Structures algébriques usuelles

MP Lycée Clemenceau

Table des matières

I Les groupes

1) Rappels et compléments

a) Définitions

Rappel : si E est un ensemble non vide, une loi de composition interne (souvent notée l.c.i.) est une application de $E \times E$ dans E.

Définition I - 1 : Groupe

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

a) l'associativité : $\forall (x,y,z) \in G^3$, $x*(y*z) = (x*y)*z = x*y*z$

b) il existe un élément neutre $e \in G$: $\forall x \in G \quad x*e = e*x = x$
On a alors (avec ces deux premières conditions) un monoïde.

c) tout élément est symétrisable (admet un symétrique unique) :

$$\forall x \in G,\ \exists y \in G \,/\, x*y = y*x = e$$

On note $y = x^{-1}$ ou $-x$.

Alors $(G,*)$ est appelé **groupe .**

Définition I - 2 : Groupe abélien

Si la loi est **commutative**, c'est-à-dire si

$$\forall (x,y) \in G^2 \quad x*y = y*x$$

on parle de groupe **abélien** ou commutatif.

Définition I - 3 : ordre d'un groupe

Si G est de **cardinal fini**, alors on parle de **groupe fini** et le cardinal de G est appelé **ordre du groupe.**

Propriété I - 1 : Groupe des permutations

Soit X un ensemble non vide. L'ensemble des permutations de X muni de la composition est un groupe. On le note S_X.

Définition I - 4 : Groupe produit

Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes d'éléments neutres respectifs e_1 et e_2.
On définit sur l'ensemble $G_1 \times G_2$ la loi de composition interne suivante :

$$\forall ((x_1,y_1),(x_2,y_2)) \in (G_1 \times G_2)^2 \quad (x_1,y_1)*(x_2,y_2) = (x_1 *_1 x_2, y_1 *_2 y_2)$$

$G_1 \times G_2$ munis de cette l.c.i. est alors un groupe appelé groupe produit des deux groupes G_1 et G_2.

Définition I - 5 : Sous groupes

Soit $(G,*)$ un groupe, soit H un sous ensemble **non vide** de G, **stable** par la l.c.i., alors si $(H,*)$ est un groupe, on dit que c'est un **sous groupe** de $(G,*)$.

b) Propriétés

Proposition I - 1 : Caractérisation des sous groupes

Soit $(G,.)$ un groupe, d'élément neutre e . On considère $H \subset G$, alors les propositions suivantes sont équivalentes :

1) H est un sous groupe de G
2) H est stable par la l.c.i., $e \in H$ et $(x \in H \Rightarrow x^{-1} \in H)$
3) H est stable, $H \neq \emptyset$ et $(x \in H \Rightarrow x^{-1} \in H)$
4) $H \neq \emptyset$, $\forall (x,y) \in H^2$, $x.y^{-1} \in H$

Proposition I - 2 : Intersection de sous-groupes

L'intersection quelconque (non vide) de sous-groupes d'un groupe G est un sous-groupe de G.

Définition I - 6 : Sous groupe engendré par une partie

Etant donner une partie A non vide d'un groupe G, l'intersection H des sous groupes de G contenant A est le plus petit (au sens de l'inclusion) sous-groupe de G contenant A.
Si A est l'ensemble vide alors $H = \{e\}$, sinon c'est l'ensemble des produits (finis) d'éléments de A et de symétriques d'éléments de A.
H est appelé sous groupe de G engendré par A. On le note usuellement $Gr(A)$.

Proposition I - 3 : Sous-groupes de $\mathbb{Z}$

Les sous-groupes de $\mathbb{Z}$ sont les sous-groupes engendrés par un élément $n \in \mathbb{N}$, noté $n\mathbb{Z}$.

