Chapitre 8
STRUCTURES ALGÉBRIQUES

Mohamed TARQI

Table des matières

••••••••••

1 Lois de compositions

1.1 Loi de composition interne

Définition 1.1 *Soit E un ensemble non vide, une loi de composition sur E est une application de E^2 dans E. À un couple (x,y) d'éléments de E, elle fait correspondre un élément appelé composé de x et de y et noté $x \top y$ (lire x truc y).*

En général on note un ensemble E, muni d'une loi $\top$, par $(E,\top)$

Remarques :

1. En général, on emploie exprès un symbole n'ayant aucune définition mathématique préalable ; en peut employer aussi $\perp$ (antitruc), $*$,...
2. Lorsque la loi est l'addition, le composé de x et y se note $x+y$ et s'appelle somme de x et y ; lorsque la loi est la multiplication le composé de x et y s'appelle produit de x et y et se note xy (ou parfois $x.y$)

Exemples :

1. Dans l'ensemble $\mathscr{P}(E)$ des parties d'un ensemble E, la réunion $\cup$ et l'intersection $\cap$ sont des lois composition internes.
2. Sur l'ensemble des applications dans un ensemble E dans lui même, l'application qu'à tout couple (f,g) associé l'application composée $g\circ f$ est une loi de composition interne.
3. Dans $\mathbb{R}$, l'application qui à tout couple (x,y) associé le nombre $x+iy$ ($i^2=1$) n'est pas une loi de composition interne, de même, dans $\mathbb{N}$, l'application qui à tout couple (x,y) associé $x-y$ n'est pas une loi de composition interne.

1.2 Commutativité et associativité

Soit $(E,\top)$ un ensemble muni d'une loi $\top$. En général il n'y pas aucune raison pour que $x\top y = y\top x$ ou bien $(x\top y)\top z = x\top(y\top z)$.

Définition 1.2 *On dit que des éléments x et y de E commutent si $x\top y = y\top x$. Si cette propriété est satisfaite pour tout couple (x,y) de E, on dit que la loi est commutative.*

Définition 1.3 *On dit que la loi est associative si pour tout triplet (x,y,z) d'éléments de E, $(x\top y)\top z = x\top(y\top z)$. La valeur commune des deux membres se note $x\top y\top z$.*

Exemples :

1. Sur l'ensemble $\mathscr{P}(E)$ des parties d'un ensemble E, la réunion $\cup$ et l'intersection $\cap$ sont toutes deux commutatives est associatives.
2. Sur l'ensemble des applications dans un ensemble E dans lui même, le composé des applications est associative, mais elle n'est pas commutative dans le cas général.

Notations : Soient E un ensemble, $\top$ ou . ou + une loi de composition interne associative dans E, $n\in\mathbb{R}$, $a_1,a_2,...,a_n\in E$, $a\in E$. On note

$$\top_{i=1}^{n} a_i = a_1\top a_2\top\ldots\top a_n,\ \prod_{i=1}^{n} a_i = a_1a_2\ldots a_n,\ \sum_{i=1}^{n} a_i = a_1+a_2+\ldots+a_n$$

$$a^n = \underbrace{aa\ldots a}_{n \text{ fois}},\quad na = \underbrace{a+a+\ldots+a}_{n \text{ fois}}$$

en particulier : $a^1 = a$.

1.3 Éléments réguliers. Élément neutre. Éléments symétrisables

E un ensemble non vide muni d'une loi de composition interne $\top$

Définition 1.4 *On dit qu'un élément a de E est régulier, ou simplifiable si pour tout couple (x,y) d'éléments de E :*

$$a\top x = a\top y \Longrightarrow x = y$$

et si de même

$$x\top a = y\top a \Longrightarrow x = y$$

Remarque : a est régulier si et seulement si les deux applications $x\longrightarrow a\top x$ et $x\longrightarrow x\top a$ sont injectives.

