Ecole
Internationale
des Sciences
du Traitement
de l'Information

Algèbre et Géométrie

CHAPITRE 5

Groupes

et

Anneaux

Sommaire

1. Lois de composition interne

1.1. Définitions

Une *loi de composition interne* sur un ensemble E, ou *opération* de E dans E, est une application de $E \times E$ dans E.

Exemple : Soit $E=\mathbb{R}$ alors l'application définie par

$$\forall p \in E,\ \forall q \in E,\ p\#q = p+q-E[p+q].$$

est une loi de composition interne à E

Soit (E,.) un ensemble muni d'une opération « . ». Cette opération est :

- *associative* si : $\forall x \in E,\ \forall y \in E,\ \forall z \in E,\ x.(y.z)=(x.y).z$
- *commutative* si : $\forall x \in E,\ \forall y \in E,\ x.y=y.x$

Une partie A de (E,.) est dite *stable* par « . » si $\forall x \in A,\ \forall y \in A,\ x.y \in A$.

Exemple (suite)
L'application # est associative et commutative. Le sous-ensemble A=[0,1[est stable par #.

1.2. Eléments particuliers

Un élément e de (E,.) est dit

- *neutre à droite* si : $\forall x \in E,\ x.e=x$,
- *neutre à gauche* si : $\forall x \in E,\ e.x=x$,
- *neutre* s'il est neutre à droite et neutre à gauche.

Propriété 1
Si e_1 et e_2 sont deux éléments neutres de (E,.), alors $e_1=e_2$.

Exemple (suite)
Considérons maintenant que E=A. Alors 0 est l'élément neutre de(E,#).

On suppose que (E,.) admet un élément neutre e. On dit que x' de E est :

- un *symétrique à droite* de $x \in E$ lorsque $x.x'=e$
- un *symétrique à gauche* de $x \in E$ lorsque $x'.x=e$
- un *symétrique* de $x \in E$ s'il est symétrique à droite et symétrique à gauche.

Si x de E admet un symétrique, on dit que x est *inversible*, et on note x^{-1} le symétrique de x.

Propriété 2
Soit (E,.) un ensemble muni de l'opération « . » associative et admettant un élément neutre. Si x_1 et x_2 sont des symétriques de x, alors $x_1=x_2$.

Propriété 3
Soit (E,.) un ensemble muni de l'opération « . » associative et admettant un élément neutre. L'ensemble U des éléments inversibles est une partie stable de E par « . ». Si a et b sont deux éléments de U, on a $(a.b)^{-1}=b^{-1}.a^{-1}$.

Exemple (suite)
On considère toujours que E=A. Alors tout élément p de E\{0} admet 1–p comme symétrique par # et 0 est son propre symétrique.

Soient (E,.) et a un élément de A. On dit que a est :
- *régulier à droite* si $\forall(x,y)\in E^2$, $x.a=y.a \Rightarrow x=y$
- *régulier à gauche* si $\forall(x,y)\in E^2$, $a.x=a.y \Rightarrow x=y$
- *régulier* s'il est régulier à droite et régulier à gauche

1.3. Distributivité

Soit E un ensemble muni de deux opérations « T » et « * ». On dite que * est :
- *distributive à droite* par rapport à « T » si $\forall(x,y,z)\in E^3$
$$(xTy)*z=(x*z)T(y*z),$$
- *distributive à gauche* par rapport à « T » si $\forall(x,y,z)\in E^3$
$$z*(xTy)=(z*x)T(z*y),$$
- *distributive* si elle est distributive à droite et distributive à gauche.

Exemple (suite)
L'opération # n'est pas distributive par rapport à l'addition ou la multiplication.

2. Groupes et morphismes de groupe

2.1. Groupes

Soit G un ensemble non vide muni d'une loi de composition interne notée . On dit que (G,*) est *un groupe* si l'opération *

i) est associative : $\forall x\in G, \forall y\in G, \forall z\in G, x*(y*z)=(x*y)*z$
ii) admet un élément neutre e : $\forall x\in G, x*e=e*x=x$
iii) tout élément de G admet un symétrique : $\forall x\in G, \exists x'\in G, x*x'=x'*x=e$.

Un groupe est dit *commutatif ou abélien*, si l'opération interne * est commutative,

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

Propriété 4
Dans un groupe (G,*), d'élément neutre e, tout élément est régulier, c'est-à-dire

$$\forall x\in G,\ \forall y\in G,\ \forall z\in G,\ x*z=y*z \Rightarrow x=y \text{ et } z*x=z*y \Rightarrow x=y.$$

Exemple
$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^*,.)$, $(\mathbb{R}^*,.)$, $(\mathbb{C}^*,.)$ sont des groupes commutatifs.
En revanche, $(\mathbb{N},+)$ et $(\mathbb{R},.)$ ne sont pas des groupes.
Soit $\mathcal{V}$ l'ensemble des vecteurs du plan, $(\mathcal{V},+)$ est un groupe commutatif.