2) Morphisme de groupe

a) Définitions

Définition I - 7 : Morphisme de groupes

Soient $(G,.)$ et $(H,\star)$ deux groupes, et soit f une application de G vers H.
f est appelée **morphisme** de groupes si elle vérifie :

$$\boxed{\forall (x,y) \in G^2, \quad f(x.y) = f(x) \star f(y)}$$

Définition I - 8 : Isomorphisme

Un morphisme bijectif est appelé **isomorphisme**.

Définition I - 9 : Endomorphisme

Un morphisme de $(G,.)$ dans lui même est appelé **endomorphisme**.
L'ensemble des endomorphismes d'un groupe G est noté : $End(G)$.

Définition I - 10 : Automorphisme
Un endomorphisme bijectif est un **automorphisme**.
L'ensemble des automorphismes de G est noté $Aut(G)$.

b) Propriétés

Proposition I - 4 :
Soit $f : (G, .) \to (G', *)$ un morphisme de groupe, soient e et e' les éléments neutres respectifs de G et G', alors on a :

$$f(e) = e' \quad \text{et} \quad f\left(x^{-1}\right) = (f(x))^{-1}$$

Proposition I - 5 :
Soit $f : (G, .) \to (G', *)$ un morphisme de groupe,
- soit H un sous groupe de G, alors $f(H)$ est un sous groupe de G'.
- soit H' un sous groupe de G', alors $f^{-1}(H')$ est un sous groupe de G

c) Noyau et image

Définition I - 11 : Image
Soit $f : (G, .) \to (G', *)$ un morphisme de groupe.
$f(G)$ est appelé l'image du morphisme f et noté $\mathrm{Im}(f)$

Définition I - 12 : Noyau
$f^{-1}(\{e'\})$ est appelé le noyau du morphisme f et noté $\ker(f)$

Proposition I - 6 :
$\mathrm{Im}(f)$ et $\ker(f)$ sont des sous groupes respectivement de G' et de G.

Proposition I - 7 : Caractérisation de l'injectivité
f est injective si et seulement si $\ker(f) = \{e\}$

d) Composition

Proposition I - 8 : Composée
La composée de deux morphismes de groupes est un morphisme de groupes.

Proposition I - 9 :
L'application réciproque d'un isomorphisme de groupes est aussi un morphisme de groupes.

Corollaire I - 1 :
L'ensemble des automorphismes d'un groupe G est un groupe noté $Aut\,(G)$

3) Groupes monogènes et groupes cycliques

a) Définitions

Définition I - 13 : Groupe monogène
On appelle groupe monogène tout groupe engendré par un seul élément.
Tout élément qui engendre le groupe est appelé générateur du groupe .

Définition I - 14 : Groupe cyclique
On appelle groupe cyclique tout groupe monogène fini.

b) Le groupe $\mathbb{Z}/n\mathbb{Z}$

Définition I - 15 : Relation de congruence
Soit $n \in \mathbb{N}^*$, deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont dits congrus modulo n si et seulement si $b - a \in n\mathbb{Z}$, ou encore $a + n\mathbb{Z} = b + n\mathbb{Z}$. On note alors $a \equiv b\,[n]$.
On a donc

$$a \equiv b\,[n] \Leftrightarrow (n \mid (a - b))$$

Propriété I - 2 :
Cette relation est une relation d'équivalence sur $\mathbb{Z}$.

Définition I - 16 :
Soit n un entier non nul, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation de congruence modulo n.

Proposition I - 10 : Cardinal
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n. Un ensemble de représentants est donné par les classes de 0, 1, .., $n - 1$.

Proposition I - 11 : Compatibilité avec l'addition
Soit $n \in \mathbb{N}^*$. On peut alors définir la loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ suivante :

$$(a, b) \in \mathbb{Z}^2 \qquad \overline{a} + \overline{b} = \overline{a + b}$$

Corollaire I - 2 : Groupe monogène
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de cette loi de composition interne est un groupe abélien monogène.