Définition 1.5 *On dit qu'un élément e de E est élément neutre si pour tout élément x de E, $x\top e = e\top x = x$.*

Proposition 1.1 **Si la loi est $\top$ admet un élément neutre elle est unique.**

Démonstration : Soit en effet ω un deuxième élément neutre, donc $e\top\omega = e$, de même puisque e élément neutre $e\top\omega = \omega$, par suite $\omega = e$. □

Exemples :

1. Dans $\mathscr{P}(E)$, le vide est un élément neutre pour la réunion la partie pleine E est élément neutre pour l'intersection.
2. Dans l'ensemble des applications dans un ensemble E dans lui même, l'application identique I_E est élément neutre pour la composition des applications.

Définition 1.6 *Soit E un ensemble muni d'un loi de composition interne $\top$ admettant un élément neutre e. On dit qu'un élément x de E est symétrisable ou inversible s'il existe un élément y de E tel que :*

$$x \top y = y \top x = e$$

.

Proposition 1.2 **Si (E,T) est associatif, un tel élémnt y, s'il existe est unique ; on l'appelle le symétrique de x.**

Démonstration : Soit en effet y' un élément de E tel que $x \top y' = y' \top x = e$. Par suite :

$$\begin{aligned} y \top (x \top y') &= (y \top x) \top y' \\ &= e \top y' \\ &= y' \end{aligned}$$

Ainsi $y' = y$ □

Remarques et exemples :

Dans l'ensemble des applications dans un ensemble E dans lui même, les éléments symétrisables ne sont autres que les applications inversibles.
D'une manière général, lorsque la loi est noté multiplicativement, les éléments symétrisables sont dites inversibles ; le symétrique d'un élément x s'appelle alors inverse de x et se note x^{-1}. Lorsque la loi est noté additivement, l'élément neutre se note 0, le symétrique d'un élément x s'appelle opposé de x et se note $-x$.

2 Groupes

2.1 Définitions des groupes

Définition 2.1 *On dit que $(G,\top)$ est un groupe s'il satisfait au trois conditions suivantes :*

1. *la loi est associative ;*
2. *il existe un élément neutre ;*
3. *tout élément de G est symétrisable.*

Remarque : La loi n'est pas nécessairement supposée commutative. Un groupe dont la loi est commutative est appelé groupe commutatif ou abélien.

Exemples :

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes additifs commutatifs.
2. $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes multiplicatifs commutatifs.

Exemple fondamental : Soit E un ensemble et τ_E l'ensemble de ces permutations (c'est à dire des bijections de E dans E).
Munissons τ_E de la loi de composition des applications à savoir :

$$(f,g) \longmapsto f \circ g$$

muni de cette loi, τ_E est un groupe, appelé groupe symétrique de E.

2.2 Règles de calcul dans un groupe

Proposition 2.1 **Soit G un groupe noté multiplicativement, a et b des éléments de G. Considérons l'équation $ax = b$ (1) où x est inconnu de G. Cette équation admet une solution et une seule, $x_0 = a^{-1}b$.**

Démonstration :

$$ax = b \Longleftrightarrow a^{-1}(ax) = a^{-1}b$$

soit, compte tenu de l'associatovité ;

$$(a^{-1}a)x = a^{-1}b$$

ou encore, puisque

$$a^{-1}a = e, \quad ex = a^{-1}b$$

Soit enfin $x = a^{-1}b$.
Inversement, l'élément $x_0 = a^{-1}b$ est effectivement solution de (1), en effet :

$$ax_0 = a(a^{-1})b = aa^{-1}b = b$$

□

Remarques :

1. De même l'équation $xa = b$ admet une solution et une seule, à savoir : $x_0 = ba^{-1}$.
2. Si G un groupe commutatif, noté additivement, l'équation $a + x = b$ admet une et une seule solution $x = b - a$.

2.3 Sous-groupes d'un groupe

Soit $(G, \top)$ un groupe, cherchons les parties de G possédant les mêmes propriétés que G.