2.2. Sous-groupes

Soit (G,*) un groupe d'élément neutre e. Une partie H de G est *un sous-groupe* de (G,*) si

i) H est stable par l'opération * : $\forall x\in H,\ \forall y\in H,\ x*y\in H$,
ii) l'élément neutre appartient à H : $e\in H$,
iii) H est stable par passage au symétrique : $\forall x\in H,\ x^{-1}\in H$,

ou x^{-1} est le symétrique (encore appelé inverse) de x.

Propriété 5
Si (G,*) est un groupe d'élément neutre e, tout sous-groupe de G contient e.

Exemple : Centre d'un groupe (G,*)
L'ensemble $C=\{c\in G,\ \forall x\in G,\ c*x=x*c\}$ est un sous-groupe de G, appelé le centre du groupe G.

Cas particuliers
Soit (G,*) un groupe, les sous-ensembles {e} et G sont des sous-groupes de G.Tout sous-groupe H de (G,*) autre que {e} et G est appelé *sous-groupe propre* de G.

Propriété 6
Soit (G,*) un groupe et H un de ses sous-groupes. Pour la restriction de la loi * à H, encore notée *, (H,*) est un groupe.

Propriété 7
Soit (G,*) un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de (G,*). Alors l'intersection des H_i est un sous-groupe de (G,*).

2.3. Morphismes de groupes

Soient $(G_1,*)$ et $(G_2,\#)$ des groupes et f une application de G_1 dans G_2. On dit que f est un *morphisme* (ou *homomorphisme*) de $(G_1,*)$ dans $(G_2,\#)$ si

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

- Un *isomorphisme* est un morphisme bijectif.
- Un *endomorphisme* est un morphisme d'un groupe sur lui-même.
- Un *automorphisme* est un endomorphisme bijectif.

Notation

- $Hom(G_1,G_2)$ est l'ensemble des homorphismes d'un groupe $(G_1,*)$ dans un groupe $(G_2,\#)$.
- $G_1\cong G_2$ s'il existe un isomorphisme de $(G_1,*)$ dans un groupe $(G_2,\#)$.
- End(G) est l'ensemble des endomorphisme de (G,*).
- Aut(G) est l'ensemble des automorphismes de (G,*).

Propriété 8

Soient $(G_1,*)$ et $(G_2,\#)$ des groupes d'éléments neutres respectifs e_1 et e_2. Soit f un morphisme de $(G_1,*)$ dans $(G_2,\#)$.

i) $f(e_1)=e_2$

ii) $\forall x\in G_1,\ f(x^{-1})=(f(x))^{-1}$

Propriété 9

Soient $(G_1,*)$ et $(G_2,\#)$ des groupes et soit f un morphisme de $(G_1,*)$ dans $(G_2,\#)$.

- Si H_1 est un sous-groupe de $(G_1,*)$, alors $f(H_1)$ est un sous-groupe de $(G_2,\#)$.
- Si H_2 est un sous-groupe de $(G_2,\#)$, alors $f^{-1}(H_2)$ est un sous-groupe de $(G_1,*)$.

Propriété 10

Soient $(G_1,*)$, $(G_2,\#)$ et $(G_3,.)$ des groupes. Si $f\in Hom(G_1,G_2)$ et $g\in Hom(G_2,G_3)$, alors $gof\in Hom(G_1,G_3)$

Exercice : Montrer que $(S(E),o)$ est un groupe, où S(E) est l'ensemble des bijections d'un ensemble E dans lui-même (encore appelé ensemble des permutations).

Propriété 11

Soit (G,*) un groupe et soit f un automorphisme de G. Alors f^{-1} est un automorphisme de G.

2.4. Noyau et image

Soient $(G_1,*)$ et $(G_2,\#)$ des groupes d'éléments neutres respectifs e_1 et e_2. Soit f un morphisme de $(G_1,*)$ dans $(G_2,\#)$.

On appelle *image* du morphisme f, l'ensemble $f(G_1)$ de G_2, noté Im f,

$$Imf=\{y\in G_2,\ \exists x\in G_1,\ y=f(x)\}.$$

On appelle *noyau* du morphisme f, l'ensemble $f^{-1}(\{e_2\})$ de G_1, noté Ker f,

$$Kerf=\{x\in G_1,\ f(x)=e_2\}.$$

Propriété 12

Kerf est un sous-groupe de $(G_1,*)$ et Imf est un sous-groupe de $(G_2,\#)$.

Propriété 13

- f est injectif si et seulement si Ker f = $\{e_1\}$.
- f est surjective si et seulement si Im f = G_2.

3. Anneaux

3.1. Définitions et règles de calcul

Un *anneau* est un triplet (A,+, .) constitué de

1) un ensemble non vide A,
2) une loi de composition interne, appelée addition de A, telle que (A,+) est un groupe abélien,
3) une loi de composition interne, appelée multiplication de A, telle que la multiplication
   - soit associative
   - admette un élément neutre
   - soit distributive par rapport à l'addition

Un anneau (A,+, .) est dit *commutatif* si sa multiplication est commutative.

Exemple : $(\mathbb{Z},+,.)$ est un anneau commutatif

Si A={a}, alors il n'y a qu'une loi de composition interne définie par a*a=a. Il existe donc un seul anneau ayant un seul élément, appelé *l'anneau nul.*

Notations

- L'élément neutre de l'addition est noté 0_A.
- L'élément neutre de la multiplication est appelé élément unité et est noté 1_A.
- Le symétrique de $a\in A$ pour l'addition est appelé opposé de a et est noté –a.