Théorème I - 1 : Les groupes monogènes

1) Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
2) Tout groupe monogène fini de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

4) Ordre d'un élément dans un groupe

Définition I - 17 :
Soit a un élément de G, l'ordre de a est le nombre d'éléments du sous groupe engendré par a. Celui-ci pouvant fini ou infini.

Proposition I - 12 :
Soit $(G, .)$ un groupe et a un élément de G. On considère l'application φ_a de $\mathbb{Z}$ dans G définie par $\varphi_a(0) = e$, où e est l'élément neutre du groupe, et $\forall n \in \mathbb{Z}^*$, $\varphi_a(n) = a^n$.
On a alors :

1) φ_a est un morphisme de groupes.
2) Son image est le sous-groupe engendré par a.
3) Son noyau est un sous groupe de $\mathbb{Z}$ et, soit $n \in \mathbb{N}$ tel que $\ker(\varphi_a) = n\mathbb{Z}$, on a
   - si $n = 0$, a est d'ordre infini
   - si $n \neq 0$, n est l'ordre de a.

Proposition I - 13 :
Soit $(G, .)$ un groupe d'élément neutre e et a un élément de G d'ordre d.
On a : pour $n \in \mathbb{Z}$, $a^n = e \Leftrightarrow d \mid n$.

Théorème I - 2 : Petit théorème de Lagrange
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe

II Les anneaux

1) Anneaux

Définition II - 1 :

On appelle anneau un ensemble A (non vide) munis de deux lois de compositions internes (+) et (.) , qui ont les propriétés suivantes :

- $(A, +)$ est un groupe abélien
- La seconde loi est associative, admet un élément neutre et est distributive par rapport à l'addition (première loi)

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

- Un anneau est dit commutatif si la seconde loi (souvent appelée multiplication) est commutative.

Notation :

– on note 0 (ou 0_A lorsqu'il faut préciser A) l'élément neutre de l'addition.
– L'élément neutre de la multiplication est noté 1_A
– On notera $(-x)$ le symétrique de tout élément de A pour l'addition, il sera alors appelé opposé de x
– On notera x^{-1} le symétrique de x, losque celui ci existe.

Proposition II - 1 : Règles de calculs

1) L'élément nul est absorbant : $\forall x \in A,\ 0.x = x.0 = 0$
2) $\forall x \in A,\ (-1).x = x.(-1) = -x$
3) Règle des signes : $\forall (x, y) \in A^2,\ x.(-y) = (-x).y = -x.y,\ (-x).(-y) = x.y$

Théorème II - 1 :

Soient a et b deux éléments de A qui commutent (ie : $ab = ba$) et $n \in \mathbb{N}$. On a les formules suivantes :

1) Formule du binôme de Newton : $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

2) Formule de Jacob Bernoulli : $a^{n+1} - b^{n+1} = (a - b)\left(\sum_{k=0}^{n} a^k b^{n-k}\right)$

Propriété II - 1 : Groupe des inversibles

Soit $(A, +, \cdot)$ un anneau. L'ensemble des éléments inversibles de A muni de la loi $\cdot$ est un groupe.

Définition II - 2 : Produit fini d'anneaux

Soit $(A_i)_{i \in [\![1,p]\!]}$ une famille finie (non vide) d'anneaux.
On définit une structure d'anneau au produit cartésien des anneaux en définissant les lois de compositions internes composantes par composantes.

Définition II - 3 : Sous anneaux

Soit $(A, +.)$ un anneau. Soit B une partie de A.
On dit que B est un sous-anneau de A si

- $1_A \in B$
- B est stable par $+$ et $.$
- B muni de ces lois est un anneau.

Propriété II - 2 : Intersection

L'intersection d'une famille de sous-anneaux est un sous-anneau.

2) Morphismes d'anneaux

Définition II - 4 :

Soient $(A,+,.)$ et $(B,+,*)$ deux anneaux.
Une application φ de A vers B est un morphisme d'anneau si

1) $\varphi(1_A) = 1_B$
2) $\forall (x,y) \in A^2$, $\varphi(x+y) = \varphi(x) + \varphi(y)$.
3) $\forall (x,y) \in A^2$, $\varphi(x.y) = \varphi(x) * \varphi(y)$.