Définition 2.2 *Soit $(E, \top)$ un ensemble muni d'une loi de composition interne. Un partie F est dite stable par $\top$ si pour tout couple (x, y) de F, $x \top y \in F$.*

Définition 2.3 *Soit G un groupe. On dit qu'une partie H de G est un sous-groupe de G si elle est stable et si munie de la loi de composition induite par celle de G, H est un groupe.*

Exemple : Sous-groupes du groupe additif $\mathbb{Z}$.
Soit H un sous-groupe de $\mathbb{Z}$, non réduit à zéro, donc il contient un élément $n \neq 0$, H contient aussi $-n$, donc H contient des entiers strictement positifs ; leur ensemble a donc un plus petit élément, soit a.
Pour tout $x \in H$, il existe (q, r) couple d'entiers tels que

$$x = aq + r \quad et \quad 0 \leq r < a$$

x et a appartenant à H, il en est de même de aq et de $r = x - aq$, a étant le plus petit entier de H strictement positif, donc $r = 0$ et $x = aq$, d'où

Proposition 2.2 **Les sous-groupes de $\mathbb{Z}$ sont les ensembles $a\mathbb{Z}$.**

Soit H un sous-groupe d'un groupe G de neutre e.
• Soit ω l'élément neutre de H et e l'élément neutre de G, alors $\omega\omega = \omega$ et par suite $e\omega = \omega\omega$, comme l'élément ω est régulier, nous en déduisons que $\omega = e$.
• Soit x un élément de H et y son symétrique dans H, donc on la relation :

$$xy = yx = \omega = e.$$

Ainsi y n'est autre que le symétrique de x dans G.
• Réciproquement, soit H une partie de G telle que :

$$e \in H \text{ et } \forall x \in H, \ x^{-1} \in H$$

alors H est un sous-groupe de G. En effet les conditions 1) 2) et 3) de la définition d'un groupe sont satisfaites.

Proposition 2.3 **Pour qu'une partie non vide H d'un groupe G soit un sous groupe de G, il faut et suffit que, pour tout couple (x, y) d'éléments de H, $xy^{-1} \in H$.**

Démonstration : Si H est un sous-groupe, l'inverse d'un élément y de H appartient ,nécessairement à H, la partie H étant stable, le produit xy^{-1} appartient à H.
Réciproquement, supposons cette condition satisfaite. Puisque H est non vide, il existe au moins un élément x de H, alors $xx^{-1} = e \in H$.
Soit $y \in H$, alors $ey^{-1} = y^{-1} \in H$. Enfin, soit (x, y) un couple d'éléments de H ; alors $y^{-1} \in H$ et $x(y^{-1})^{-1} = xy \in H$.
Ainsi la partie H est stable. □

Exemples :

1. Pour tout groupe G, G lui même et $\{e\}$, e élément neutre de G, sont des sous-groupes de G.
2. Soit τ_E le groupe des permutations d'un ensemble E. Soit $H_x = \{\sigma \in \tau_E / \sigma(x) = x\}$, avec $x \in E$, H_x est un sous-groupe de τ_E, en effet, $I_E \in \tau_E$ puisque $I_E(x) = x$ et pour tout couple (σ, ϱ) de H_x, $\sigma\varrho^{-1}(x) = \sigma(x) = x$, donc $\sigma\varrho^{-1} \in H_x$.

2.4 Intersection de sous-groupes. Sous-groupe engendré par une partie

Proposition 2.4 **L'intersection de deux sous-groupes d'un groupe G est un sous-groupe de G.**

Démonstration : Soient H_1 et H_2 deux sous-groupes d'un groupe G.
• $e \in H_1 \cap H_2$ puisque $e \in H_1$ et H_2.
• Soit (x, y) un couple de $H_1 \cap H_2$, alors $xy^{-1} \in H_1$ et $xy^{-1} \in H_2$, donc $xy^{-1} \in H_1 \cap H_2$. □

Remarque : Soit $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe G, alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Proposition 2.5 ***(et définition)*** **Soit A une partie non vide d'un groupe G, l'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, on l'appelle sous-groupe engendré par la partie A.**

Exercice : Décrire les éléments d'un sous-groupe engendré par une partie A d'un groupe G.

