AlloSchool

Mathématiques : 2Bac SMA-SMB

Séance 10-2-1 : Structures algébriques - Partie 2 (Cours)

Professeur : Mr CHEDDADI Haitam

Sommaire

V- Groupe

5-1/ Définition d'un groupe

Définition 1

Soit G un ensemble muni d'une loi de composition interne (notée $*$).

On dit que $(G;*)$ est un groupe lorsque :

1. La loi $*$ est associative,
2. $(G;*)$ possède un élément neutre,
3. Tout élément de G possède un symétrique dans G pour la loi $*$.

Si de plus la loi $*$ est commutative, on dit que $(G;*)$ est un groupe commutatif (ou groupe abélien).

Remarques

Lorsqu'on travaille de manière abstraite dans un groupe non connu, il est fréquent d'emprunter les notations d'un groupe usuel, par exemple $(\mathbb{R};+)$ ou $(\mathbb{R}^*;\times)$.

Deux types de notations seront ainsi fréquemment utilisées : La notation additive et la notation multiplicative.

Loi	Composé de deux éléments	Neutre	Symétrique d'un élément x	Composé de x et d'un symétrique
$+$	$x+y$	0	$-x$	$x-y$
$\times$ ou $\cdot$	xy	1	x^{-1}	xy^{-1}

De la même façon, si $x \in G$ et si $n \in \mathbb{N}^*$, on notera :

- $nx = \underbrace{x+x+x+\ldots.+x}_{n\ fois}$ si la notation est additive.
- $x^n = \underbrace{xxx.\ldots.x}_{n\ fois}$ si la notation est multiplicative.

Par abus de langage et lorsqu'il n'y a aucune ambiguïté, on dit souvent « soit G un groupe ...» sans préciser la loi.

Applications

On considère l'ensemble : $\mathbb{U} = \{z \in \mathbb{C} / |z| = 1\}$

Montrer que $(\mathbb{U}; \times)$ est un groupe commutatif.

5-2/ Principales propriétés d'un groupe

Proposition 1

Soit $(G; *)$ un groupe. Alors :

1- G est non vide : il contient au moins son élément neutre.

2- L'élément neutre e de G est unique.

3- Le symétrique de tout élément de G est unique.

4- Pour tout $(x; y) \in G^2$: $(x')' = x$ et $(x * y)' = y' * x'$. (x' étant le symétrique de x dans $(G; *)$).

5- Tout élément $x \in G$ est régulier. Autrement dit, pour tout $(a; x; y) \in G^3$:

$$(a * x = a * y \Rightarrow x = y) \text{ et } (x * a = y * a \Rightarrow x = y)$$

Proposition 2

Soit $(G; *)$ un groupe d''élément neutre e.

Pour tout $(a; b) \in G^2$, l'équation $a * x = b$ (resp. $x * a = b$) admet une solution unique dans G qui est $x = a' * b$ (resp. $x = b * a'$), où a' désigne le symétrique de a dans $(G; *)$.

En d'autres termes, pour tout $(a; b; x) \in G^3$:

$$(a * x = b \Leftrightarrow x = a' * b) \text{ et } (x * a = b \Leftrightarrow x = b * a')$$

Applications

Soit $(G;*)$ un groupe et a un élément de G.

On considère les applications f et g définies de G dans G par $f(x) = a * x$ et $g(x) = x * a$.

1. Montrer que les applications f et g sont bijectives de G dans G.

Soit $(G;*)$ un groupe tel que : $\left(\forall (x;y;z) \in G^3\right)$ $x * y * z = y * z * x$

2. Montrer que le groupe $(G;*)$ est commutatif.

5-3/ Sous-groupes

Définition 2

Soit $(G;*)$ un groupe et H une partie non vide de G

On dit que H est un sous-groupe de $(G;*)$ lorsque :

- H est stable par la loi $*$, c'est-à-dire : $\left(\forall (x;y) \in H^2\right)$ $x * y \in H$
- $(H;*)$ est un groupe.

5-4/ Propriété caractéristique d'un sous-groupe

Proposition 3

Soit $(G;*)$ un groupe d'élément neutre e, et H une partie de G.

H est un sous-groupe de $(G;*) \Leftrightarrow \begin{cases} H \neq \emptyset \\ \left(\forall (x;y) \in H^2\right) x * y' \in H \end{cases}$

où y' est le symétrique de y dans $(G;*)$.