Si on a $(A,+,.) = (B,+,*)$ alors on parle d'endomorphisme d'anneau.

Par propriétés de calculs dans un anneau, la conservation de la structure permet d'avoir les propriétés suivantes.

Propriété II - 3 :

1) $\varphi(0_A) = 0_B$
2) $\forall x \in A$, $\varphi(-x) = -\varphi(x)$
3) $\forall x \in A$, $\forall n \in \mathbb{Z}$, $\varphi(nx) = n\varphi(x)$
4) $\forall x \in A$, $\forall n \in \mathbb{N}$, $\varphi(x^n) = (\varphi(x))^n$
5) si $x \in A$ est un élément inversible, on a $\varphi(x)$ est aussi inversible et $(\varphi(x))^{-1} = \varphi\left(x^{-1}\right)$

Proposition II - 2 : Images directes et réciproques

Soient $(A,+,.)$ et $(B,+,*)$ deux anneaux et φ un morphisme d'anneaux de A vers B.
- Si A' est un sous anneau de A alors $\varphi(A')$ est un sous anneau de B
- Si B' est un sous anneau de B alors $\varphi^{-1}(B')$ est un sous anneau de A

Définition II - 5 : Image et noyau

Soient $(A,+,.)$ et $(B,+,*)$ deux anneaux et φ un morphisme d'anneaux de A vers B.
On appelle image de φ le sous-anneau de B : $\varphi(A)$ et on le note $\mathrm{Im}(\varphi)$.
On appelle noyau de φ, $\varphi^{-1}(\{0_B\})$ et on le note $\ker(\varphi)$.

Propriété II - 4 : Injectivité, surjectivité

Un morphisme d'anneaux est injectif si et seulement si son noyau est réduit à $\{0\}$.
Un morphisme d'anneaux φ de A dans B est surjectif si et seulement si $\varphi(A) = B$.

Comme pour les morphismes de groupes on a les définitions suivantes.

Définition II - 6 :

Un morphisme d'anneaux bijectif est appelé isomorphisme d'anneaux.
Un morphisme d'anneaux d'un anneau dans lui même est un endomorphisme d'anneau.
Si, de plus, celui-ci est bijectif alors on parle d'automorphisme.

Propriété II - 5 : $Aut\,(A)$

L'ensemble des automorphismes d'un anneau A, muni de la composition est un groupe noté $Aut\,(A)$.

3) Anneaux intègres, corps

Définition II - 7 : Diviseurs de 0

Soit $(A,+,.)$ un anneau. On appelle diviseur de 0 tout élément $x \in A$ non nul tel qu'il existe $y \in A$ vérifiant $x.y = 0$ (diviseur à droite) ou $y.x = 0$ (diviseur à gauche).

Définition II - 8 : Anneau intègre

Un anneau est dit intègre s'il est commutatif et si tout élément non nul est régulier pour la loi multiplicative. C'est à dire qu'il n'existe pas de diviseur de 0.

Définition II - 9 : Corps

Soit A un anneau. On dit que A est un corps si tout élément non nul est inversible (symétrisable pour la loi multiplicative).

Définition II - 10 : Sous-corps

On appelle sous-corps d'un corps K tout sous-anneau possédant la structure de corps.

Définition II - 11 : Morphisme

Un morphisme de corps est un morphisme d'anneaux défini entre deux corps.

Propriété II - 6 :

Soit f un morphisme de corps défini de K dans L. On a
- $\forall x \in \mathsf{K} \setminus \{0\},\ f\left(x^{-1}\right) = (f(x))^{-1}$.
- f est injective et son image est un sous-corps de L.

4) Idéaux d'un anneau commutatif

a) Généralité

Définition II - 12 : Idéal d'un anneau commutatif

On dit qu'une partie non vide I d'un anneau commutatif $(A,+,.)$ est un idéal de A si

1) I est stable par l'addition.