2.5 Groupe monogène. Groupe cyclique

Définition 2.4 *Un groupe ayant une partie génératrice réduite à un élément est dit monogène. Un groupe cyclique est tout groupe monogène et fini, on le note (a).*

Exemple : $(\mathbb{Z},+)$ est un groupe monogène, dont un générateur est 1 (ou -1).

Définition 2.5 *Soit G un groupe, d'élément neutre e, et a un élément de G. Si le groupe engendré par a est fini son cardinal est appelé ordre de a dans G et noté $w(a)$.*

3 Morphismes de groupes

Définition 3.1 *Soient $(G, \top)$ et $(G', \perp)$ des groupes. On dit qu'une application f de G dans G' est un morphisme de groupes si pour tout couple (x, y) d'éléments de G,*

$$f(x \top y) = f(x) \perp f(y)$$

Si f est bijective, on dit que f est un un isomorphisme de G
Un homomorphisme de G dans lui même est un endomorphisme de G et un isomorphisme de G dans G est un automorphisme de G.

Proposition 3.1 **Si f est un homomorphisme de G, d'élément neutre e, dans un groupe G',d'élément neutre e', alors**

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

Démonstration : $\forall\, x \in G$, $f(x) = f(xe) = f(x)f(e) = f(ex) = f(e)f(x)$, donc $f(e) = e'$.
d'autre par

$$e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1}) = f(x^{-1})f(x)$$

alors $f(x^{-1}) = [f(x)]^{-1}$. □

Proposition 3.2 **Soient G et G' des groupes et f un morphisme de G dans G'. L'image par f de tout sous-groupe H de G est un sous-groupe de G'.**

Démonstration : D'abord $e' = f(e) \in f(H)$. Soit (x', y') couple d'éléments de $f(H)$, alors il existe un couple (x, y) d'éléments de H tel que : $x' = f(x)$ et $y' = f(y)$, donc $x'y'^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$. □
En particulier, $f(G)$ est un sous-groupe de G' ; on l'appelle image de f et on la note $Im(f)$.

Proposition 3.3 **Soient G et G' des groupes et f un morphisme de G dans G'. L'image réciproque par f de tout sous-groupe H' de G' est un sous-groupe de G.**

Démonstration : • $f(e) = é \in H' \Longrightarrow e = f^{-1}(e') \in H$
• Soit $(x, y) \in f^{-1}(H)$, alors $f(x)$ et $f(y)$ appartient à H', donc $f(x)f(y)^{-1} = f(xy^{-1}) \in H'$. □
En particulier, l'image réciproque du sous-groupe $\{e'\}$ de G' est un sous-groupe de G ; on l'appelle noyau de f et on le note $\ker f$.

Proposition 3.4 **Pour que le morphisme f soit injectif, il faut et il suffit que $\ker f = \{e\}$.**

Démonstration : Soient x, y des éléments de G tels que $f(x) = f(y)$, alors

$$f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(x)^{-1} = e'$$

et par suite $xy^{-1} \in \ker f = \{e\}$, c'est-à-dire $xy^{-1} = e$ ou encore $x = y$.
Réciproquement, si le morphisme f est injectif, alors

$$\forall x \in G,\quad f(x) = f(e) \Longrightarrow x = e$$

d'où $\ker f = \{e\}$. □
En pratique pour montrer qu'un morphisme est injectif, il faut et il suffit de montrer que l'équation $f(x) = e'$ admet pour seule solution $x = e$.

Théorème 3.1 **La bijection réciproque d'un isomorphisme de groupe est un isomorphisme.**

Démonstration : C'est évident.

