Compléments : Ensembles, Groupes et Anneaux

I) Ensembles et Applications

Définition 1 Soit E et F deux ensembles, et $f : E \to F$ une application.

f injective $\iff \forall x_1, x_2 \in E, \quad f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$

f surjective $\iff \forall y \in F, \exists x \in E / \quad y = f(x)$

f bijective $\iff$ f injective et surjective $\iff \forall y \in F, \exists! x \in E / \quad y = f(x)$

Définition 2 E fini de cardinal $n \iff \exists f : \{1, \dots, n\} \to E$ bijective.

On peut numéroter les éléments de E, grâce à une partie finie de $\mathbb{N}$. Une partie finie de $\mathbb{N}$ est une partie qui admet un plus grand élément.

Théorème 1 Soit $f : E \to F$. Si Card $E =$ Card $F < \infty$, alors

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective.}$$

Propriété 2 Soit A et B deux parties finies d'un ensemble E.

$$\text{Card}\,(A \cup B) = \text{Card}\ A + \text{Card}\ B - \text{Card}\,(A \cap B)$$

La suite de ce chapitre est *hors programme* : les notions de groupe et d'anneau permettent surtout de structurer ses connaissances et de mieux comprendre certaines propriétés d'objets au programme : $\mathscr{L}(E)$, GL_n, $\mathbb{R}[X]$, etc...

II) Groupes

A) Définition des objets

Définition 3 (groupe) Un ensemble G muni d'une loi de composition interne $*$ est un *groupe* si

la loi $*$ est associative : $\forall (x, y, z) \in G^3, \quad (x * y) * z = x * (y * z)$

la loi $*$ possède un élément neutre e : $\forall x \in G \qquad x * e = e * x = x$

tout élément a un inverse : $\forall x \in G, \exists y \in G \quad x * y = y * x = e$

Notation 1 Additive : $(G, +)$, le neutre est noté 0_G, et l'inverse de x est $-x$.

Multiplicative : $(G, *)$; le neutre est noté 1_G, et l'inverse de x est x^{-1}.

Définition 4 Lorsque la loi est commutative, le groupe est dit commutatif ou abélien.

Exemple 1

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$, $\mathscr{M}_n(\mathbb{K})$, $\mathscr{F}(\mathbb{R}, \mathbb{R})$ avec $+$.
- $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ avec $\times$.
- $\mu_n = \{e^{2ik\pi/n} / k \in \mathbb{Z}\}$, $\mathbb{U} = \{z \in \mathbb{C} / |z| = 1\}$ avec $\times$.
- $\mathscr{O}_n(\mathbb{R})$, $\mathcal{GL}_n(\mathbb{K})$ avec le produit matriciel : non commutatif !

Contre-exemple 2 Pas des groupes : $(\mathscr{F}(\mathbb{R}, \mathbb{R}), \times)$, $(\mathscr{F}(\mathbb{R}, \mathbb{R}), \circ)$, $(\mathscr{M}_n(\mathbb{K}), \times)$.

Remarque 1 La plupart du temps, pour prouver que G est un groupe, on prouve que c'est un sous-groupe d'un groupe classique. La propriété 3 et la liste de l'exemple 1 sont donc fondamentales.

B) Sous-groupes

Définition 5 (sous-groupe) Une partie H d'un groupe $(G,*)$ est un *sous-groupe* de $(G,*)$ si $(H,*)$ est un groupe.

Propriété 3 $H \subset G$ est un *sous-groupe* de $(G,*)$ si et seulement si $\forall (x,y) \in H^2 \quad x * y^{-1} \in H$ et $H \neq \emptyset$.

On teste d'un même coup la stabilité par la loi $*$ et par passage à l'inverse.

Exemple 3
- Relever les différents sous-groupes de $(\mathbb{C},+)$ puis de $(\mathbb{C}^*,\times)$ dans l'exemple 1.
- Exemples de sous-groupes de $GL_2(\mathbb{R})$: groupe des rotations, groupe des isométries (applications qui conserve les distances), etc...

