STRUCTURES ALGEBRIQUES

1) Loi de composition

On considère un ensemble non vide E.

loi de composition interne

* est appelée loi de composition interne sur E si : $\forall (a,b) \in E \times E, \exists ! c \in E, a*b = c$. On dit alors que (E,*) est un **magma**.

Remarque :
On peut étendre la définition une loi de composition interne à plusieurs éléments :
$\forall n \geq 3, \forall (a_1,...,a_n) \in E^n, a_1*...*a_n = (a_1*...*a_{n-1})*a_n$, ou bien :
$\forall n \geq 3, \forall (a_1,...,a_n) \in E^n, a_1*...*a_n = a_1*(a_2*...*a_n)$, ce qui ne donne pas les mêmes résultats.

loi de composition externe

T est appelée loi de composition externe sur *E* muni de l'ensemble d'opérateurs Ω si :
$\forall (\alpha, a) \in \Omega \times E, \exists ! b \in E, \alpha T a = b$.

loi associative

Soit (E,*) un magma. On dit que * est associative si : $\forall (a,b,c) \in E^3, a*(b*c) = (a*b)*c$. On dit alors que (e,*) est un **magma associatif**.

élément neutre

Soit (E,*) un magma.
On dit que *e* est **élément neutre à gauche** de (E,*) (resp. à **droite**) si : $\forall a \in E, e*a = a$ (resp. $\forall a \in E, a*e = a$)
On dit que *e* est **élément neutre** de (E,*) s'il est élément neutre à gauche et à droite.

Remarque :
Un élément neutre d'un magma, s'il existe est unique. En effet :
Supposons qu'il existe un élément neutre e_1 de (E,*). Soit e_2 un élément neutre de (E,*).
On a $e_1*e_2 = e_2*e_1 = e_2$ (car e_1 est élément neutre). On a aussi $e_1*e_2 = e_2*e_1 = e_1$ (car e_2 est élément neutre). Il en résulte que $e_1 = e_2$.

inverse d'un élément :

Soit (E,*) un magma possédant un élément neutre *e*. Soit *a* un élément de E. On dit qu'un élément *b* de E est un élément inverse de *a* à gauche (resp. à droite) si $b*a = e$ (resp. $a*b = e$). On dit que *b* est un inverse de *a* s'il est à la fois un inverse à droite et à gauche de *a*.

Remarque :
Si la loi * est associative, l'inverse d'un élément, s'il existe, est unique. En effet :

Considérons un magma (E,*) associatif possédant un élément neutre *e*. Soit *a* un élément de E. On suppose qu'il existe un inverse de *a*, noté *b*. Soit *c* un inverse de *a*. On a $a*b=b*a=e$ (car *b* est un inverse de *a*). Alors $c*(a*b)=c*e$. La loi * étant associative, $c*(a*b)=(c*a)*b=e*b=b$ (car $c*a=e$, *c* étant un inverse de *a*). Comme $c*e=c$, il en résulte que $b=c$.

2) Groupes et sous-groupes

groupe

Soit (G,*) un magma. On dit que G est un **groupe** si :

- * est associative
- * possède un élément neutre
- tout élément de G possède un inverse

Si * est commutative, on dit que G est un groupe commutatif ou abélien.

Exemples : $(R,+)$ est un groupe. $(R,\times)$ n'est pas un groupe puisque 0 n'a pas d'inverse pour l'opération $\times$. En revanche, $(R^*,\times)$ est un groupe.

ordre d'un groupe

Si G possède un nombre fini d'éléments, on dit que G est un **groupe fini** et on appelle **ordre** de G le nombre d'éléments de G, noté ord(G).

sous-groupe

Soit (G,*) un groupe. On dit qu'une partie H non vide de G est un **sous-groupe** de G si :

- $HH\subset H$ (c'est-à-dire $\forall(a,b)\in H\times H, a*b\in H$)
- $H^{-1}\subset H$ (c'est-à-dire $\forall a\in H, a^{-1}\in H$)

caractérisation de sous-groupes

Soit (G,*) un groupe. $H\subset G$ est un sous-groupe de (G,*) si et seulement si $H\neq\emptyset$ et $HH^{-1}\subset H$ (c'est-à-dire $\forall(a,b)\in H\times H, a*b^{-1}\in H$).