Exemple : Soit $a \in \mathbb{R}^{*+} \setminus \{1\}$.

$$\begin{array}{rccc} f: & (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}^{*+}, \times) \\ & x & \longmapsto & a^x \end{array}$$

est un isomorphisme de groupes. En particulier

$$\begin{array}{rccc} f: & (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}^{*+}, \times) \\ & x & \longmapsto & e^x \end{array}$$

et un isomorphisme de groupe et son isomorphisme réciproque est :

$$\begin{array}{rccc} f^{-1}: & (\mathbb{R}^{*+}, \times) & \longrightarrow & (\mathbb{R}, +) \\ & x & \longmapsto & \ln x \end{array}$$

Proposition 3.5 **Soit $(G, .)$ un groupe, de neutre e. Soit $a \in G$, l'application f définie de $\mathbb{Z}$ dans G par : $f(m) = a^m$ est un homomorphisme de groupes.**
L'image de f n'est autre que le sous-groupe (a) de G engendré par a. De plus il existe un unique $n \in \mathbb{R}^*$ tel que $\ker f = n\mathbb{Z}$.

Démonstration : On a : $\forall m,p \in \mathbb{Z}$, $f(mp) = a^{m+p} = a^m a^p = f(m)f(p)$. D'autre par $\ker f$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. □
1er Cas : Si $\ker f = \{0\}$, f est injective, ceci implique $\forall\ m,p \in \mathbb{Z}$, $m \neq p \Longrightarrow a^m \neq a^p$, donc $(a) = \{a^m / m \in \mathbb{Z}\}$ est infini.
2^{e} Cas : Si $\ker f = n\mathbb{Z}$, avec $n \neq 0$.
$\forall\ m \in \mathbb{Z}$, $a^m = e \Longleftrightarrow m \in n\mathbb{Z} \Longleftrightarrow \exists k \in \mathbb{Z} / m = kn$.
Soit $m \in \mathbb{Z}$, il existe $k \in \mathbb{Z}$, tel que $m = kn + r$ et $0 \leq r < n$ donc

$$a^m = (a^n)^k a^r = a^r$$

donc on déduit que

$$(a) = \{a^k / 0 \leq k \leq n-1\}$$

Conclusion : n n'est autre que le cardinal de (a), c'est-à-dire l'ordre de a, donc c'est le plus petit entier strictement positif vérifiant $a^n = e$.

Exemple fondamental : Soit $n \in \mathbb{R}^*$, on note $\mathcal{U}_n = \{s \in \mathbb{C} \ / \ z^n = 1\}$ (les éléments sont appelés racines $n$ièmes de l'unité) $(\mathcal{U}_n, \times)$ est un sous-groupe de $(\mathbb{C}, \times)$, on a :

$$\begin{aligned} \mathcal{U}_n &= \{(e^{\frac{2i\pi}{n}})^k \ / \ 0 \leq k \leq n-1\} \\ &= \{w^k \ / \ 0 \leq k \leq n-1\} \\ &= \{1, w, w^2, ..., w^{n-1}\} \end{aligned}$$

avec $w = e^{\frac{2i\pi}{n}}$. $\mathbb{U}_n$ est un groupe cyclique d'ordre n.

4 Anneaux et corps

4.1 Structure d'anneau

Définition 4.1 *On appelle anneau ensemble A muni de deux lois de composition internes, notées additivement et multiplicativement, satisfaisant aux conditions suivantes :*

1. $(A, +)$ *est un groupe commutatif.*
2. *la multiplication est associative et distributive par rapport à l'addition.*
3. *il existe un élément neutre pour $\times$, noté 1_A*

Les anneaux dont la loi $\times$ est commutative sont appelés anneaux commutatifs.

Exemples :

1. Soit G un groupe additif à un seul élément, noté 0, muni de la multiplication définie par $0.0 = 0$, G est un anneau commutatif, unitaire. L'élément unité est évidement égal à 0.
2. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
3. Voici maintenant un exemple fondamental d'anneau construit à partir d'un autre anneau : Soit E un ensemble et A anneau. On munit l'ensemble $\mathcal{F}(E, A)$ des applications de E dans A des deux lois de compositions :
$$(f, g) \longmapsto f + g \text{ et } (f, g) \longmapsto fg$$
où pour tout élément x de E,
$$(f + g)(x) = f(x) + g(x) \text{ et } (fg)(x) = f(x)g(x)$$
Alors $\mathcal{F}(E, A)$ est un anneau commutatif unitaire d'élément unite l'application identique.
4. Soit E un ensemble non vide, $(\mathcal{P}(E), \triangle, \cap)$ est un anneau commutatif.

