Université de Provence 2009–2010

Mathématiques Générales 1 - Parcours PEI

GROUPES

1 Généralités.

Définition. Soit E un ensemble. On appelle *loi de composition interne* toute application $f : E \times E \to E$. On note souvent, pour $x,y \in E$, $f(x,y) = x * y$ ou $x.y$ ou $x + y$ ou $x \times y$ ou $x \circ y$ ou $x \odot y$ ou $x \oplus y$, ou $x \otimes y$, etc...

Exemples : L'addition sur $\mathbb{N}$ (ou sur $\mathbb{Z}$ ou $\mathbb{Q}$ ou $\mathbb{R}$ ou $\mathbb{C}$) est une loi de composition interne, le produit aussi.

Si $\mathscr{S}_n$ est l'ensemble des permutations de $\{1,\ldots,n\}$, la loi $\circ$ est une loi de composition interne.

Définition. Soit E un ensemble muni d'une loi de composition interne $*$.

On dit que cette loi est *commutative* si et seulement si : $\forall (x,y) \in E^2$, $x * y = y * x$.

On dit que cette loi est *associative* si et seulement si, $\forall (x,y,z) \in E^3$, $(x * y) * z = x * (y * z)$.

On dit que $e \in E$ est un *élément neutre* pour cette loi si et seulement si, $\forall x \in E$, $x * e = e * x = x$.

Exemples : l'addition sur $\mathbb{N}$ (ou sur $\mathbb{Z}$ ou $\mathbb{Q}$ ou $\mathbb{R}$ ou $\mathbb{C}$) est une loi commutative et associative. 0 est l'élément neutre.

La multiplication sur $\mathbb{N}$ (ou sur $\mathbb{Z}$ ou $\mathbb{Q}$ ou $\mathbb{R}$ ou $\mathbb{C}$) est une loi commutative et associative. 1 est l'élément neutre.

La loi $\circ$ sur $\mathscr{S}_n$ est associative, mais pas commutative. L'élément neutre est Id.

Théorème. *Si E muni de la loi de composition interne $*$ possède un élément neutre, celui-ci est unique.*

Preuve. En effet, si e et e' sont deux éléments neutres, $e * e' = e'$ car e est élément neutre, et $e * e' = e'$ car e' est élément neutre. Donc $e = e'$.

Définition. Soit E muni de la loi de composition interne $*$.

Si e est l'élément neutre, si $x \in E$, on dit que x' est *symétrique* de x si et seulement si $x' * x = x * x' = e$.

Exemples. Dans $(\mathbb{N},+)$, aucun de ses éléments ne posséde de symétrique, hormis 0.

Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$, tout élément x possède le symétrique $-x$.

Dans $(\mathbb{N},\times)$ et $(\mathbb{Z},\times)$, aucun de leurs éléments ne possèdent de symétrique hormis 1 pour $\mathbb{N}$ et 1 et -1 pour $\mathbb{Z}$.

Dans $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$, tout élément x hormis 0 possède le symétrique $\dfrac{1}{x}$.

Dans $(\mathscr{S}_n,\circ)$, toute permutation f possède un symétrique : f^{-1}.

Théorème. *Si $(E,*)$ est ensemble muni d'une loi de composition associative et e l'élément neutre et si $x \in E$ possède un symétrique, celui-ci est unique. On le note alors x^{-1}.*

Preuve. En effet, si x' et x'' sont deux symétriques du point x, nous avons $(x' * x) * x'' = e * x'' = x''$ et $(x' * x) * x'' = x' * (x * x'') = x' * e = x'$, donc $x' = x''$.

2 Groupes

Définition. Soit G muni de la loi de composition interne $*$. On dit que $(G,*)$ est un *groupe* si et seulement si $*$ est associative, possède un élément neutre (forcément unique) et tout élément possède un symétrique (lui aussi forcément unique).

Exemples. $(\mathbb{N},+)$ n'est pas un groupe mais $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes.

$(\mathbb{N},\times)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$ ne sont pas des groupes. Par contre, $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes.

$(\mathscr{S}_n,\circ)$ est un groupe.

3 Lois induites. Sous-groupes.

Définition. Soit E muni de la loi de composition interne $*$ et A une partie de E. On dit que A est *stable par* $*$ si et seulement si : $\forall (x,y) \in A^2$, $x * y \in A$.

L'application $A \times A \ni (x,y) \mapsto x * y$ est appelée *loi induite sur A par $*$*

Propriétés. Si la loi est associative, la loi induite aussi.

Si la loi est commutative, la loi induite aussi.

Par contre, si la loi possède un élément neutre, la loi induite peut ne pas en posséder.

De même si $x \in A$ possède un symétrique x' dans E, il ne possède pas forcément de symétrique pour la loi induite.

