Groupes

Maxime CARRIERE

26 septembre 2011

Table des matières

Chapitre 1

Généralités

1.1 Notion de "Groupe"

Un groupe désigne un ensemble, sur lequel on a définit une opération devant vérifier certaines propriétés. En fait, on peut voir un groupe comme un ensemble qui, par son opération, possède une certaine "structure". On dit qu'il s'agit d'une structure algébrique. Il existe en mathématiques d'autres structures algébriques, les principales étant les anneaux et les corps.

La structure de groupe est quant à elle omniprésente en mathématiques et commune à des ensembles d'objets mathématiques bien différents (voir Exemple 1.1.1). Le rôle de la notion de groupe, est de fournir un cadre d'étude général pour tous ces ensembles.

Définition 1.1.1 (Loi de composition interne) *On appelle loi de composition interne $*$ sur un ensemble X, toute application*

$$f : \begin{cases} X \times X \longrightarrow X \\ (x, y) \longmapsto z = f(x, y) \end{cases}$$

On note alors $x * y = f(x, y)$ et on dira que X est stable par $*$

Remarque 1.1.1 *Dire que $*$ est une loi de composition interne sur X signifie que, si l'on opère deux éléments de X, alors on reste dans X.*

Définition 1.1.2 (Groupe) *On appelle groupe, un couple $(G, *)$, où G est un ensemble et $*$ une loi de composition interne sur G vérifiant les trois propriétés suivantes :*

1. *Associativité : $\forall x, y, z \in G$, $[(x * y) * z = x * (y * z)]$*
2. *Existence d'un élément neutre : $\exists e \in G$, $\forall x \in G$, $[x * e = e * x = x]$*
3. *Existence d'un symétrique : $\forall x \in G$, $\exists y \in G$, $[x * y = y * x = e]$*

Remarque 1.1.2

- *L'associativité signifie que l'on peut mettre les parenthèses où l'on veut.*
- *On peut voir l'élément neutre comme "l'élément central" du groupe.*
- *La 3^{me} propriété signifie que pour tout élément x de G, il existe un élément qui permet de "revenir au milieu".*

Définition 1.1.3 *On dit que $(G, *)$ est un groupe commutatif (ou abélien) si la loi $*$ est commutative, i.e. si elle vérifie :*

$$\forall x, y \in G,\ x * y = y * x$$

Remarque 1.1.3

- *La commutativité signifie que l'ordre n'a pas d'importance*
- *Attention ! En règle général, un groupe n'est pas commutatif, et on ne peut donc pas dans les calculs, inverser x et y.*

Exemple 1.1.1

- *$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{R}*, \times)$, sont des groupes commutatifs, mais $(\mathbb{N}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ ne sont pas des groupes (où $+$ et $\times$ désigne l'addition et la multiplication des nombres entiers).*
- *$(\mathcal{M}_{n,k}, +)$ est un groupe commutatif (où $+$ désigne l'addition des matrices)*
- *L'ensemble des applications bijectives munit de la loi de composition pour les fonctions $\circ$ est un groupe non commutatif.*
- *L'ensemble des translations du plan munit de la loi $\circ$ est un groupe abélien*
- *$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif (où $\mathbb{Z}/n\mathbb{Z}$ désigne l'ensemble des entiers modulo n et $+$ désigne l'addition des entiers modulo n)*
- *L'ensemble S_n des permutations de l'ensemble $X = \{1, ..., n\}$, munit de la loi $\circ$, est un groupe non commutatif*

Méthode 1.1.1 *Pour prouver que $(G, *)$ est un groupe, on doit montrer que :*

1. *$*$ est une loi de composition interne : On montre que $\forall x, y \in G,\ x * y \in G$*
2. *$*$ est associative : On calcule $(x * y) * z$ et $x * (y * z)$ pour montrer qu'on arrive au même résultat.*
3. *Il existe un élément neutre : On doit trouver un élément e de G qui vérifie : $x * e = x$ et $e * x = x$*
4. *Tout élément de G est symétrisable : Pour tout $x \in G$, on cherche un y qui "annule" x. On vérifie que ce y est bien le symétrique de x.*