Remarques : Soit $\mathbb{R}^I$ l'anneau des applications de l'intervalle I dans $\mathbb{R}$. On sait, si I non réduit à 0, qu'il existe des applications non nulles dont le produit est nul. Par exemple les applications $\chi_{\{a\}}$ et $\chi_{\{b\}}$ (a et b deux éléments distincts de I) sont non nuls, mais leur produit est 0. Ceci nous conduit à poser la définition suivante :

Définition 4.2 *Lorsqu'il existe dans un anneau des éléments a, b tels que :*

$$a \neq 0,\ \ b \neq 0 \text{ et } ab = 0$$

on dit que a et b sont des diviseurs de 0.
On appelle anneau d'intégrité ou anneau intègre un anneau commutatif, non réduit à 0 et dépourvu de diviseurs de 0.

Exemples :

1. $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux intègres.
2. Soit E un ensemble non vide. L'anneau $(\mathscr{P}(E),\triangle,\cap)$ n'est pas intègre ($\forall X \in \mathscr{P}(E),\ X \cap \overline{X} = \emptyset$).

Proposition 4.1 **Soit A un anneau non nul. On note A^* l'ensemble des éléments inversibles pour le produit. A^* est un groupe pour la loi $\times$.**

Démonstration : • $1_A \in A^*$, car $1_A 1_A = 1_A$
• Soient x et y in A^*, alors il existe x' et $y' \in A^*$ tels que $xx' = 1_A$ et $yy' = 1_A$, donc $xy'(xy')' = xy'yx' = x1_Ax' = xx' = 1_A \Longrightarrow xy' \in A^*$. □

Exemples :

1. $\mathbb{Z} = \{1,-1\}$
2. Soit $A = \mathbb{R}^{\mathbb{R}}$ l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. A^* c'est l'ensemble des fonctions qui ne s'annulent jamais, l'inverse de f est $\frac{1}{f}$.

4.2 Règles de calcul dans un anneau

Soit A un anneau. Pour tout triplet (x,y,z) d'éléments de A.

$$x(z-y) = xz - xy$$

en effet :

$$x(z-y) + xy = x[(z-y)+y] = xz$$

ou encore

$$x(z-y) = xz - xy$$

en particulier si $z = y = 0$ on obtient $x.0 = 0.x = 0$.

Théorème 4.1 **Soit A un anneau, alors pour tout couple (a,b) d'éléments de A tels que $ab = ba$ on a :**

$$\forall n \in \mathbb{N}^*,\ (a+b)^n = \sum_{p=0}^{p=n} C_n^p a^p b^{n-p}$$

et

$$a^n - b^n = (a-b)\sum_{k=0}^{k=n-1} a^{n-1-k}b^k.$$

En particulier : $\forall q \in A$, $\forall n \in \mathbb{R}^*$,

$$1 - q^n = (1-q)\sum_{k=0}^{k=n-1} q^k$$

On en déduit que si $q^n = 0$, $1-q$ est inversible et $(1-q)^{-1} = \sum_{k=0}^{k=n-1} q^k$.

4.3 Sous-anneau d'un anneau

Définition 4.3 *Soit A un anneau. On dit qu'une partie B de A est un sous-anneau de A si elle satisfait aux conditions suivantes :*

1. $1 \in B$;
2. $(B,+)$ *est un sous-groupe de* $(A,+)$;
3. B *est stable par la multiplication.*

Définition 4.4 *$(A,+,\times)$ et $(A',+,\times)$ deux anneaux. On dit qu'une application $f : A \longrightarrow A'$ est un morphisme d'anneaux si les conditions suivantes sont satisfaites :*

1. $\forall (x,y) \in A^2, f(x+y) = f(x) + f(y)$;
2. $\forall (x,y) \in A^2, f(x \times y) = f(x) \times f(y)$;
3. $f(1_A) = 1_{A'}$.

