Petit pense-bête de définitions à connaître.

I/ Lois

I.1 Applications

Étant donnés deux ensembles E et F, une application f de E vers F se définit par la donnée d'une partie G de $E \times F$ vérifiant

$$\forall x \in E,\ \exists! y \in F \mid (x,\ y) \in G$$

À chaque $x \in E$, est ainsi associé un unique $y \in F$ qu'on appelle l'image de x par f et qu'on note $f(x)$. G s'appelle le graphe de f. En pratique, c'est $f(x)$ que l'on donne « en fonction de x » à l'aide, typiquement, d'une formule, ce qui revient à définir le graphe G en compréhension.

I.2 Opérations

Étant donné un ensemble E, on appelle loi de composition interne (ou opération) sur E toute application $\top$ [1] de $E \times E$ dans E. L'usage est de noter $x \top y$ l'image du couple $(x,\ y)$ à la place de la notation habituelle $\top(x,\ y)$.

Exemples :

- $+$ est une opération sur $\mathbb{N}$: $(p,\ q) \mapsto p + q$; il existe une multitude d'ensembles sur lesquelles on définit une opération notée $+$ et appelée addition...
- Soit E l'ensemble des mots construits sur l'alphabet $\{a, b, c\}$ (un mot=une suite finie de lettres notée par juxtaposition, par exemple ; $aabacca$). La concaténation est une opération sur E. $(m_1,\ m_2) \mapsto m_1 m_2$
- le produit scalaire n'est pas une opération sur l'ensemble des vecteurs géométriques du plan ; le produit vectoriel $(\overrightarrow{x},\ \overrightarrow{y}) \mapsto \overrightarrow{x} \wedge \overrightarrow{y}$ est une opération sur l'ensemble $\overrightarrow{E}$ des vecteurs géométriques de l'espace ;
- La réunion et l'intersection sont des opérations sur l'ensemble $E = \mathcal{P}(\Omega)$ des parties d'un ensemble Ω ;
- La composition est une opération sur l'ensemble σ_{E} des bijections de E dans E (qu'on appelle aussi des permutations) ;

I.3 Lois externes

Étant donnés deux ensembles E et F, on appelle loi de composition externe sur E, toute application $\bullet$ de $F \times E$ dans E. On note aussi usuellement $\lambda \bullet x$ l'image par $\bullet$ du couple $(\lambda,\ x)$.

Exemples :

- $\mathbb{Z} \times \mathbb{R} \to \mathbb{R}$ $(n,\ x) \mapsto n\,x$ est une loi externe sur $\mathbb{R}$;
- $\mathbb{R} \times \mathbb{R}^I \to \mathbb{R}^I$ $(\lambda,\ f) \mapsto \lambda\, f$ est une loi externe sur l'ensemble des applications de I dans $\mathbb{R}$;

En pratique, les lois externes ne sont pas dénotées ; on abrège $\lambda \bullet x$ en $\lambda\, x$.

II/ Groupes

II.1 Définition

Un groupe est un couple $(G,\ \top)$ formé d'un ensemble G et d'une opération $\top\ :\ G \times G \to G$ vérifiant les axiomes suivants :
G1 associativité : $\forall (a,\ b,\ c) \in G^3,\ \ (a \top b) \top c = a \top (b \top c)$;
G2 existence d'un élément neutre : $\exists\ e \in G \mid \forall x \in G,\ \ x \top e = e \top x = x$;
G3 symétricité [2] :
$\forall x \in G,\ \exists\ x' \in G \mid x \top x' = x' \top x = e$. On dit que x' est le symétrique de x (dans G relativement à l'opération $\top$.

Si de plus, on a la propriété :
G4 commutativité : $\forall (x,\ y) \in G^2,\ \ x \top y = y \top x$
on dit que le groupe $(G,\ \top)$ est commutatif (ou abélien).

Dans chaque exemple de groupe, il existe une notation particulière (et parfois une appellation particulière) pour le symétrique d'un élément.