Il existe deux types de notations pour la loi de composition d'un groupe :

Notation 1.1.1 (Multiplicative) *Elle est utilisée pour énoncer les propriétés générales des groupes et lorsque $*=\times$, $.$, $\circ$. On dira alors que le groupe est multiplicatif*

- *$x * y$ est appelé produit de x et y*
- *L'élément neutre est noté e ou 1*
- *On appelle inverse de x, noté x^{-1} le symétrique de x.*
- *On note $x^n = x * x \cdots * x$ (n-fois).*
- *Par convention on pose $x^0 = 1$ ou e et $x^{-n} = (x^n)^{-1} = (x^{-1})^n$*
- *Dans la pratique, pour plus de clarté, on omettra d'écrire le signe de la loi : Ainsi on écrira souvent xy au lieu $x * y$*

Notation 1.1.2 (Additive) *Elle est utilisé pour l'étude des groupes commutatifs et lorsque $*=+$. On dira alors que le groupe est additif*

- *$x + y$ est appelé somme de x et y*
- *L'élément neutre est noté 0*
- *On appelle opposé de x, noté $-x$ le symétrique d'un élément x.*
- *On note $nx = x + x \cdots + x$ (n-fois).*
- *Par convention on pose $0x = 0$ et $-nx = -(nx) = n(-x)$*

Table d'un groupe :

Si G est un groupe fini, c'est à dire qui ne contient qu'un nombre fini d'éléments $x_1, \cdots, x_n$, alors on peut alors construire la table de la loi $*$:

$*$	x_1	x_2	$\cdots$	x_n
x_1	$x_1 * x_1$	$x_1 * x_2$	$\cdots$	$x_1 * x_n$
x_2	$x_2 * x_1$	$x_2 * x_2$	$\cdots$	$x_2 * x_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	$x_n * x_1$	$x_n * x_2$	$\cdots$	$x_n * x_n$

Cette table peut permettre de mettre en évidence l'élément neutre, ou les éléments symétriques des différents éléments du groupe.

Voici maintenant quelques propriétés élémentaires :

Propriétés 1.1.1 *Soit $(G, *)$ un groupe, alors*

1. *L'élément neutre est unique et est son propre symétrique*
2. *$\forall x \in G$, le symétrique de x est unique*

Preuve :

1. • Supposons qu'il existe deux éléments neutres e_1 et e_2. Alors :
   · $e_1 * e_2 = e$ car e_2 élément neutre de G
   · $e_1 * e_2 = e_2$ car e_1 élément neutre de G
   Donc $e_1 = e_2$ ce qui prouve l'unicité
   • Soit e l'unique élément neutre de G.
   On a $e * e = e$ ce qui prouve que e est son propre symétrique
2. Soit $x \in G$. Supposons qu'il existe deux symétriques y et z de x. Alors :
   $y = y * e$ (car e élément neutre)
   $= y * (x * z)$ (car z symétrique de x)
   $= (y * x) * z$ (par associativité)
   $= e * z$ (car y symétrique de x)
   $= z$ (car e élément neutre)
   Donc $y = z$ ce qui prouve l'unicité du symétrique.

Propriétés 1.1.2 *Soit $(G, *)$ un groupe, alors : $\forall x, y \in G$, $(x*y)^{-1} = y^{-1} * x^{-1}$*

Preuve :

• Soit $x, y \in G$. On a :
$(x * y) * (y^{-1} * x^{-1})$
$= x * (y * y^{-1}) * x^{-1}$ (par associativité)
$= x * e * x^{-1}$
$= x * x^{-1} = e$
• Ainsi, $(y^{-1} * x^{-1})$ est le symétrique de $(x * y)$ et $(x * y)^{-1} = y^{-1} * x^{-1}$