On note $\ker f = \{a \in A / f(a) = 0_{A'}\}$.

4.4 Structure d'un corps

Définition 4.5 *On dit qu'un anneau $\mathbb{K}$ est un corps s'il n'est pas réduit à $\{0\}$ et si tout élément non nul de $\mathbb{K}$ est inversible pour le produit.*

Exemples :

1. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des des corps commutatifs.
2. $(\mathbb{Z},+,\times)$ n'est pas un corps.

ℝm Tout corps est intègre, en effet soit a,b tel que $ab = 0$, si $a \neq 0$, alors $a^{-1}ab = a^{-1}0 = 0$, donc $b = 0$.

Sous-corps d'un corps

Définition 4.6 *Soit $\mathbb{K}$ un corps. On dit qu'une partie $\mathbb{K}'$ de $\mathbb{K}$ est un sous-corps de $\mathbb{K}$ si elle stable par les deux lois de compositions sur $\mathbb{K}$ et si, munie des lois induites par celles de $\mathbb{K}$, $\mathbb{K}'$ est corps.*

Proposition 4.2 **$\mathbb{K}'$ est un sous-corps de $\mathbb{K}$ si, et seulement si,**

1. $1 \in \mathbb{K}'$;
2. $\forall a,b \in \mathbb{K}'$, $a-b \in \mathbb{K}'$;
3. $\forall a,b \in \mathbb{K}'$ avec $b \neq 0$, $ab^{-1} \in \mathbb{K}'$.

Exercice d'application : Soit $\mathbb{K}$ l'ensemble des matrices carrées d'ordre 2 réelles de la forme $M(x,y) = \begin{pmatrix} x & y \\ -y & x+y \end{pmatrix}$. Montrer que $(\mathbb{K},+,\times)$ est un corps commutatif.

Solution :

1. $\mathbb{K}$ est une partie non vide de $\mathscr{M}_2(\mathbb{R})$ ($I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{K}$), stable par addition et multiplication, en effet :

   Soit $M(x,y) = \begin{pmatrix} x & y \\ -y & x+y \end{pmatrix}$ et $M(x',y') = \begin{pmatrix} x' & y' \\ -y' & x'+y' \end{pmatrix}$ deux éléments de $\mathbb{K}$

   • $M + M' = \begin{pmatrix} x+x' & y+y' \\ -y-y' & x+x'+y+y' \end{pmatrix} = \begin{pmatrix} X & Y \\ -Y & X+Y \end{pmatrix}$, avec $X = x+x'$ et $Y = y+y'$, donc $M+M' \in \mathbb{K}$

   • De même $MM' = \begin{pmatrix} X & Y \\ -Y & X+Y \end{pmatrix}$ avec $X = xx' - yy'$ et $Y = xy' - yx' + yy'$, donc $MM' \in \mathbb{K}$

2. Montrons que $(\mathbb{K},+,\times)$ est un anneau unitaire commutatif.

   • $(\mathbb{K},+)$ est un sous-groupe de $\mathscr{M}_2(\mathbb{R})$), en effet, soit $M(x,y) = \begin{pmatrix} x & y \\ -y & x+y \end{pmatrix}$ et $M(x',y') = \begin{pmatrix} x' & y' \\ -y' & x'+y' \end{pmatrix}$ deux éléments de $\mathbb{K}$

   $M - M' = \begin{pmatrix} x-x' & y-y' \\ -y+y' & x-x'+y-y' \end{pmatrix} = \begin{pmatrix} X & Y \\ -Y & X+Y \end{pmatrix}$, avec $X = x-x'$ et $Y = y-y'$, donc $M-M' \in \mathbb{K}$ et par conséquent $(\mathbb{K},+)$ est un sous-groupe de $\mathscr{M}_2(\mathbb{R})$).

   • Comme la multiplication des matrices est associative dans $\mathscr{M}_2(\mathbb{R})$), il est de même dans la partie K, de même la multiplication est distributive par rapport à l'addition dans $(K,+,\times)$.