- Le symétrique de $a \in A$ pour la multiplication, s'il existe, est appelé inverse de a et est noté a^{-1}.

Un anneau commutatif dont tous les éléments sont inversibles sauf l'élément neutre pour l'addition est appelé *un corps.*

Exemples : Les corps les plus communément utilisés sont $\mathbb{R}$ et $\mathbb{C}$.

Opérations externes

Etant donné $a \in A$ et $n \in \mathbb{Z}$, on définit l'élément $na \in A$ par :

- $1a=a$ et $0a=0_A$,
- pour $n>1$, na est la somme de n termes égaux à a,
- pour $n<0$, $na=(-n)(-a)$, est la somme de $-n$ termes égaux à l'opposé de a.

Etant donné $a \in A$ et $n \in \mathbb{N}$, on définit l'élément a^n par :

- $a^0=1_A$, $a^1=a$,
- pour $n>1$, $a^n=a.a^{n-1}=a^{n-1}.a$

Propriété 14 : Règles de calcul

- Pour tout $a \in A$, $0_A.a=a.0_A=0_A$.
- Si Card $A>1$, on a $0_A \neq 1_A$.
- $\forall a \in A, \forall b \in A$, $(-a).b=a.(-b)=-(a.b)$
- $\forall a \in A, \forall b \in A$, $(-1_A).a=-a$ et $(-a).(-b)=a.b$
- $\forall a \in A, \forall b \in A, \forall c \in A$, $a.(b-c)=a.b-a.c$ et $(b-c).a=b.a-c.a$
- $\forall a \in A, \forall b \in A$ et $\forall n \in \mathbb{Z}$, $(na).b=a.(nb)=n(a.b)$

Propriété 15

Si a et b sont des éléments de A qui commutent, on a

pour tout $n \in \mathbb{N}$, $(a+b)^n = \sum_{k=0}^{n} C_n^k a^k . b^{n-k}$ (formule du binôme)

pour tout $n \in \mathbb{N}^*$, $a^n - b^n = (a-b).\sum_{k=0}^{n-1} a^{n-1-k}.b^k$

3.2. Anneaux intègres

Soit $(A,+,.)$ un anneau non nul et $a \in A \setminus \{0_A\}$. On dit que a est

- *diviseur de 0_A à droite* s'il existe $x \neq 0_A$ tel que $x.a=0_A$,
- *diviseur de 0_A à gauche* s'il existe $y \neq 0_A$ tel que $a.y=0_A$,
- *diviseur de 0_A* s'il est diviseur à droite et diviseur à gauche.

Propriété 16

Si un anneau $(A,+,.)$ n'admet pas de diviseur de 0_A alors

$$\forall a \in A, \forall b \in A, a.b=0_A \Rightarrow a=0_A \text{ ou } b=0_A.$$

Un anneau (A,+, .) est *intègre* s'il est commutatif et sans diviseur de 0_A.

Un élément non nul $a \in A$ est *nilpotent* s'il existe un entier non nul n tel que $a^n=0_A$.

Exemple : $(\mathbb{Z},+, .)$ est un anneau intègre.

3.3. Sous-anneaux et anneaux produit

Soit (A,+, .) un anneau.

Une partie non vide B de A est un *sous-anneau* de (A,+, .) si

i) $1_A \in B$
ii) B est un sous-groupe de (A,+)
iii) B est stable par la multiplication de A

Exemple : Produit d'anneaux
Soient (A,+, .) et (B,#,*) deux anneaux. On munit $A \times B$ des lois de composition internes,
$\forall (a,b) \in A \times B, \ \forall (a',b') \in A \times B$

$$(a,b)\Theta(a',b')=(a+a',b\#b')$$
$$(a,b)\times(a',b')=(a.a',b*b')$$

Alors $(A \times B, \Theta, \times)$ est un anneau appelé *l'anneau produit* de (A,+, .) et (B,#,*).

3.4. Morphismes d'anneaux

Soient $(A_1,+,\times)$ et $(A_2,\#,*)$ deux anneaux, et f une application de A_1 dans A_2. On dit que f est un *homomorphisme* (ou *morphisme*) d'anneaux si

i) $\forall x \in A_1, \ \forall y \in A_1, \ f(x+y)=f(x)\#f(y)$
ii) $\forall x \in A_1, \ \forall y \in A_1, \ f(x \times y)=f(x)*f(y)$
iii) $f(1_{A_1}) = 1_{A_2}$

- Un *isomorphisme* est un morphisme bijectif.
- Un *endomorphisme* est un morphisme d'un groupe sur lui-même.
- Un *automorphisme* est un endomorphisme bijectif.

Exemple :
Soient (A,+, .) et (B,#,*) deux anneaux. Alors l'application f de $A \times B$ dans A définie par f : $(a,b) \mapsto a$ est un morphisme d'anneaux. Cette application est appelée l'injection canonique de $A \times B$ dans A.