Remarque 1.1.4

- *Attention en règle général $(x * y)^{-1} \neq (x^{-1} * y^{-1})$.*
- *On a l'égalité seulement dans le cas où G est un groupe commutatif.*

1.2 Sous-groupes

Un sous-groupe désigne une partie d'un groupe qui possède la même "structure" que celui-ci :

Définition 1.2.1 (Sous-Groupe) *Soit $(G,*)$ un groupe. On dit qu'une partie H de G est un sous-groupe de G ssi :*

1. *$*$ est une loi de composition interne pour H*
2. *$(H,*)$ est un groupe*

Remarque 1.2.1
- *Par définition un sous-groupe est un groupe.*
- *G et $\{e\}$ sont des sous-groupes du groupe G. Ils sont appelés les sous-groupes triviaux de G*

Propriétés 1.2.1 *Soit $(G,*)$ un groupe et H un sous-groupe de G. Alors :*

1. *G et H ont le même élément neutre : e_G=e_H*
2. *$\forall x \in H$, x admet le même symétrique dans G et dans H*

Preuve : Soit $(G,*)$ un groupe, et H un sous-groupe de G

1. Soit e_G et e_H les éléments neutres de G et H. On a : $x * e_G = x = x * e_H$. En composant à gauche par x^{-1}, le symétrique de x dans G, on obtient $e_G = e_H$.
2. Soient $x \in H$, x^{-1} le symétrique de x dans G et x' le symétrique de x dans H. On a $x * x' = x * x^{-1} = e$. En composant par x^{-1} à gauche on obtient $x^{-1} = x'$

La notion de sous-groupe est caractérisée par le théorème suivant :

Théorème 1.2.1 *Soit $(G,*)$ un groupe et soit H une partie de G. H est un sous-groupe de G ssi :*

1. *$H \neq \emptyset$*
2. *$\forall x, y \in H$, $x * y^{-1} \in H$*

Preuve : Soit $(G,*)$ un groupe
$\Rightarrow$: Soit H un sous-groupe de G. Montrons qu'il vérifie la propriété précédente.
• H est un groupe, donc il existe un élément neutre e dans H et $H \neq \emptyset$.
• Soit $x, y \in H$. Comme H est un groupe, $y^{-1} \in H$. Comme par hypothèse $*$ est une loi de composition interne, on a $x * y^{-1} \in H$.
$\Leftarrow$: Soit H une partie de G vérifiant la propriété précédente. Montrons qu'il s'agit d'un sous-groupe.
• **Élément neutre** : $H \neq \emptyset \Rightarrow \exists h \in H$. Par (2) on a : $h * h^{-1} \in H$, d'où $e \in H$
• **Symétrique** : Par (2) encore, $\forall x \in H, e * x^{-1} \in H$, d'où $x^{-1} \in H$
• **Stabilité de H par $*$** : Par (2) toujours, $\forall x, y \in H$, $x * (y^{-1})^{-1} \in H$ i.e. $x * y \in H$ ce qui prouve que $*$ est une loi de composition interne pour H.
• **Associativité** : G est un groupe, donc $*$ est associative, et sa restriction à H l'est donc aussi.
• Finalement, on a prouvé que $*$ est une loi de composition interne pour H et $(H,*)$ est un groupe, c'est à dire que H sous-groupe de G

Exemple 1.2.1
- $(\mathbb{Z}, +)$ *est un sous-groupe de* $(\mathbb{R}, +)$
- $(\mathbb{R}_+*, \times)$ *est un sous-groupe de* $(\mathbb{R}*, \times)$
- $\forall n \in \mathbb{N}$, *l'ensemble des multiples de* n, *noté* $n\mathbb{Z}$ *est un sous-groupe de* $\mathbb{Z}$
- *L'ensemble des applications bijectives et continues est un sous groupe du groupe des bijections.*

Méthode 1.2.1
• *Pour prouver que* H *est un sous-groupe de* G *on utilise la propriété précédente :*
- *On montre par exemple que* $e \in H$ *où* e *est l'élément neutre de* G.
- *On montre successivement que* $x \in H \Rightarrow x^{-1} \in H$ *et que* $x, y \in H \Rightarrow (x * y) \in H$.

