7 Compléments : Quelques structures algébriques

Introduction : L'ensemble des nombres rationnels est muni de deux opérations : l'addition et la multiplication vérifiant des propriétes qui sont utilisées les yeux fermés. Dans l'ensemble de ce cours, nous rencontrerons de nombreux autres ensembles munis de lois vérifiant des propriétés qui gouvernent les calculs entre leurs éléments : le corps des nombres rationnels, réels ou complexes, l'ensemble des matrices carrées de taille n pour les lois de multiplication et d'addition, les n-uplets de réels muni des lois d'addition et de multiplication par un réel. Ces lois sont la structure algébrique de ces ensembles.

Un objectif général de ce cours sera de définir les espaces vectoriels et d'en étudier les premières propriétés. Pour situer ce paragraphe, disons seulement qu'un espace vectoriel sur un corps sera défini comme un ensemble muni d'un loi interne et d'une loi externe défini au moyen de ce corps.

Nous donnons ainsi dans ce paragaphe les définitions de quelques structures algébriques de base : groupes, groupes commutatifs, anneaux, anneaux commutatifs, corps, espaces-vectoriels sur un corps.

Il s'agit d'un paragraphe qui servira de références dans le cours. Dans un premier temps, nous attendons que l'étudiant lise le sous-paragraphe **??** sur les groupes qui n'est pas facile et se pose quelques questions à son sujet ....

7.1 Groupes

Groupes : Soit G un ensemble et une application :

$$G \times G \longrightarrow G \ : \ (x, y) \longmapsto x * y$$

que nous appelons loi de composition interne. Relativement à cette loi interne, nous disons que G est un *groupe* si les trois propriétés suivantes sont vérifiées :

i) La loi est associative : pour tout $x, y, z \in G$:

$$(x * y) * z = x * (y * z) \ .$$

Cet élément est alors noté $x * y * z$.

ii) Existence d'un *élément neutre* : il existe $e \in G$ tel que pour tout $x \in G$:

$$x * e = e * x = x \ .$$

Cet élément est alors unique et est appelé l'élément neutre du groupe.

iii) Existence d'un *symétrique* : pour tout élément $x \in G$, il existe un élément $x' \in G$ tel que

$$x * x' = x' * x = e \ .$$

Cet élément x' est alors unique. Il est appelé le symétrique de x.

Si la loi d'un groupe est notée . ou sans signe, l'élément neutre est noté 1 et le symétrique d'un élément x de G est noté x^{-1}.

Exemple de base : Le groupe $\mathcal{S}(X)$ des bijections d'un ensemble X vers lui même muni de la loi de composition.

Pour expliquer cet exemple, il nous faut revenir sur la notion d'application bijective. Soit X et Y deux ensembles. Une application $f : X \to Y$ est dite bijective si pour tout $y \in Y$, il existe $x \in X$ unique tel que $f(x) = y$. Cet élément x est alors noté $f^{-1}(y)$ et l'application :

$$f^{-1} : Y \to X \ : \ y \mapsto f^{-1}(y)$$

est appelé l'application réciproque ou inverse de f. Cette application f^{-1} est elle même bijective de réciproque f. On peut alors vérifier que pour tout $x \in X$: $f^{-1} \circ f(x) = x$ et pour tout $y \in Y$, $f \circ f^{-1}(y) = y$.

Désignons par Id_X l'application :

$$\mathrm{Id}_X : X \to X \ : \ x \mapsto \mathrm{Id}_X(x) = x \quad .$$

Pour toute bijection $f : X \to Y$, nous avons :

$$f^{-1} \circ f = \mathrm{Id}_X \quad , \quad f \circ f^{-1} = \mathrm{Id}_Y$$

Enfin, si $f : X \to Y$ et $g : Y \to Z$ sont deux bijections, nous vérifions que la composée $g \circ f : X \to Z$ est une bijection et que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Assertion : Soit X un emsemble, l'ensemble $\mathcal{S}(X)$ des bijections de X vers X muni de la loi de composition des applications est alors un groupe. L'application Id_X en est l'élément neutre et l'application $f^{-1} : X \to X$ n 'est autre que le symétrique de l'élément f.
Exercice : Soit $X = \{a, b, c\}$ un ensemble à 3 éléments. Montrer que le groupe $S(\{a, b, c\})$ a 6 éléments et décrire ce groupe.