Exemples :

- $(\mathbb{N},\ +)$ n'est pas un groupe (il manque G3) mais $(\mathbb{Z}, +)$ est un groupe commutatif ; le symétrique de $x \in \mathbb{Z}$ relativement à $+$ se note $-x$ et s'appelle l'opposé de x ;
- $(\sigma_E,\ \circ)$ est un groupe, non commutatif dès que $\mathrm{card}(E) > 2$; le symétrique de $f \in \sigma_E$ relativement à $\circ$ se note f^{-1} et s'appelle la réciproque de f ;
- $(\mathbb{R}^*, \times)$ est un groupe commutatif mais pas $(\mathbb{R},\ _times)$; le symétrique de $x \in \mathbb{R}^*$ se note x^{-1} (ou $\frac{1}{x}$) et s'appelle l'inverse de x ;
- $(\mathfrak{M}_n(\mathbb{K}), \times)$ n'est pas un groupe ;
- $(GL_n(\mathbb{K}), \times)$ est un groupe, non commutatif dès que $n > 1$;

1. Lire $\top$ « truc ».
2. Néologisme non standard, mais le français est assez inapte dans ce domaine.

II.2 Sous-groupes

Étant donné un groupe $(G,\ \top)$, un sous-groupe est un groupe $(H,\ \top)$ avec $\emptyset \neq H \subset G$ et le même élémet neutre ; autrement dit, $(H,\ \top)$ est un sous-groupe de $(G,\ \top)$ ssi :
– $\top$ est une opération sur H : $\forall (x,\ y) \in H^2,\ x \top y \in H$; on dit que H est stable par $\top$;
– $e \in H$;
– $\forall x \in H,\ x' \in H$.

Exemples :

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$;
- $(O(n), \times)$ est un sous-groupe de $(\mathsf{GL}_n(\mathbb{R}), \times)$;
- Soit $n \in \mathbb{N}^*$ et $\mathbb{U}_n$ l'ensemble des racines n-ième de l'unité ; $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{C},\ \times)$;

II.3 Morphisme de groupes

Étant donnés deux groupes $(G,\ \top)$ et $(\Gamma,\ *)$, on appelle morphisme (ou homomorphisme) de $(G,\ \top)$ vers $(\Gamma,\ *)$ toute application $\phi\ :\ G \to \Gamma$ vérifiant :

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

Exemples :

- $n \mapsto 2\,n$ est un morphisme de $(\mathbb{Z},\ +)$ vers lui-même ;
- $\ln$ est un morphisme de $(\mathbb{R}^{*+}, \times)$ vers $(\mathbb{R}, +)$;
-

III/ Anneaux

III.1 Définition

Un anneau est un triplet $(A,\ \top,\ *)$ formé d'un ensemble G et de deux opérations $\top$ et $*$ sur A vérifiant les axiomes suivants :
A1 associativité de $\top$: $\forall (a,\ b,\ c) \in A^3,\ (a \top b) \top c = a \top (b \top c)$;
A2 existence d'un élément neutre de $\top$: $\exists\ e \in A \mid \forall x \in A,\ x \top e = e \top x = x$;
A3 symétricité de $\top$: $\forall x \in A,\ \exists\ x' \in A \mid x \top x' = x' \top x = e$.
A4 commutativité de $\top$: $\forall (x,\ y) \in A^2,\ x \top y = y \top x$
autrement dit $(A,\ \top)$ est un groupe commutatif ;
A5 associativité de $*$: $\forall (a,\ b,\ c) \in A^3,\ (a\ *\ b) * c = a\ *\ (b\ *\ c)$;
A6 existence d'un neutre de $*$: $\exists\ u \in A \setminus \{e\} \mid \forall\, x \in A,\ u\ *\ x = x\ *\ u = x$;
A8 distributivité de $*$ par rapport à $\top$: $\forall (x,\ y,\ z) \in A^3,\ x\ *\ (y \top z) = (x\ *\ y) \top (x\ *\ z)$;
si de plus, on a la propriété :
A9 commutativité de $*$: $\forall\,(x,\ y) \in A^2,\ x\ *\ y = y\ *\ x$
on dit que l'anneau $(A,\ \top,\ *)$ est commutatif.

un anneau $(A,\ \top,\ *)$ est dit intègre si et seulement si : $\forall (x,\ y) \in A^2,\ (x\ *\ y = e\ \Rightarrow\ x = e$ ou $y = e)$.

Exemples :

- $(\mathbb{Z},\ +,\ \times)$ est un anneau commutatif intègre ;
- $(\mathfrak{M}_n(\mathbb{K}),\ +,\ \times)$ est un anneau, non commutatif dès que $n \geqslant 2$ et non intègre ;
- $(\mathbb{K}[X],\ +,\ \times)$ est un anneau commutatif intgre ;
- $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$ car il n'est pas stable par produit ;
- si E est un ensemble, $\big(\mathcal{P}(E), \cup, \cap\big)$ n'est pas un anneau.