2) $\forall\,(a,x) \in A \times I,\ a.x \in I$. On parle alors de stabilité forte par la multiplication.

Propriété II - 7 :

Un idéal de $(A,+,.)$ est un sous groupe de $(A,+)$.

Proposition II - 3 : Noyau d'un morphisme

Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.

Proposition II - 4 :

Soient I et J deux idéaux de A on a :

- $I+J$ est un idéal de A. C'est le plus petit contenant les deux.
- $I \cap J$ est un idéal : c'est le plus grand contenu dans les deux.

Définition II - 13 : Relation de divisibilité

Soit $(A,+,.)$ un anneau commutatif intègre. Soient x et y deux éléments de A. On dit que x divise y, ou que y est un multiple de x ou encore que x est un diviseur de y si il existe $q \in A$ tel que $y = x.q$.
Dans ce cas on note $x \mid y$.

Proposition II - 5 : Interprétation à l'aide des idéaux

Pour que x divise y, il faut et il suffit que $Ay \subset Ax$.

b) Idéaux de $\mathbb{Z}$

Théorème II - 2 : Idéaux de $\mathbb{Z}$

Les idéaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Proposition II - 6 : Caractérisation du PGCD et PPCM

Soient a et b deux éléments de $\mathbb{Z}$.

1) $a\mathbb{Z} + b\mathbb{Z} = a \wedge b\mathbb{Z}$. Autrement dit le PGCD de deux entiers est le générateur de l'idéal $a\mathbb{Z} + b\mathbb{Z}$
2) $a \vee b\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Autrement dit le PPCM de deux entiers est le générateur de l'intersection des deux idéaux.

Théorème II - 3 : de Bézout

Deux entiers a et b sont premiers entre eux si et seulement si $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

Exemple II - 1 :
86 banque CCINP

1. Soit $(a,b,p) \in \mathbb{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
2. Soit p un nombre premier.
   (a) Prouver que $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis en déduire que p divise $\binom{p}{k}$.
   (b) Prouver que : $\forall n \in \mathbb{N}$, $n^p \equiv n \mod p$.
   Indication : procéder par récurrence.
   (c) En déduire, pour tout entier naturel n, que : p ne divise pas $n \Longrightarrow n^{p-1} \equiv 1 \mod p$.

5) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition II - 7 : Multiplication de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On peut alors définir la loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ suivante :

$$(a,b) \in \mathbb{Z}^2 \qquad \overline{a}.\overline{b} = \overline{a.b}$$

Théorème II - 4 : L'anneau $\mathbb{Z}/n\mathbb{Z}$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des deux lois de compositions internes définies par les lois sur $\mathbb{Z}$ est un anneau commutatif.
Le morphisme d'anneau : π_n de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui à k associe $\overline{k}$ est appelé morphisme canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Théorème II - 5 : Générateurs et éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Les générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les classes des entiers k telles que k est premier avec n.
Ce sont aussi les éléments inversibles de l'anneau.

Corollaire II - 1 : Corps

$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.
Dans ce cas le corps est noté $\mathbb{F}_p$

Théorème II - 6 : chinois

Soit n et m deux entiers naturels non nuls et premiers entre eux.
On a un isomorphisme d'anneaux entre $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Exemple II - 2 :

94 banque CCINP

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux.
   Soit $c \in \mathbb{N}$.
   Prouver que : $(a|c \text{ et } b|c) \iff ab|c$.
3. On considère le système (S) : $\begin{cases} x & \equiv & 6 & [17] \\ x & \equiv & 4 & [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.
   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Définition II - 14 : Indicatrice d'Euler

Soit $n \in \mathbb{N}^*$. On note $\varphi(n)$ le cardinal de $\{r \in [\![0, n-1]\!] \ / \ r \wedge n = 1\}$.
C'est aussi le nombre de générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, ainsi que le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$.
L'application φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ ainsi définie est appelée indicatrice d'Euler.