Définition 6 (ordre d'un élément) Soit $a \in G$ groupe. L'*ordre* de a est le cardinal du sous-groupe engendré par a, lorsque celui-ci est fini :

$$\text{Card}\left(\{a^n / n \in \mathbb{Z}\}\right)$$

Dès que l'on a un élément, on a un sous-groupe qui vient naturellement avec, $< a >= \{a^n / n \in \mathbb{Z}\}$. C'est le plus petit sous-groupe contenant a.

C) Morphismes

Après les objets (ici les groupes), on s'intéresse aux applications entre ces objets qui sont « compatibles »avec la structure de groupe.

Définition 7 (morphisme) Soit $(G,*)$ et $(G',\star)$ deux groupes. Une application $f : G \to G'$ est un *morphisme de groupes* si

$$\forall (x,y) \in G^2, \qquad f(x*y) = f(x) \star f(y)$$

Conséquence 1 $f(e_G) = e_{G'}$.

Exemple 4
- La multiplication par 2 de $(\mathbb{Z},+)$ dans lui-même (ou de $(\mathbb{R},+)$ dans lui-même).
- $\ln : (\mathbb{R}_+^*,\times) \to (\mathbb{R},+)$, et sa fonction réciproque, exp.
- Le déterminant sur $GL_n(\mathbb{K})$: $\det : GL_n(\mathbb{K}) \to \mathbb{K}$.

Propriété 4 Soit $f : G \to G'$ un morphisme de groupes.
Si $H' \subset G'$ sous-groupes de G', alors $f^{-1}(H')$ est un sous-groupe de G.
Si $H \subset G$ sous-groupe de G, alors $f(H)$ sous-groupe de G'.

Le morphisme f préserve la structure de groupe...
La composée de deux morphismes est un morphisme. L'inverse d'un morphisme est un morphisme.

Définition 8 (noyau) Soit $f : G \to G'$ un morphisme de groupes. On appelle *noyau* de f le sous-groupe

$$\text{Ker } f = f^{-1}(\{e_{G'}\}) = \{g \in G / f(g) = e_{G'}\}$$

Propriété 5 f injective si et seulement si $\text{Ker } f = \{e_G\}$.

Démonstration. On peut se contenter de tester l'injectivité en un seul point (par exemple $e_{G'}$) puisque f est compatible avec la loi $*$.

$\boxed{\Longrightarrow}$ Supposons f injective. $\forall x \in G, \quad (x \in \text{Ker } f \Rightarrow f(x) = e_{G'} = f(e_G) \Rightarrow x = e_G)$. Donc $\text{Ker } f = \{e_G\}$.

$\boxed{\Longleftarrow}$ Supposons Ker $f = \{e_G\}$. On utilise la structure de groupe qui permet de « tout passer d'un seul coté »pour se ramener à l'élément neutre. $\forall (x,y) \in G^2$,

$$[f(x) = f(y)] \Rightarrow [f(x) * f(y)^{-1} = f(x * y^{-1}) = e_{G'}] \Rightarrow [x * y^{-1} \in \text{Ker } f = \{e_G\}] \Rightarrow [x * y^{-1} = e_G] \Rightarrow [x = y]$$

Donc f injective.

□

Définition 9 (image) Soit $f : G \to G'$ un morphisme de groupe. Le sous-groupe $f(G)$ de G' est appelée l'*image* de f, et est notée Im f.

La structure de groupe n'intervient pas dans la construction de l'image...

Propriété 6 f surjective si et seulement si Im $f = G'$

Puisqu'il n'y a rien de propre aux groupes, la propriété est vraie aussi au I et ne fait pas intervenir les groupes.

III) Anneaux

A) Définition des objets

Définition 10 (anneau) Un ensemble A muni de deux lois de composition interne $+$ et $\times$ est un *anneau* si

- $(A, +)$ est un groupe commutatif ;
- La loi $\times$ est associative ;
- La loi $\times$ est distributive par rapport à $+$: $\forall (x,y,z) \in A^3$, $\begin{cases} x \times (y+z) = x \times y + x \times z \\ (y+z) \times x = y \times x + z \times x \end{cases}$.