Définition. Soit $(G,*)$ un groupe. Soit $H \subset G$. On dit que $H \subset G$ est un *sous-groupe* de G si et seulement si H est stable et H muni de la loi induite est un groupe.

Théorème. *Soit $(G,*)$ un groupe et e son élément neutre. Soit H un sous-ensemble non vide de G. Alors H est un sous-groupe si et seulement si :*

- $\forall (x,y) \in H^2$, $x * y \in H$
- $e \in H$
- $\forall x \in H$, $x^{-1} \in H$.

Preuve. Si H vérifie les trois conditions énoncées, il est alors clair que H muni de la loi induite est un groupe car la loi est associative, possède un élément neutre, et tout élément de H possède un symétrique dans H.

Réciproquement, si H est un sous-groupe, alors H est stable, d'où la première assertion : $\forall (x,y) \in H^2$, $x * y \in H$.

Soit e_H l'élément neutre du groupe H muni de la loi induite. Montrons (ce qui n'est pas évident !) que e_H est égal à e, l'élément neutre de G. Comme H est non vide, soit $x \in H$. On a $e_H * x = x$. Or $e_H \in G$ et $x \in G$. Donc le symétrique x^{-1} de x dans G vérifie $(e_H * x) * x^{-1} = x * x^{-1} = e$. D'autre part, nous avons $(e_H * x) * x^{-1} = e_H * (x * x^{-1}) = e_H * e = e_H$. Ceci montre bien que $e_H = e$ et donc que $e \in H$.

Enfin, si $x \in H$, le symétrique x' de x dans H vérifie $x' * x = x * x' = e$. Comme le symétrique x^{-1} de x dans G vérifie aussi $x^{-1} * x = x * x^{-1} = e$ et que celui-ci est unique, on a donc $x' = x$. Ceci prouve que $x^{-1} \in H$.

Corollaire. *Soit $(G,*)$ un groupe et H un sous-ensemble de G non vide. H est un sous-groupe de G si et seulement si :*

$\forall (x,y) \in H^2, \qquad x * y \in H$

$\forall x \in H, \qquad x^{-1} \in H.$

Preuve. Il est clair que si H est un sous-groupe de G, les deux assertions sont vérifiées.

Réciproquement, si ces deux assertions sont vérifiées, pour montrer que H est un sous-groupe, il suffit de vérifier que $e \in H$. Comme H est non vide, soit x un élément de H. x^{-1} est un élément de H. On en déduit que $x * x^{-1} = e$ aussi, ce qui prouve le corollaire.

Corollaire. *Soit $(G,*)$ un groupe et H un sous-ensemble de G non vide. H est un sous-groupe de G si et seulement si :*

$$\forall (x,y) \in H^2, \qquad x * y^{-1} \in H$$

Preuve. Il est clair que si H est un sous-groupe de G, l'assertion est vérifiée.

Réciproquement, si cette assertion est vérifiée, pour montrer que H est un sous-groupe, il suffit de vérifier que $e \in H$, que pour $x \in H$, $x^{-1} \in H$ et que, pour x, y dans H, $x * y \in H$.

Comme H est non vide, soit $x \in H$. On a $e = x * x^{-1} \in H$. Puis, si $x \in H$, $e * x^{-1} = x^{-1} \in H$. Enfin, si x et y sont dans H, on a $x * y = x * (y^{-1})^{-1} \in H$ car x et y^{-1} sont dans H. Ceci termine la preuve.

Théorème. *Soit H un sous-groupe de G. Soit $x \in H$ et $y \in G \setminus H$. Alors $x * y \in G \setminus H$.*

Preuve. En effet, supposons que $x*y \in H$. On en déduit que $x^{-1}*(x*y) \in H$. Or $x^{-1}*(x*y) = (x^{-1}*x)*y = e * y = y$. Donc $y \in H$. C'est absurde.

4 Morphismes.

Définition. Soient $(G,\cdot)$ et $(G',\odot)$ deux groupes. Soit $f : G \to G'$ une application. On dit que f est un *morphisme* de groupes si et seulement si :

$$\forall (x,y) \in G^2, \qquad f(x \cdot y) = f(x) \odot f(y).$$

On dit que f est un *isomorphisme* si de plus f est bijectif.

Théorème. *Soient $(G,\cdot)$ et $(G',\odot)$ deux groupes et f un morphisme de $(G,\cdot)$ dans $(G',\odot)$.*

- *Si e est l'élément neutre de G et e' celui de G' alors $f(e) = e'$.*
- *Si H est un sous-groupe de $(G,\cdot)$, alors $f(H)$ est un sous-groupe de $(G',\odot)$.*
- *Si $x \in G$, le symétrique de $f(x)$ est $f(x^{-1})$.*
- *Si de plus f est un isomorphisme, alors $f^{-1} : G' \to G$ est aussi un isomorphisme.*

Preuve. En effet, si $x \in G$, $f(x) = f(x \cdot e) = f(x) \odot f(e)$. Si y est le symétrique de $f(x)$ dans $(G',\odot)$, on a $e' = y \odot f(x) = y \odot (f(x) \odot f(e)) = (y \odot f(x)) \odot f(e) = f(e)$.