Corollaire II - 2 : Calcul de $\varphi(n)$

Si m et n sont deux nombres premiers entre eux alors $\varphi(mn) = \varphi(n)\varphi(m)$.

Si $n = \prod_{i=1}^{j} p_i^{\alpha_i}$ est la décomposition de n en facteurs premiers alors $\varphi(n) = n\prod_{i=1}^{j}\left(1 - \frac{1}{p_i}\right)$.

Théorème II - 7 : d'Euler

Si a et n sont deux nombres premiers entre eux alors $a^{\varphi(n)} \equiv 1\,[n]$.

Théorème II - 8 : (petit) de Fermat

Si p est un nombre premier et si $a \in \mathbb{N}^*$ n'est pas divisible par p alors $a^{p-1} \equiv 1\,[p]$.

6) Anneaux de polynômes à une indéterminée

Proposition II - 8 : Intégrité

L'anneau $(\mathbb{K}[X], +, \times)$ est un anneau intègre.

Définition II - 15 : Ensemble des multiples

Soit A un élément de $\mathbb{K}[X]$, l'ensemble des multiples de A est un idéal noté (A).

Théorème II - 9 : Idéaux de $\mathbb{K}[X]$

Les idéaux de $\mathbb{K}[X]$ sont les idéaux (A) avec $A \in \mathbb{K}[X]$

Proposition II - 9 : PGCD

Soient A et B deux éléments de $\mathbb{K}[X]$, le PGCD de A et B est le polynôme unitaire D tel que $(A) + (B) = (D)$.

Corollaire II - 3 : Relation de Bézout

Soient A et B deux éléments de $\mathbb{K}[X]$ et $D = A \wedge B$.
Il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $D = UA + VB$.

Définition II - 16 : Polynômes premiers entre eux

On dit que deux polynômes A et B sont premiers entre eux si $A \wedge B = 1$.

Théorème II - 10 : Lemme de Gauss

Si un polynôme A est premier avec B et divise le produit BC, alors A divise C

Définition II - 17 : Eléments irréductibles

Un polynôme non constant $A \in \mathbb{K}[X]$ est dit irréductible sur $\mathbb{K}[X]$ s'il n'est divisible que par les polynômes constants et ses polynômes associés.

Théorème II - 11 : Décomposition

Si A est un polynôme non constant de $\mathbb{K}[X]$, on peut écrire

$$A = \lambda \prod_{k=1}^{m} P_k^{\alpha_k}$$

avec $\lambda \in \mathbb{K}^*$, $m \in \mathbb{N}^*$, P_1, ...,P_m des polynômes irréductibles unitaires deux à deux distincts et α_1, ..., α_m des entiers non nuls.
De plus, cette décomposition est unique à l'ordre près des facteurs.

III Algèbres

Définition III - 1 :

On appelle $\mathbb{K}$-algèbre tout quadruplet $(A, +, \times, .)$ formé d'un ensemble A, de deux lois de composition internes $+,\times$ sur A et d'un produit extérieur (loi de composition externe) opérant de $\mathbb{K}$ sur A vérifiant :

1) $(A, +, .)$ est un $\mathbb{K}$-espace vectoriel

2) $(A, +, \times)$ est un anneau

3) $\forall \lambda \in \mathbb{K}$, $\forall (x, y) \in A^2$ $(\lambda.x) \times y = \lambda.(x \times y) = x \times (\lambda.y)$.

Définition III - 2 : Sous-algèbre

Une sous-algèbre est une partie non vide d'une algèbre A,contenant 1_A, stable par combinaisons linéaires et par la multiplication. C'est donc à la fois un sous-espace vectoriel et un sous-anneau.

Définition III - 3 : Morphisme d'algèbres

Un morphisme d'algèbres est une application linaire qui est aussi un morphisme d'anneaux.