Groupes commutatifs : Le groupe G est dit *abélien* ou *commutatif* si et seulement si pour tout $x, y \in G$:

$$x * y = y * x \ .$$

La loi d'un groupe commutatif est souvent notée $+$. L'élément neutre est alors noté 0, le symétrique d'un élément x de G noté $-x$ et nous posons pour tout $x, y \in G$, $x + (-y) = x - y$.

Exemple de base : L'ensemble $\mathbf{Z}$ des entiers relatifs muni de la loi d'addition est un groupe commutatif noté $(\mathbf{Z}, +)$.

Sous-groupes : Soit G un groupe pour la loi $*$ et H un sous-ensemble de G. Nous supposons que H vérifie les trois propriétés :

i) Pour tout $x, y \in H$, $x * y \in H$.

ii) Le neutre de G est dans H.

iii) Pour tout $x \in H$, le symétrique x' de x est dans H.

Considérons alors l'applicatiion :

$$H \times H \longrightarrow H \ : \ (x,\, y) \longmapsto x * y$$

Cette application est d'après la propriété i) bien définie. Elle définit donc une loi interne sur H que nous continuons à noter $*$. On dit que cette loi est obtenue par restriction à partir de celle de G. Alors, nous pouvons vérifier que cette loi $*$ sur H munit H d'une structure de groupe. Son élément neutre est l'élément neutre de G (qui appartient à H d'après la propriété ii)). Nous disons alors que H est *un sous-groupe* de G.

Exemple de base : L'ensemble noté $17\,\mathbf{Z}$ des entiers relatifs multiple de 17 est un sous-groupe du groupe $\mathbf{Z}, +$.

Morphismes de groupes : Un *morphisme de groupes ou homomorphisme de groupes* est une application entre deux groupes qui respecte les structures des groupes. Plus précisément, si $(G, *)$ et $(G', \star)$ sont deux groupes d'éléments neutres respectifs e et e', une application $f : G \to G'$ est un morphisme de groupe lorsque pour tout $x, y \in G$:

$$f(x * y) = f(x) \star f(y) \ .$$

Les deux propriétés suivantes sont alors des conséquences immédiates de la définition d'un morphisme de groupe et de la définition d'un groupe :

$$f(e) = e' \quad \text{et} \quad \forall x \in G,\ f(x^{-1}) = [f(x)]^{-1} \, .$$

On laisse le soin au lecteur de les démontrer.

Exemple de base : L'application de multiplication par 17 :

$$\mathbf{Z} \to \mathbf{Z} \ : \ m \mapsto 17m$$

est un morphisme du groupe $(\mathbf{Z}, +)$.

7.2 Anneaux

A partir de maintenant, on se permettra de noter dans les formules mathématiques l'expression "pour tout " par $\forall$. Cela, seulement dans les formules, afin de ne pas mélanger les formules mathématiques et le texte qui les mets en jeu.

Anneaux : Un ensemble A muni de deux lois de composition interne :

$$A \times A \longrightarrow A \ : \ (x,\, y) \longmapsto x + y \ \text{ dite additive}$$

$$A \times A \longrightarrow A \ : \ (x,\, y) \longmapsto xy \ \text{ dite multiplicative}$$

est un *anneau* si les quatre propriétés suivantes sont vérifiées :

i) La loi additive est une loi de groupe commutatif.

ii) La loi multiplicative est associative :

$$\forall\, x, y, z \in A \quad , \quad (xy)z = x(yz)\ .$$

iii) La loi multiplicative est distributive par rapport à l'addition, c'est-à-dire :

$$\forall\, x, y, z \in A \quad , \quad x\,(y+z) = x\,y + x\,z \quad \text{et} \quad (y+z)\,x = y\,x + z\,x\ .$$

iv) La loi multiplicative a un élément neutre : il existe $e \in A$ tel que pour tout $x \in A$:

$$xe = ex = x\ .$$

Cet élément est alors unique et noté 1.