démonstration :

- Supposons que $H\subset G$ soit un sous-groupe de (G,*). D'après la définition d'un sous-groupe, $H\neq\emptyset$. Soient *a* et *b* deux éléments de H. $H^{-1}\subset H$ donc $b^{-1}\in H$. $HH\subset H$ donc $a*b^{-1}\in H$
- Supposons maintenant que $H\neq\emptyset$ et $HH^{-1}\subset H$. Soient *a* et *b* deux éléments de *H*. $a*a^{-1}\in H$, c'est-à-dire $e\in H$. Donc pour tout $x\in H$, $e*x^{-1}\in H$, c'est-à-dire $x^{-1}\in H$. Donc $a*(b^{-1})^{-1}\in H$ donc $a*b\in H$. Par conséquent, on a bien $HH\subset H$ et $H^{-1}\subset H$.

3) Anneaux et corps

On considère un ensemble A non vide.

distributivité d'une loi sur une autre

Soient * et $\otimes$ deux lois définies sur A. On dit que * est **distributive à gauche** (resp. à droite) par rapport à $\otimes$ dans $(E,\otimes,*)$ si : $\forall (a,b,c)\in E^3, a*(b\otimes c)=a*b\otimes a*c$ (resp. $\forall (a,b,c)\in E^3, (a\otimes b)*c=a*c\otimes b*c$. On dit que * est **distributive** par rapport à $\otimes$ si elle est distributive à gauche et à droite par rapport à $\otimes$.

Remarque : si * est commutative, la distributivité à gauche équivaut à la distributivité à droite.

anneau

On dit que $(A,+,.)$, où + et **.** sont deux lois de composition internes sur A, est un **anneau** si :

- $(A,+)$ est un groupe abélien
- **.** est une loi associative
- **.** est distributive sur +

L'élément neutre pour + est appelé **élément nul**. Si de plus **.** possède un élément neutre, on dit que A est un **anneau unitaire** (cet élément neutre pour **.** est alors appelé **élément unité** de l'anneau A). Si **.** est commutative, on dit que A est un **anneau commutatif**. Si 0 n'a pas de diviseurs, on dit que A est un **anneau intègre** (on alors la propriété suivante : $a.b=0\Rightarrow (a=0)\vee (b=0)$)

Exemple : $(R,+,\times)$ est un anneau commutatif unitaire. R est intègre. Les propriétés énoncées pour R sont aussi valables pour Q,C,Z.

corps

On dit que K est un **corps** si $(K,+,.)$ est un anneau dont tout élément non nul est inversible, c'est-à-dire si :

- $(K,+,.)$ est un anneau
- $(K-\{0\},.)$ est un groupe

Si **.** est commutative, on dit que K est un **corps commutatif**.

Exemple : $(R,+,.)$ est un corps.

Remarque : L'inverse d'un élément a de K (pour **.**) est souvent noté a^{-1}. L'opposé de a (pour +) est souvent noté $-a$.

4) Modules et espaces vectoriels

module

Soit $(E,+)$ un groupe abélien. Soit $(A,+,\times)$ un anneau unitaire. On considère une loi de composition interne sur E notée **.** et dont l'ensemble d'opérateur est A. On dit que $(E;+,A;\times)$ est un

module sur l'anneau *A* (ou un *A*-module) si les propriétés suivantes sont vérifiées pour tous $a,b \in E$ et $\alpha,\beta \in A$:

(1) $\alpha .(a+ b) = \alpha . a + \alpha . b$
(2) $(\alpha + \beta) . a = \alpha . a + \beta . b$
(3) $(\alpha \times \beta) . b = \alpha . (\beta . b)$
(4) $1.a = a$

espace vectoriel

Soit *K* un corps (non nécessairement commutatif). Un *K*-module est appelé **espace vectoriel**. Si $(E;+,K,.)$ est un module, on dit aussi que *E* est un **espace vectoriel sur le corps *K***.

sous espace vectoriel

Soit E un espace vectoriel sur le corps K. Soit F une partie non vide de E. On dit que F est un **sous espace vectoriel de E** si F est stable pour les lois + et **.** , c'est-à-dire :

(i) $\forall (x, y) \in F,\ x + y \in F$
(ii) $\forall (\alpha, x) \in K \times F,\ \alpha.x \in F$