   • On vérifie que $\forall M,M' \in \mathbb{K}$, $MM' = M'M$

   Conclusion : $(\mathbb{K},+,\times)$ est un anneau commutatif unitaire.

3. Pour conclure, il reste à vérifier que chaque élément de $\mathbb{K}^*$ est inversible dans K. Soit $M(a,b) = \begin{pmatrix} a & b \\ -b & a+b \end{pmatrix}$ un élément inversible de K, alors il existe $M'(x,y) = \begin{pmatrix} x & y \\ -y & x+y \end{pmatrix}$ de $\mathbb{K}$ tel que $MM' = I$, ceci est équivalent au système

$$\begin{aligned} ax - by &= 1 \\ bx + (a+b)y &= 0 \end{aligned}$$

$\triangle = a^2 + b^2 + ab$ et on a : $(a,b) \neq (0,0) \Longleftrightarrow a^2 + b^2 + ab > 0$. D'où chaque élément non nul de $\mathbb{K}$ est inversible, donc $(\mathbb{K}, +, \times)$ est un corps commutatif.

Définition 4.7 *Une application f entre deux corps $(\mathbb{K}, +, \times)$ et $(\mathbb{K}', +, \times)$ est un morphisme de corps si et seulement si c'est un morphisme d'anneaux.*

4.5 Corps des fractions d'un anneau

Soit A un anneau, cherchons un corps $\mathbb{K}$ tel que A soit un sous-anneau de $\mathbb{K}$. D'autre part A, sous-anneau de $\mathbb{K}$, devra être dépourvu de diviseurs de zéro. Nous allons voir une construction générale qui permet de construire un corps à partir d'un anneau.
Soit $(A, +, \times)$ un anneau. Sur l'ensemble $A \times A^*$, on définit une relation par :

$$\forall ((a,b),(a',b')) \in A \times A^*, \ (a,b) R (a',b') \Longleftrightarrow a \times b' = a' \times b$$

On vérifie que R est une relation d'équivalence sur $A \times A^*$. On note $\mathbb{K}$ l'ensemble des classes d'équivalences de cette relation. Un élément $k \in \mathbb{K}$ est donc la classe d'un couple $(a,b) \in A \times A^*$, et on note cette classe

$$k = \frac{a}{b}$$

Sur l'ensemble $\mathbb{K}$, on définit deux lois notées $(+)$ et $(\times)$. Soient $k = cl(a,b)$ et $k' = cl(a',b') \in \mathbb{K}$ deux classes d'équivalences de représentants (a,b) et (a',b). On note :

$$k + k' = cl(a \times b' + b \times a', b \times b') \text{ tel que } \frac{a}{b} + \frac{a'}{b'} = \frac{a \times b' + b \times a'}{b \times b'}$$

$$k \times k' = cl(a \times a', b \times b') \text{ tel que } \frac{a}{b} \times \frac{a'}{b'} = \frac{a \times a'}{b \times b'}$$

et on vérifie que ces classes sont indépendantes des représentants $(a,b) \in k$ et $(a',b') \in k'$ choisis.
on montre aussi que $(\mathbb{K}, +, \times)$ est un corps commutatif, appelé corps des fractions de l'anneau $(A, +, \times)$. De plus en peut prolonger l'anneau A dans le corps $\mathbb{K}$, à l'aide de l'injection :

$$\begin{array}{rccc} \phi : & A & \longrightarrow & \mathbb{K} \\ & a & \longmapsto & cl(a,1) \end{array}$$

Théorème 4.2 **Soient $(A, +, \times)$ un anneau intègre. Il existe un corps $(\mathbb{K}, +, \times)$ unique à un isomorphisme près, tel que A est un sous-anneau de $\mathbb{K}$ et tel que**

$$\mathbb{K} = \{ab^{-1} \ / \ a, b \in A, \ \ b \neq 0\}$$

On dit que K est le corps des fractions de la'anneau intègre A.

Exemple : Le corps $(\mathbb{Q}, +, \times)$ c'est le corps de fractions de l'anneau intègre $(\mathbb{Z}, +, \times)$.

••••••••••