III.2 Idéaux

Étant donné un anneau $(A,\ \top,\ *)$, un idéal de A est une partie J de A vérifiant :
I1 $(J,\ \top)$ est un sous-groupe de $(A,\ \top)$;
I2 $\forall x \in J,\ \forall a \in A,\ a\ *\ x \in A$

Exemples :

- $2\,\mathbb{Z}$ alias l'ensemble des relatifs pairs est un idéal de l'anneau $(\mathbb{Z},\ +,\ \times)$;
- $X\,\mathbb{K}[X]$ alias l'ensemble des polynômes admettant 0 pour racine, est un idéal de l'anneau $(\mathbb{K}[X],\ +,\ \times)$.

IV/ Corps

Un corps est un triplet $(K, \top, *)$ formé d'un ensemble K et de deux opérations $\top$ et $*$ sur K vérifiant les axiomes suivants :
K1 associativité de $\top$: $\forall (a, b, c) \in K^3,\ (a \top b) \top c = a \top (b \top c)$;
K2 existence d'un élément neutre de $\top$: $\exists\, e \in K \mid \forall x \in K,\ x \top e = e \top x = x$;
K3 symétricité de $\top$: $\forall x \in K,\ \exists\, x' \in K \mid x \top x' = x' \top x = e$.
K4 commutativité de $\top$: $\forall (x, y) \in K^2,\ x \top y = y \top x$
autrement dit $(K, \top)$ est un groupe commutatif ;
K5 associativité de $*$: $\forall (a, b, c) \in K^3,\ (a * b) * c = a * (b * c)$;
K6 existence d'un neutre de $*$: $\exists\, u \in K \setminus \{e\} \mid \forall\, x \in K,\ u * x = x * u = x$;
K7 symétricité de $*$: $\forall x \in K \setminus \{e\}, \exists\, 'x \in K \mid x * 'x =' x * x = u$;
autrement dit, $(K, *)$ est un groupe ;
K8 distributivité de $*$ par rapport à $\top$: $\forall (x, y, z) \in A^3,\ x * (y \top z) = (x * y) \top (x * z)$;
autrement dit, un corps est un anneau dans lequel tout élément distinct du neutre de la première opération à un symétrique pour la seconde opération.
si de plus, on a la propriété :
K9 commutativité de $*$; : $\forall\, (x, y) \in K^2,\ x * y = y * x$
on dit que le corps $(K, \top, *)$ est commutatif.

Exemples :

- $(\mathbb{Z}, +, \times)$ n'est pas un corps (il manque K7) ;
- $(\mathbb{Q}, +, \times)$ est un corps commutatif ;
- $(\mathbb{R}, +, \times)$ est un corps commutatif ;
- $(\mathbb{C}, +, \times)$ est un corps commutatif ;
- $(\mathfrak{M}_n(\mathbb{R}), +, \times)$ n'est pas un corps (il manque K7) ;

Convention : dans la pratique, la première opération d'un corps est toujours notée $+$ et son neutre 0, et la seconde opération par juxtaposition et son neutre 1 (comme dans les corps de nombres).

IV.1 $\mathbb{R}$

Le corps des réels possède une structure algébrique spéciale ; c'est un *corps commutatif totalement ordonné*. Cela signifie qu'il existe sur $\mathbb{R}$ un relation d'ordre total $(\leqslant)$ compatible avec les opérations de la structure de corps.

On a besoin de quelques définitions :