Les anneaux que nous croiseront seront toujours muni d'un élément neutre 1_A pour le produit. Ils sont dit « unitaires ».

Définition 11 Lorsque le produit est commutatif, A est dit commutatif.

Exemple 5
- Les ensembles de nombres muni de leurs opérations naturelles.
- $\mathbb{K}[X]$.
- $\mathscr{F}(I, \mathbb{R})$ muni du produit $(f.g)(x) = f(x)g(x)$ est un anneau commutatif. Plus généralement, les fonctions à valeur dans un anneau forment un anneau.
- $\mathscr{M}_n(\mathbb{K})$ est anneau non commutatif.

Contre-exemple 6 $\mathscr{F}(\mathbb{R}, \mathbb{R})$ muni de $\circ$ est n'est pas un anneau, car la distributivité n'est pas vérifiée : $f \circ (g + h)$ ne se développe pas.

Remarque 2 Tout comme pour les groupes, on montre le plus souvent qu'un ensemble est un sous-anneau d'un anneau classique, la propriété 7 et la liste ci-dessus sont donc fondamentales.

Définition 12 (anneau intègre) Un anneau A est dit intègre si $\forall (x,y) \in A^2 \quad xy = 0 \Longrightarrow x = 0$ ou $y = 0$.

Exemple 7 $\mathbb{Z}$ ou $\mathbb{K}[X]$ sont intègres. Par contre $(\mathscr{F}(I, \mathbb{R}), +, \times)$ n'est pas intègre [1] : il suffit de considérer f nulle sur une partie de I et g nulle sur le reste de I, mais toutes deux différente de la fonction identiquement nulle.

1. Dès que $I \neq \{a\}$

B) Sous-anneaux

Définition 13 (sous-anneau) Une partie B d'un anneau $(A, +, \times)$ est un *sous-anneau* de A si $(B, +, \times)$ est un anneau (pas nécessairement unitaire).

Propriété 7 $B \subset A$ est un sous-anneau de A si et seulement si $\begin{cases} B \neq \emptyset \\ \forall (x,y) \in B, \qquad x - y \in B \quad \text{et} \quad xy \in B \end{cases}$

C) Morphismes

Définition 14 (morphisme) Soit A et A' deux anneaux. Une application $f : A \to A'$ est un *morphisme d'anneaux* si

$$\forall (x,y) \in A^2 \qquad f(xy) = f(x)f(y) \qquad \text{et} \qquad f(x+y) = f(x) + f(y)$$

Propriété 8 Soit $f : A \to A'$ un morphisme d'anneaux.
Si $B' \subset A'$ sous-anneaux de A', alors $f^{-1}(B')$ est un sous-anneau de A.
Si $B \subset A$ sous-anneau de A, alors $f(B)$ sous-anneau de A'.

Le morphisme f préserve la structure d'anneau...
La composée de deux morphismes est un morphisme. L'inverse d'un morphisme est un morphisme.

Définition 15 (noyau) Soit $f : A \to A'$ un morphisme d'anneaux. On appelle *noyau* de f le sous-anneau

$$\text{Ker } f = f^{-1}(\{0_{A'}\}) = \{g \in A / f(g) = 0_{A'}\}$$

Propriété 9 f injective si et seulement si Ker $f = \{0_A\}$.

Pour l'image, la définition et la propriété est complètement identique à celle pour les groupes...

IV) Et ensuite

Vous remarquerez que vous pouvez écrire un paragraphe identique pour les espaces vectoriels, sous-espace vectoriel et morphismes d'espaces vectoriels – appelés applications linéaires. Nous le reverrons dans le chapitre d'algèbre linéaire, ces notions seront pour le coup complètement au programme et à maîtriser parfaitement.