• *Pour prouver qu'un ensemble est un groupe, on peut montrer que c'est un sous-groupe d'un groupe plus vaste.*

Définition 1.2.2 *Soit* $(G, *)$ *un groupe. Soit* S *l'ensemble de ses-sous groupes. On définit la relation* $\leqslant$ *sur* S *de la manière suivante :*

$$\forall H_1, H_2 \in S,\ [H_1 \leqslant H_2 \Longleftrightarrow H_1] \text{ est un sous groupe de } H_2$$

Théorème 1.2.2 $\leqslant$ *est une relation d'ordre sur* S

Preuve :
- Réflexivité : $\forall H \in S,\ H \leqslant H$ (car H est toujours sous-groupe de lui-même)
- Symétrie : $\forall H_1, H_2 \in S,\ [(H_1 \leqslant H_2 \text{ et } H_2 \leqslant H_1) \Rightarrow H_1 = H_2]$ (car $[H_1 \subset H_2 \text{ et } H_2 \subset H_1] \Rightarrow H_1 = H_2$)
- Transitivité : $\forall H_1, H_2, H_3 \in S,\ [(H_1 \leqslant H_2 \text{ et } H_2 \leqslant H_3) \Rightarrow H_1 \leqslant H_3]$ (car $[H_1 \subset H_2 \text{ et } H_2 \subset H_3] \Rightarrow H_1 \subset H_3$)

Remarque 1.2.2 *En général,* $\leqslant$ *n'est pas une relation d'ordre totale. En effet,* $2\mathbb{Z}$ *et* $3\mathbb{Z}$ *sont des sous-groupes de* $\mathbb{Z}$, *mais aucun des deux ensembles est un sous-groupe de l'autre.*

Définition 1.2.3 (Centre d'un groupe) *Soit* $(G, *)$ *un groupe. On appelle centre de* G, *noté* $Z(G)$, *l'ensemble des éléments de* G *qui commutent avec tous les éléments du groupe :*

$$Z(G) = \{x \in G \,|\forall y \in G,\ x * y = y * x\}$$

Théorème 1.2.3 *Soit* $(G, *)$ *un groupe alors* $Z(G)$ *est un sous-groupe de* G

Preuve :
- Il est clair que $e \in Z(G)$
- Soit $x \in Z(G)$ alors $\forall y \in G,\ x * y = y * x$. En multipliant à gauche et à droite par x^{-1}, on obtient $\forall y \in G,\ x^{-1} * y = y * x^{-1}$. Donc $x^{-1} \in G$.
- Soit $x, y \in Z(G)$, alors en utilisant successivement la commutativité de z et de y, on a : $\forall z \in G,\ x * y * z = x * z * y = z * x * y$. Donc $x * y \in Z(G)$ et $Z(G)$ est stable par $*$

1.3 Morphismes de groupes

Un morphisme de groupe désigne une application qui conserve la structure des groupes. Ces applications vont jouer un rôle très important dans la théorie des groupes, ainsi que dans ses applications.

Définition 1.3.1 (Morphisme de groupe) *Soient deux groupes $(G_1, *)$ et $(G_2, *')$ et f une application de G vers H. On dit que f est un morphisme de groupe (ou homomorphisme de groupe) si elle vérifie :*

$$\forall x, y \in G_1,\ f(x * y) = f(x) *' f(y)$$

Définition 1.3.2
- *Un appelle isomorphisme tout morphisme bijectif.*
- *Un appelle endomorphisme tout morphisme d'un groupe dans lui même*
- *Un appelle automorphisme tout endomorphisme bijectif*

Définition 1.3.3 *On dit que deux groupes $(G_1, *)$ et $(G_2, *')$ sont isomorphes, si il existe un isomorphisme de G_1 vers G_2. On note alors $G_1 \approx G_2$.*