1. une relation binaire sur un ensemble E est une partie $\mathcal{R}$ de $E \times E$. Soit (x, y) un couple d'éléments de E ; on dit que x est en relation avec y par la relation $\mathcal{R}$ et on écrit $x\mathcal{R}y$ ssi $(x, y) \in \mathcal{R}$. Pratiquement toujours $\mathcal{R}$ est définie en compréhension.
   Exemples :
   - Sur $\mathbb{N}$, $a\mathcal{R}b$ ssi il existe $c \in \mathbb{N}$ tel que $b = a + c$; chacun a compris que $\mathcal{R} = \leqslant$.
   - Soit $n \in \mathbb{N},\ n \geqslant 2$ fixé. Sur $\mathbb{Z}$, $a\mathcal{R}b$ ssi il existe $k \in \mathbb{Z}$ tel que $b - a = k\,n$; chacun a reconnu la relation de congruence modulo n ; on note d'ailleurs $a \equiv b \bmod n$.
   - Sur $\mathcal{P}(E)$, ensemble des parties de l'ensemble E, $A\mathcal{R}B$ ssi $(\forall x \in E,\ x \in A \Rightarrow x \in B)$; chacun a reconnu la relation d'inclusion $\subset$.
2. une relation d'ordre sur un ensemble E est une relation binaire $\mathcal{R}$ vérifiant les 3 axiomes :
   R réflexivité : $\forall x \in E,\ x\mathcal{R}x$;
   AS antisymétrie : $\forall (x, y) \in E^2, (x\mathcal{R}y)$ et $(y\mathcal{R}x) \Rightarrow x = y$;
   T transitivité ; $\forall (x, y, z) \in E^3,\ (x\mathcal{R}y)$ et $(y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.
   Si de plus, pour tout $(x, y) \in E^2,\ x\mathcal{R}y$ ou $y\mathcal{R}x$, on dit que l'ordre est total.
   Exemples :
   - $\leqslant$ sur $\mathbb{N}$ est une relation d'ordre total sur $\mathbb{N}$.
   - $\subset$ est une relation d'ordre non total sur $\mathcal{P}(E)$.

L'ordre sur $\mathbb{R}$ est défini par la donnée du sous-ensemble R^+ : $x \leqslant y$ ssi il existe $z \in \mathbb{R}^+$ tel que $y = x + z$ (autrement dit $y - x \in \mathbb{R}^+$.
La relation $\leqslant$ est dite compatible avec la structure de corps au sens suivant :
– $\forall (x, y, z) \in \mathbb{R}^3,\ (x \leqslant y \Rightarrow x = z \leqslant y + z)$;
– $\forall (x, y, z) \in \mathbb{R}^3,\ (x \leqslant y)$ et $(0 \leqslant z) \rightarrow x\,z \leqslant y\,z$.

V/ Espaces vectoriels

V.1 Définitions

Étant donné un corps commutatif $\mathbb{K}$, un espace vectoriel sur $\mathbb{K}$ est un triplet $(E, \top, \bullet)$ formé d'un ensemble E, d'une opération $\top$ sur E et d'une loi externe $\bullet$: $\mathbb{K} \times E \rightarrow E$ sur E vérifiant les axiomes suivants :
E1 associativité : $\forall (a, b, c) \in E^3,\ (a \top b) \top c = a \top (b \top c)$;
E2 existence d'un élément neutre : $\exists\, e \in E \mid \forall x \in E,\ x \top e = e \top x = x$;

E3 symétricité : $\forall x \in E,\ \exists\, x' \in E \mid x \top x' = x' \top x = e$. On dit que x' est le symétrique de x (dans E relativement à l'opération $\top$.

E4 commutativité : $\forall (x,\, y) \in E^2,\ x \top y = y \top x$

autrement dit $(E,\ \top)$ est un groupe commutatif ;

E5 $\forall (\lambda,\, x,\, y) \in \mathbb{K} \times E \times E,\ \lambda \bullet (x \top y) = (\lambda \bullet x) \top (\lambda \bullet y)$;

E6 $\forall (\lambda,\, \mu,\, x) \in \mathbb{K} \times \mathbb{K} \times E,\ (\lambda + \mu) \bullet x = (\lambda \bullet x) \top (\mu \bullet x)$;

E7 $\forall (\lambda,\, \mu,\, x) \in \mathbb{K} \times \mathbb{K} \times E,\ (\lambda \mu) \bullet x = \lambda \bullet (\mu \bullet x)$;

E8 $\forall x \in E,\ 1 \bullet x = x$.

Convention : en pratique l'opération d'un espace vectoriel est toujours notée additivement, soit $+$, mais attention ce n'est pas le même $+$ que celui de $\mathbb{K}$! Et la loi externe est toujours notée par juxtaposition, mais attention ce n'est pas la seconde opération de $\mathbb{K}$! ! Faire l'effort de réécrire les axiomes de définition de la structure avec ces conventions.

Les éléments d'un espace vectoriel sont appelés génériquement des vecteurs.

On appelle combinaison linéaire de deux vecteurs x et y de E, tout vecteur de la forme $\lambda\, x + \mu\, y$ avec $(\lambda,\, \mu) \in \mathbb{K}^2$. La définition se généralise à des combinaisons linéaires de n vecteurs. Dans un espace vectoriel, c'est l' « opération » importante, qu'il importe de percevoir.