Les deux propriétés suivantes sont des conséquences immédiates de la définition :

$$\forall\, x, y, z \in A, \quad 0x = 0 \quad , \quad x\,(y - z) = x\,y - x\,z \quad \text{et} \quad (y - z)\,x = y\,x - z\,x\ .$$

Exemple de base : Soit n un entier, l'ensemble $\mathcal{M}_n(\mathbf{R})$ des matrices $n \times n$ à coefficients réels muni de sa loi d'addition et de produit est un anneau.

Anneaux commutatifs : L'anneau A est dit *commutatif* si la loi multiplicative est commutative, c'est à dire :

$$\forall\, x, y \in A \quad , \quad xy = yx\ .$$

Exemple de base : L'ensemble $\mathbf{Z}$ des entiers relatifs munis des lois d'addition et de multiplication.

Éléments inversibles d'un anneau : Un élément a d'un anneau A est dit *inversible*, s'il existe $a' \in A$ tel que

$$aa' = a'a = 1\ .$$

Cet élément est alors unique, noté a^{-1} et appelé inverse de a. L'ensemble des éléments inversibles d'un anneau A forment alors un groupe pour la loi mutiplicative. Ce groupe est noté A^*.

Sous-anneaux : Soit A un anneau et B un sous-ensemble de A. Nous supposons que B vérifie les deux propriétés :

i) B est un sous-groupe de A relativement à la loi additive de A.

ii) $\forall\, x, y \in B \quad , \quad xy \in B \quad .$

iii) $1 \in B \quad .$

alors, les lois additive et multiplicative de A définissent par restriction (voir la définition d'un sous-groupe) des lois internes de B qui munissent B d'une structure d'anneau. Nous disons alors que B est un *sous-anneau* de A.

Exemple de base : Soit n un entier, le sous-ensemble des matrices diagonales est un sous-anneau de $\mathcal{M}_n(\mathbf{R})$.

Morphismes d'anneaux : Un *morphisme d'anneaux ou homomorphisme d'anneaux* est une application entre deux anneaux qui respecte les structures d'anneaux. Autrement dit, si A et A' sont deux anneaux , une application $f : A \to A'$ est dite un morphisme d'anneaux si :

- $\forall\, x, y \in A \quad , \quad f(x+y) = f(x) + f(y) \quad .$
- $\forall\, x, y \in A \quad , \quad f(xy) = f(x) f(y) \quad .$
- $f(1) = 1 \quad .$

Il en résulte que si $a \in A$ est inversible, $f(a)$ est inversible et $f(a^{-1}) = [f(a)]^{-1}$.

7.3 Corps

Corps : Un ensemble K muni de deux lois de composition interne :

$$K \times K \longrightarrow A \ : \ (x,\, y) \longmapsto x + y \ \text{ dite additive}$$

$$K \times K \longrightarrow A \ : \ (x,\, y) \longmapsto x\, y \ \text{ dite multiplicative}$$

est un *corps* si les propriétés suivantes sont vérifiées :

i) Muni de la loi additive, K est un groupe commutatif.

ii) Muni de la loi multiplicative, $K - \{0\}$ est un groupe commutatif.

iii) La loi multiplicative est distributive par rapport à l'addition, c'est-à-dire :

$$\forall\, x, y, z \in K \quad , \quad x\,(y+z) = x\,y + x\,z \quad \text{et} \quad (y+z)\,x = y\,x + z\,x \ .$$

Autrement dit un corps K non réduit à $\{0\}$ est un anneau dont tout élément non nul est inversible ou encore un anneau tel que $K^* = K - \{0\}$. Le neutre de K comme anneau est le neutre du groupe multiplicatif $K - \{0\}$.

Exemple de base : Munis des opérations usuelles d'addition et de multiplication, l'ensemble $\mathbf{R}$ des nombres réels ou $\mathbf{C}$ des nombres complexes est un corps.