Remarque 1.3.1 *Deux groupes isomorphes possèdent, d'une part le même nombre d'éléments, et d'autre part la même structure entre ses éléments. Ainsi, la seule chose qui diffère entre deux groupes isomorphes, c'est le nom de ses éléments : Deux groupes sont isomorphes s'ils sont égaux au nom des variables près. Aussi, deux groupes isomorphes possèdent les mêmes propriétés, et en particulier la même table.*

Exemple 1.3.1
- *Soit $(G_1, *)$ et $(G_2, *')$ d'éléments neutres respectifs e et e' L'application suivante est un morphisme :*

$$\phi : \begin{cases} G_1 \longrightarrow G_2 \\ x \longmapsto e' \end{cases}$$

- *L'application exponentielle est un isomorphisme de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+*, \times)$*
- *L'application logarithme est un isomorphisme de $(\mathbb{R}_+*, \times)$ vers $(\mathbb{R}, +)$*
- *L'application identité est un automorphisme*

Théorème 1.3.1 *La composée de deux morphismes est encore un morphisme*

Preuve :

Soient trois groupes $(G_1, *)$ et $(G_2, *')$ et $(G_3, *'')$ et soient deux morphismes de groupes $f : G_1 \to G_2$ et $g : G_2 \to G_3$. Alors $\forall x, y \in G_1$ on a :
$(g \circ f)(x * y) = g(f(x * y))$
$= g(f(x) *' f(y))$ (car f morphisme)
$= g(f(x)) *'' g(f(y))$ (car g morphisme)
$= (g \circ f)(x) *'' (g \circ f)(y)$
Ce qui prouve que $g \circ f$ est un morphisme de groupe.

Théorème 1.3.2 *La réciproque d'un isomorphisme est un isomorphisme*

Preuve :

Soient deux groupes $(G_1, *)$ et $(G_2, *')$ et $f : G_1 \to G_2$ un isomorphisme de groupe. Soit $x, y \in G_2$. f est bijective donc $\exists! a, b \in G_1$ tel que $f(a) = x$ et $f(b) = y$, i.e. $a = f^{-1}(x)$ et $b = f^{-1}(y)$. f est un morphisme donc :

$f(a * b) = f(a) *' f(b)$

$\Leftrightarrow f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) *' f(f^{-1}(y)) = x *' y$

$\Leftrightarrow f^{-1}(x) * f^{-1}(y) = f^{-1}(x *' y)$ (En composant par f^{-1})

Ce qui prouve que f^{-1} est un morphisme de groupe

Théorème 1.3.3 *Soit deux groupes $(G_1, *)$ et $(G_2, *')$ d'éléments neutres respectifs e et e' et f un morphisme de groupe de G_1 vers G_2. On a :*

1. $f(e) = e'$
2. $\forall x \in (G, *)_1 \ f(x^{-1}) = f(x)^{-1}$
3. $\forall x \in (G, *)_1, \forall n \in \mathbb{Z}, \ f(x^n) = f(x)^n$

Preuve :

1. $f(e) *' f(e) = f(e * e) = f(e)$. Donc en multipliant par $f(e)^{-1}$, on obtient $f(e) = f(e) *' f(e)^{-1} = e'$
2. $f(x) *' f(x^{-1}) = f(x * x^{-1}) = f(e) = e'$ donc $f(x^{-1})$ est l'inverse de $f(x)$ d'où $f(x)^{-1} = f(x^{-1})$
3. • Soit $x \in G_1$. Montrons par récurrence que $\forall n \in \mathbb{N}$, on a : $f(x^n) = f(x)^n$:
   · D'après (1) la propriété est vraie au rang 0
   · Supposons que la propriété est vraie au rang n, montrons qu'elle est vraie au rang $n + 1$:
   $f(x^{n+1}) = f(x^n * x) = f(x^n) *' f(x) =^{(HdR)} f(x)^n *' f(x) = f(x)^{n+1}$
   · Donc $\forall n \in \mathbb{N}$, la propriété $f(x^n) = f(x)^n$ est vraie
   • Soit $x \in G_1$, Montrons que $\forall n \in \mathbb{Z} \setminus \mathbb{N}$, on a $f(x^n) = f(x)^n$:
   $f(x^n) = f((x^{-n})^{-1}) =^{(*)} f(x^{-n})^{-1} =^{(**)} (f(x)^{-n})^{-1}) = f(x)^n$
   (*) On applique (2)
   (**) Comme $-n \in \mathbb{N}$, on peut appliquer la première partie de la preuve.