Exemples :

- $(\mathbb{K},\, +,\, \times)$ est un espace vectoriel sur $\mathbb{K}$;
- $(\mathbb{C},\, +,\, \times)$ est un espace vectoriel sur $\mathbb{R}$;
- $(\mathbb{K}^n,\, +,\, \cdot)$ est un espace vectoriel sur $\mathbb{K}$;
- $(\mathfrak{M}_{m \times n}(\mathbb{K})$ est un espace vectoriel sur $\mathbb{K}$;
- $(\mathbb{K}_n[X],\, +,\, \times)$ est un espace vectoriel sur $\mathbb{K}$.

V.2 Sous-espace vectoriel

Étant donné un espace vectoriel sur $\mathbb{K}$ $(E,\, +,\, \cdot)$, un sous-espace vectoriel de E est une partie non vide F de E stable par combinaisons linéaires, c-à-d vérifiant :

$$\forall (\lambda,\, \mu) \in \mathbb{K}^2,\ \forall (x,\, y) \in F^2,\ \lambda\, x + \mu\, y \in F$$

V.3 Morphismes d'espaces vectoriels

Un morphisme du $\mathbb{K}$-espace vectoriel $(E,\, +,\, \cdot)$ vers le $\mathbb{K}$-espace vectoriel $(\widehat{E},\, \hat{+},\, \hat{\cdot})$ est une application $\phi\ :\ E \to \widehat{E}$ vérifiant :

– $\forall (x,\, y) \in E^2,\ \phi(x + y) = \phi(x) \,\hat{+}\, \phi(y)$;

– $\forall (\lambda,\, x) \in \mathbb{K} \times E,\ \phi(\lambda \cdot x) = \lambda \,\hat{\cdot}\, \phi(x)$

Les morphismes d'espaces vectoriels sont bien connus sous le nom d'applications linéaires...

V.4 Produit

Étant donnés deux espaces vectoriels $(E,\, +,\, \cdot)$ et $(\widehat{E},\, \hat{+},\, \hat{\cdot})$, on appelle produit (ou application bilinéaire) sur E à valeurs dans $\widehat{E}$, toute application $\phi\ :\ E \times E \to \widehat{E}$ vérifiant :

– $\forall x \in E,\ \phi(x,\, \bullet)$ est linéaire de E vers $\widehat{E}$;

– $\forall y \in E,\ \phi(\bullet,\, y)$ est linéaire de E vers $\widehat{E}$.

Exemples :

- $(x,\, y) \mapsto x\, y$ est un produit sur $(\mathbb{R},\, +,\, \times)$;
- $(\overrightarrow{x},\, \overrightarrow{y}) \mapsto \overrightarrow{x} \cdot \overrightarrow{y}$ est un produit sur $\overrightarrow{E}$;
-

VI/ ALGÈBRE

VI.1 Définition

Étant donné un corps $\mathbb{K}$, une algèbre sur $\mathbb{K}$ est un quadruplet $(\mathcal{A},\, \top,\, *,\, \bullet)$ formé d'un ensemble $\mathcal{A}$, de deux opérations $\top$ et $*$ sur $\mathcal{A}$, d'une loi externe $\bullet$ vérifiant les axiomes :

A1 $(\mathcal{A},\, \top,\, *)$ est un anneau ;

A2 $(\mathcal{A},\, \top,\, \bullet)$ est un $\mathbb{K}$-espace vectoriel ;

A3 $(x,\, y) \mapsto x * y$ est un produit sur $\mathcal{A}$, ce qui équivaut (étant donné A1 et A2) à :

$$\forall (\lambda,\, x,\, y) \in \mathbb{K} \times E \times E,\ (\lambda \bullet x) * y = x * (\lambda \bullet y) = \lambda \bullet (x * y)$$

si de plus l'anneau $(\mathcal{A},\, \top,\, *)$ est intègre, on dit que l'algèbre est intègre.

Exemples :

- $(\mathbb{R},\, +,\, \times,\, \times)$ est une $\mathbb{R}$-algèbre intègre ;

- $(\mathfrak{M}_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre non intègre ;
- $(\mathbb{K}[X], +, \times, \cdot)$ est une $\mathbb{K}$-algèbre intègre ;
- Soit $\mathcal{C}^0(I, \mathbb{R})$ l'ensemble des applications numériques continues sur I ; $(\mathcal{C}^0(I, \mathbb{R}), +, \times, \cdot)$ est une $\mathbb{R}$-algèbre non intègre.