Remarques

En notation additive, la propriété caractéristique précédente s'écrit :

$$\begin{cases} H \neq \emptyset \\ \left(\forall (x;y) \in H^2\right) x - y \in H \end{cases}$$

En notation multiplicative, la propriété caractéristique précédente s'écrit :

$$\begin{cases} H \neq \emptyset \\ \left(\forall (x;y) \in H^2\right) x.y^{-1} \in H \end{cases}$$

Muni de la loi induite, un sous-groupe est un groupe. C'est la méthode habituelle, car la plus efficace, pour montrer que l'on a affaire à un groupe : on démontre en général que c'est un sous-groupe d'un groupe connu. Cela permet, en particulier, de ne pas à avoir à montrer l'associativité.

5-5/ Morphismes de groupes

Proposition 4

Soit f un morphisme d'un groupe $(G;*)$ dans un groupe $(F;T)$.

Alors : L'image de groupe $(G;*)$ est le groupe $(f(G);T)$.

Remarques

Soit f un morphisme d'un groupe $(G;*)$ dans un groupe $(F;T)$. On dit aussi :

- f est un isomorphisme de groupes si f est bijectif.
- f est un endomorphisme de groupe $(G;*)$ si f est défini de $(G;*)$ dans $(G;*)$.
- f est un automorphisme de groupe $(G;*)$ si f est un endomorphisme bijectif.

Si le morphisme f est surjectif ou un isomorphisme de groupes alors $f(G) = F$, et dans ce cas, l'image du groupe $(G;*)$ par f est le groupe $(F;T)$. On dit alors que le morphisme f transfère « la structure du groupe $(G;*)$ » en celle du groupe $(F;T)$.

Si f est un isomorphisme de $(G;*)$ dans $(F;T)$, alors $(G;*)$ et $(F;T)$ ont la même structure. En particulier :

- Si $(G;*)$ est un groupe, alors $(F;T)$ est un groupe.
- Si $(G;*)$ est un groupe commutatif, alors $(F;T)$ est un groupe commutatif.

Ce résultat est très utile en pratique.

VI- Anneau

6-1/ Distributivité

Définition 3

Soit E un ensemble muni de deux lois de composition interne $\oplus$ et $\otimes$.

On dit que la loi $\otimes$ est distributive par rapport à la loi $\oplus$ si pour tous x, y et z de E, on a :

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \text{ et } (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$$

6-2/ Structure d'anneau

Définition 4

Soit A un ensemble muni de deux lois de composition interne $\oplus$ et $\otimes$.

On dit que $(A;\oplus;\otimes)$ est un anneau lorsque :

1. $(A;\oplus)$ est un groupe commutatif.
2. La loi $\otimes$ est associative et distributive par rapport à la loi $\oplus$

On dit que l'anneau $(A;\oplus;\otimes)$ est commutatif si la loi $\otimes$ est commutative.

On dit que l'anneau $(A;\oplus;\otimes)$ est unitaire si la loi $\otimes$ possède un élément neutre pour la loi $\otimes$.

6-3/ Règles de calcul dans un anneau

Proposition 5

Soit $(A;+;\bullet)$ un anneau unitaire. On a les propriétés suivantes :

1- Pour tout $x \in A$: $0_A \bullet x = x \bullet 0_A = 0_A$

2- Pour tout $x \in A$: $(-1_A) \bullet x = x \bullet (-1_A) = -x$

3- Pour tout $(x;y) \in A^2$: $(-x) \bullet y = x \bullet (-y) = -(x \bullet y)$

4- Pour tout $(x;y) \in A^2$: $(-x) \bullet (-y) = x \bullet y$

Remarques

1- En appliquant les règles de calcul citées dans la proposition 5 dans l'anneau $(\mathbb{R};+;\times)$, on obtient :

$$0 \times x = x \times 0 = x$$
$$(-1) \times x = x \times (-1) = -x$$
$$x \times (-y) = (-x) \times y = -(x \times y)$$
$$(-x) \times (-y) = x \times y$$

2- Attention, il ne faut pas déduire trop hâtivement de la première propriété qu'un produit n'est nul que lorsqu'un des deux éléments multipliés est nul.

Par exemple, dans l'anneau $(\mathbb{M}_2(\mathbb{R}); +; \times)$: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ malgré que les deux matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ ne sont pas nulles

3- Il peut arriver que l'on rencontre, dans la littérature, une autre définition de la notion d'anneau dans laquelle on suppose la seconde loi admit un élément neutre. D'ailleurs, tous les anneaux envisagés dans ce cours seront unitaires. Les anneaux non unitaires n'ont pas en général d'intérêt pratique car on peut toujours injecter un anneau non unitaire dans un anneau unitaire.

6-4/ Diviseurs de zéro dans un anneau - Anneau intègre

Définition 5

Soit $(A; +; \bullet)$ un anneau et $a \in A - \{0_A\}$.