Montrons la deuxième assertion. Tout d'abord $e \in H$, donc $f(e) = e' \in f(H)$.

Ensuite, si $y,y' \in f(H)$, il existe $x,x' \in H$ tels que $f(x) = y$ et $f(x') = y'$. On a alors $y \odot y' = f(x) \odot f(x') = f(x \cdot x') \in H$ car H est stable. Ceci montre que $f(H)$ est stable.

Enfin si $y \in f(H)$ et si $x \in H$ est tel que $f(x) = y$, alors $e' = f(e) = f(x \cdot x^{-1}) = f(x) \odot f(x^{-1})$. Ceci montre que le symétrique de $y = f(x)$ est $f(x^{-1})$ qui est bien dans $f(H)$ car x^{-1} est dans H. Ceci montre aussi la troisème assertion.

Pour la dernière assertion, il suffit de montrer que $g = f^{-1}$ est un morphisme de groupes de $(G',\odot)$ dans $(G,\cdot)$ car la bijection réciproque d'une bijection est encore bijective.

Soit donc y, $y' \in G'$. Notons $x = g(y) \in G$ et $x' = g(y') \in G$. On a alors

$$g(y \odot y') = g(f(x) \odot f(x')) = g(f(x \cdot x')) = x \cdot x' = g(y) \cdot g(y').$$

Ceci prouve bien que g est un morphisme.

Définition. Soient $(G,\cdot)$ et $(G'\odot)$ deux groupes et $f : (G,\cdot) \to (G',\odot)$ un morphisme de groupes. On appelle *noyau de f* et on note $\ker f$ l'ensemble

$$\ker f = \{x \in G \ / \ f(x) = e'\}$$

où e' est l'élément neutre de G'.

Théorème. *Avec les notations précédentes,* $\ker f$ *est un sous groupe de G.*

f est injective si et seulement si $\ker f = \{e\}$ *où e est l'élement neutre de G.*

Preuve. En effet, $\ker f$ est non vide car il contient e.

Il est stable car si x,$y \in \ker f$, on a $f(x \cdot y) = f(x) \odot f(y) = e' \odot e' = e'$ donc $x \cdot y \in \ker f$.

Enfin, si $x \in \ker f$, $x^{-1} \in$ker f aussi car $f(x^{-1}) = f(x)^{-1} = e'^{-1} = e'$.

Tout ceci prouve bien la première assertion.

Pour la seconde assertion, on remarque que si f est injective, $\ker f = \{e\}$.

Si maintenant $\ker f = \{e\}$, montrons que f est injective. Soient donc x,$x' \in G$ tels que $f(x) = f(x')$. On a alors $e' = f(x) \odot [f(x')]^{-1} = f(x) \odot f(x'^{-1}) = f(x \cdot x'^{-1})$, donc $x \cdot x'^{-1} \in \ker f = \{e\}$. On a alors $x \cdot x'^{-1} = e$, soit encore $x = x'$. Ceci prouve bien l'injectivité de f.

5 Anneaux, Corps.

Définition. Soit A un ensemble muni de deux lois de composition interne, $+$ et $\cdot$. On dit que A est un *anneau* si et seulement si (A,+) est un groupe commutatif, $\cdot$ est une loi de composition interne associative et de plus,

$$\forall (x,y,z) \in A^3 \qquad x \cdot (y+z) = x \cdot y + x \cdot z$$

$$\forall (x,y,z) \in A^3 \qquad (y+z) \cdot x = y \cdot x + z \cdot x.$$

On dit alors que la multiplication est *distributive* par rapport à l'addition. On dit aussi que $(A, +, \cdot)$ est un anneau.

Définition. Soit $(K, +, \cdot)$ un anneau. On dit que K est un *corps* si et seulement si $(K^*, \cdot)$ est un groupe, où $K^* = K \setminus \{0\}$ et où 0 est l'élément neutre de la loi $+$.

Exemples. $(\mathbb{N}, +, \times)$ n'est pas un anneau. $(\mathbb{Z}, +, \times,)$, $(\mathbb{Q}, +, \times,)$, $(\mathbb{R}, +, \times,)$ et $(\mathbb{C}, +, \times,)$ sont des anneaux.

$(\mathbb{N}, +, \times)$ et $(\mathbb{Z}, +, \times,)$ ne sont pas des corps. $(\mathbb{Q}, +, \times,)$, $(\mathbb{R}, +, \times,)$ et $(\mathbb{C}, +, \times,)$ sont des corps.