Sous-corps : Soit K un corps et L un sous-ensemble de K. Nous supposons :

i) L est pour la loi additive un sous-groupe de K,

ii) L^* est pour la loi multiplicative un sous-groupe de K^*.

alors les lois additive et multiplicative de K induisent par restrictions des lois internes sur L qui munissent L d'une sructure de corps. Nous disons alors que L est un *sous-corps* de K.

Exemple de base : L'ensemble $\mathbf{Q}$ des nombres rationnels (ensemble dont les éléments sont les quotients de nombres entiers relatifs) est un sous-corps du corps des nombres réels.

Morphismes de corps : Un *morphisme de corps ou homomorphisme de corps* est une application entre deux corps qui respecte les structures de corps . Ainsi, si K et K' sont deux corps , une application $f : K \to K'$ est un morphisme de corps si :

- $\forall\, x, y \in K \quad , \quad f(x+y) = f(x) + f(y) \quad .$
- $\forall\, x, y \in K \quad , \quad f(xy) = f(x)f(y) \quad .$
- $f(1) = 1 \quad .$

Exemple de base : La conjugaison est un morphisme du corps des nombres complexes vers lui même.

7.4 K-espaces vectoriels

K-espaces vectoriels : Soit K désigne un corps et E un ensemble muni
- d'une loi interne dite d'addition :

$$E \times E \to E, (u, v) \mapsto u + v \quad ,$$

- d'une loi externe dite de multiplication par un scalaire :

$$K \times E \to E, (\lambda, u) \mapsto \lambda u \quad .$$

E est dit est un *K-espace vectoriel* si :

i) La loi interne d'addition est une loi de groupe commutatif.

ii) La loi externe vérifie pour tout $u \in E$ et $\lambda, \mu \in K$:

$$1u = u \quad , \quad \lambda(\mu u) = (\lambda\mu)u \; .$$

iii) Les lois vérifient entre elles pour tout $u, v \in E$ et $\lambda, \mu \in K$:

$$(\lambda + \mu)u = \lambda u + \mu u \quad , \quad \lambda(u + v) = \lambda u + \lambda v \; .$$

Pour le distinguer du neutre de l'addition de K, nous notons $\vec{0}$ le neutre de l'addition de E. Il résulte alors des définitions :

$$\forall\, \lambda \in K \,, \forall\, u \in E \quad , \quad \lambda\vec{0} = \vec{0} \quad , \quad 0u = \vec{0} \quad , \quad (-\lambda)u = -(\lambda u) \quad .$$

Nous notons alors $(-\lambda)u = -(\lambda u) = -\lambda u$.

Exemple de base : L'ensemble des nombres complexes muni de l'addition et de la multiplication par les nombres réels est un **R**-espace vectoriel.

Sous-espaces vectoriels : Soit E un K-espace vectoriel et F un sous-ensemble de E. Si les conditions suivantes sont réalisées :

i) $\forall\, u, v \in F \quad , \quad u + v \in F \quad ,$

ii) $\forall\, u, \in F\ , \forall\, \lambda \in K \quad , \quad \lambda u \in F \quad .$

Alors la loi additive et la loi externe de E induisent par restrictions sur F une la loi interne additive et une loi externe sur F qui munissent F d'une structure de K-espace vectoriel. Nous disons alors que F est un *sous-espace vectoriel* de E.

Exemple de base : L'ensemble des nombres réels forment un sous-espace vectoriel **R**-espaces vectoriel des nombres complexes.

Morphismes de K-espaces vectoriels : Soit E et F deux K-espaces vectoriels. Une application $f : E \to F$ est dite une *application linéaire* si

- $\forall\, u, v \in E \quad , \quad f(u + v) = f(u) + f(v) \quad ,$
- $\forall\, \lambda \in K\ , \forall u \in E \quad , \quad f(\lambda u) = \lambda f(u).$

Il résulte alors des définitions les propriétés :

$$\forall\, \lambda \in K\, , \forall\, u \in E \quad , \quad f(-\lambda u) = -\lambda f(u)\ .$$

Exemple de base : La conjugaison est un morphisme du **R**-espace vectoriel des nombres complexes vers lui même.