Théorème 1.3.4 *Soit deux groupes $(G_1, *)$ et $(G_2, *')$ d'éléments neutres respectifs e et e' et f un morphisme de groupe de G_1 vers G_2. Soit H_1 un sous-groupe de G_1 et H_2 un sous-groupes de G_2 On a :*

1. *$f(H_1)$ est un sous-groupe de G_2. (où $f(H_1) = \{f(x) \mid x \in H_1\}$)*
2. *$f^{-1}(H_2)$ est un sous-groupe de G_1. (où $f^{-1}(H_2) = \{x \mid f(x) \in H_2\}$)*

Preuve :

1. • $e' = f(e) \in f(H_1)$ donc $f(H_1) \neq \emptyset$
   • Soit $x, y \in f(H_1)$ alors $\exists a, b \in H_1$ tel que $f(a) = x$ et $f(b) = y$. $x *' y^{-1} = f(a) *' f(b)^{-1} = f(a * b^{-1})$ (On utilise la propriété précédente). Or, comme H_1 est un groupe on a $a * b^{-1} \in H_1$ et $x *' y^{-1} \in f(H_1)$
   • Conclusion : $f(H_1)$ est un sous-groupe de G_2
2. • $f(e) = e' \in (H_2)$ donc $e \in f^{-1}(H_2) \neq \emptyset$
   • Soit $x, y \in f^{-1}(H_2)$ alors $\exists a, b \in H_2$ tel que $f(x) = a$ et $f(y) = b$. $f(x * y^{-1}) = f(x) *' f(y)^{-1} = a *' b^{-1}$ (On utilise la propriété précédente). Or, comme H_2 est un groupe on a $a * b^{-1} \in H_2$ et $x *' y^{-1} \in f^{-1}(H_2)$
   • Conclusion : $f^{-1}(H_2)$ est un sous-groupe de G_1

Corollaire 1.3.1 *Soit deux groupes $(G_1, *)$ et $(G_2, *')$ d'éléments neutres respectifs e et e' et f un morphisme de groupe de G_1 vers G_2.*

1. *$Im(f) = f(G_1)$, appelée image de f, est un sous-groupe de G_2*
2. *$ker(f) = f^{-1}\{e'\} = \{x \in G_1 \mid f(x) = e'\}$, appelé noyau de f, est un sous-groupe de G_1*

Preuve :
C'est une conséquence directe du théorème précédent :

1. G_1 est un sous-groupe de lui-même
2. $\{e'\}$ est un sous-groupe trivial de G_2

Théorème 1.3.5 *Soit deux groupes $(G_1, *)$ et $(G_2, *')$ d'éléments neutres respectifs e et e' et f un morphisme de groupe de G_1 vers G_2. On a :*

$$f \text{ est injective} \iff ker(f) = e$$

Preuve :
$\Rightarrow$: Supposons $ker(f) \neq \{e\}$ c'est à dire $\exists x \neq e$ tel que $f(x) = e'$. On a donc $f(x) = f(e) = e'$ et l'injectivité de f donne $x = e$ ce qui contredit l'hypothèse de départ. Donc $ker(f) = e$.
$\Leftarrow$: $\forall x, y \in G_1$, on a $f(x) = f(y) \Rightarrow f(x) *' f(y)^{-1} = e' \Rightarrow f(x * y^{-1}) = e'$. Comme $ker(f) = e$, on a donc $x * y^{-1} = e$ i.e. $x = y$. Donc f injective.