On dit que a est un diviseur de zéro dans l'anneau A s'il existe $b \in A - \{0_A\}$ tel que :

$$a \bullet b = 0_A \text{ ou } b \bullet a = 0_A$$

Définition 6

On dit qu'un anneau $(A; +; \bullet)$ est intègre s'il n'est pas réduit à zéro et n'admet aucun diviseur de zéro.

Autrement dit : $[(A; +; \bullet)$ est intègre$] \Leftrightarrow \left[\left(\forall (a; b) \in A^2\right) ab = 0_A \Rightarrow (a = 0_A \; ou \; b = 0_A)\right]$

Proposition 6

Soit $(A; +; \bullet)$ un anneau unitaire et $a \in A$.

Si a est inversible dans $(A; \bullet)$, alors a n'est pas un diviseur de zéro dans l'anneau $(A; +; \bullet)$.

Remarques

Soit $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice de $(\mathbb{M}_2(\mathbb{R}); +; \times)$.

On rappelle que : $detM = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc$

La matrice M est inversible dans $(\mathbb{M}_2(\mathbb{R}); +; \times)$ si, et seulement si, son déterminant est non nul.

Si $detM \neq 0$, alors la matrice inverse de M est donnée par la formule :

$$M^{-1} = \frac{1}{detM} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

VII- Corps

Définition 7

On appelle corps tout anneau unitaire $(K;+;\bullet)$ non réduit à $\{0_K\}$ tel que tout élément autre que 0_K est inversible pour la loi $\bullet$.

Un corps est dit commutatif si sa multiplication $\bullet$ est commutative.

Remarques

1- Il peut arriver que l'on rencontre, dans la littérature, une autre définition de la notion de corps dans laquelle on suppose la commutativité de la multiplication $\bullet$.

D'ailleurs, tous les corps envisagés dans ce cours seront commutatifs. Les corps non commutatifs n'ont pas en général d'intérêt pratique.

2- D'après la proposition 6, l'intégrité est une condition nécessaire, mais insuffisant, pour qu'un anneau soit un corps. Ainsi, $(\mathbb{Z}/6\mathbb{Z};+;\times)$ n'est pas un corps car il n'est pas un anneau intègre.

Proposition 7

Soit $(K;+;\bullet)$ un ensemble muni de deux lois de composition interne $+$ et $\bullet$.

Pour que $(K;+;\bullet)$ soit un corps, il faut et il suffit que les trois axiomes suivants soient vérifiés :

1. $(K;+)$ est un groupe commutatif.
2. $(K-\{0_K\};\bullet)$ est un groupe.
3. La loi $\bullet$ est distributive par rapport à la loi $+$.

Proposition 8

Soit $(K;+;\bullet)$ un corps. On a alors les propriétés suivantes :

1- Tout élément a de $K-\{0_K\}$ est régulier pour l'opération $\bullet$:

$$\text{Pour tout } (x;y)\in K^2 : a\bullet x = a\bullet y \Rightarrow x=y \text{ et } x\bullet a = y\bullet a \Rightarrow x=y$$

2- $(K;+;\bullet)$ est un anneau intègre :

$$\left(\forall\,(x;y)\in K^2\right)\ [x\bullet y = 0_K \Rightarrow (x=0_K \text{ } ou \text{ } y=0_K)]$$

3- Pour tous $a\in K-\{0_K\}$ et $b\in K$, on a :

$$a\bullet x = b \Leftrightarrow x = a^{-1}\bullet b \text{ et } \ x\bullet a = b \Leftrightarrow x = b\bullet a^{-1}$$

Remarque

Soit $(A;\oplus;\otimes)$ un anneau unitaire d'élément unité 1_A, et soit K une partie de A stable pour les lois $\oplus$ et $\otimes$ dans A.

On peut avoir $(K;\oplus;\otimes)$ un corps commutatif d'élément unité 1_K différent de 1_A.

À titre d'exemple, considérons : $A=\mathbb{M}_2(\mathbb{R})$ et $K=\left\{\begin{pmatrix} x & x \\ x & x\end{pmatrix}/x\in\mathbb{R}\right\}$

$(K;+;\times)$ est un corps commutatif. Son zéro est $O_2=\begin{pmatrix} 0 & 0 \\ 0 & 0\end{pmatrix}$ et son élément unité est $J=\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}\end{pmatrix}$.

Par contre, l'élément unité de $(A;+;\times)$ est la matrice identité $I_2=\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$.

L'inverse de $M = \begin{pmatrix} x & x \\ x & x \end{pmatrix} / x \neq 0$ est la matrice $M^{-1} = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = \frac{1}{4x} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.