G'$ est un **homomorphisme** de $(G, *)$ dans $(G', *')$ si :

$$\forall (x, y) \in G \times G, \quad f(x * y) = f(x) *' f(y).$$

2) Un **isomorphisme** f de $(G, *)$ sur $(G', *')$ est une bijection de G sur G' telle que f et f^{-1} soient des homomorphismes de groupes.

Exemple 1.– L'application : $n \mapsto (-1)^n$ réalise un homomorphisme du groupe $(\mathbb{Z}, +)$ sur le groupe $(\{-1, 1\}, \times)$.

Exemple 2.– La fonction logarithme népérien (ln) est un isomorphisme de $\left(\mathbb{R}_+^*, \times\right)$ sur $(\mathbb{R}, +)$. L'application exponentielle (exp) réalise l'isomorphisme réciproque.

Remarque 1.– L'intérêt de l'utilisation d'un isomorphisme réside dans le fait que l'on peut transporter un problème donné dans un groupe dans un groupe plus sympathique.

Bibliographie

[ArnFra] J.-M. Arnaudies, H. Fraysse, *Cours de Mathématiques, t.1 Algèbre*, Dunod, 1996

[EU] Encyclopaedia Universalis, vol. 8, 59-80, 1980

[Lem] H. Lemberg, *Bien commencer ses études supérieures en Mathématiques*, Collection Studio Sup, Vuibert Supérieur, 1997

[ReiSoe] F. Reinhardt, H. Soeder, *Atlas des Mathématiques*, Le livre de poche, 1997

David Azuelos, Patrick Cabau, 1999-2013