Chapitre 1 : structures algébriques

Introduction

L'ensemble $\mathbb{R}$ des nombres réels que vous connaissez bien (mais aussi l'ensemble $\mathbb{Q}$ des nombres rationnels, ou l'ensemble $\mathbb{C}$ des nombres complexes) possède une structure algébrique extrêmement riche).

→ on peut additionner deux nombres réels. La loi d'addition, notée "+", possède plusieurs propriétés remarquables :

$(\mathbb{R},+,0)$ est un groupe :
- elle est associative : $(x+y)+z = x+(y+z)$ quels que soient $x,y,z \in \mathbb{R}$.
- elle admet un élément neutre : $x+0 = x = 0+x$ quel que soit $x \in \mathbb{R}$.
- quel que soit $x \in \mathbb{R}$, $x+(-x) = 0 = (-x)+x$.

$(\mathbb{R},+,0)$ est un groupe abélien :
- elle est commutative : $x+y = y+x$ quels que soient $x,y \in \mathbb{R}$.

→ on peut multiplier deux nombres réels. La loi de multiplication, notée "×" ou simplement "·", possède également des propriétés remarquables :

$(\mathbb{R},+,0,\times,1)$ est un anneau :
- elle est associative : $(x\times y)\times z = x\times(y\times z)$ quels que soient $x,y,z \in \mathbb{R}$.
- elle admet un élément neutre : $x\times 1 = x = 1\times x$ quel que soit $x \in \mathbb{R}$.
- elle est distributive (à droite et à gauche) par rapport à l'addition : $x\times(y+z) = (x\times y)+(x\times z)$ et $(y+z)\times x = (y\times x)+(z\times x)$.

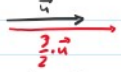
$(\mathbb{R},+,0,\times,1)$ est un anneau commutatif :
- elle est commutative : $x\times y = y\times x$ quel que soient $x,y \in \mathbb{R}$

$(\mathbb{R},+,0,\times,1)$ est un corps :
- quel que soit $x \in \mathbb{R}\setminus\{0\}$, $x\times\frac{1}{x} = 1 = \frac{1}{x}\times x$.

Dans ce premier chapitre, nous allons définir les notions de **groupe**, d'**anneau**, et de **corps**, et voir plusieurs exemples.

⚠ L'ensemble $\mathbb{R}^2$ des vecteurs du plan (et plus généralement $\mathbb{R}^n$) possède aussi une loi d'addition qui en fait un groupe abélien :

Mais il n'y a pas de manière naturelle de multiplier deux vecteurs. Néanmoins, on peut multiplier un vecteur par un scalaire (c-à-d un nombre réel) :



Cette loi de multiplication externe possède des propriétés sur lesquels nous reviendrons dans le Chapitre 2, et qui font de $\mathbb{R}^2$ un **espace vectoriel**.

Au début de ce cours, vous allez rencontrer beaucoup de nouvelles définitions. Il est indispensable de les connaître et d'apprendre son cours avant chaque séance de TD.

Lois de composition internes

1.1 Définition : une **loi de composition (interne)** sur un ensemble E est une application $E\times E \to E$.

1.2 ⚠ Pour les lois de composition on utilise en général la notation **opérationnelle**. Autrement dit, l'application d'une loi $*$ à un couple (x,y) s'écrit $x*y$.
La notation opérationnelle est, comme son nom l'indique, celle qu'on utilise pour écrire des opérations sur une feuille de papier.
La notation **fonctionnelle** est utilisée :
- en analyse : on note $f(x,y)$ pour la valeur de la fonction de deux variables f évaluée en (x,y).
- par certaines calculatrice graphiques : on tappe alors $+(3,5)$ pour calculer la somme de 3 et 5.
- pour les applications linéaires (que nous verrons plus tard).

pour calculer la somme de $\vec{3}$ et $\vec{5}$.
- pour les applications linéaires (que nous verrons plus tard).

1.3 Exemples :
- la somme (addition) et le produit (multiplication) définissent des lois de composition sur les ensembles qui suivent : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- la soustraction définit une loi de composition sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, mais pas sur $\mathbb{N}$.
- la division définit une loi de composition sur $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ et $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
- Soit X un ensemble. On note $E = X^X$ l'ensemble des applications $X \to X$. La composition des applications définit une loi de composition sur E. On rappelle que pour $f, g : X \to X$, leur composée $f \circ g : X \to X$ est définie par $f \circ g(x) = f(g(x))$.
- la somme et le produit des matrices définissent des lois de composition sur l'ensemble $M_n(A)$ des matrices de taille $n \times n$ à coefficients dans $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

1.4 Construction : soit $(E, *)$ un ensemble muni d'une loi de composition interne. Pour tout ensemble X, on munit l'ensemble E^X des applications $X \to E$ de la loi $*$ définie comme suit :
Pour $f, g : X \to E$ et $x \in X$, on pose $(f * g)(x) = f(x) * g(x)$.

Par exemple, l'ensemble des suites à valeurs dans E (cas où $X = \mathbb{N}$) ou celui des fonctions d'une variable réelle à valeurs dans E (cas où $X = \mathbb{R}$) héritent tous deux des lois de E.

1.5 Définition : soit $* : E \times E \to E$ une loi de composition interne.
(a) On dit que $*$ est **associative** si : $\forall x, y, z \in E$, $(x * y) * z = x * (y * z)$.
(b) On dit que $*$ est **commutative** si : $\forall x, y \in E$, $x * y = y * x$.
(c) On dit que $e \in E$ est un **élément neutre** pour $*$ si : $\forall x \in E$, $x * e = x = e * x$.

1.6 Exemples et contre-exemples :
- dans tous les exemples de **1.3** les lois de somme et de produit sont associatives et possèdent un élément neutre. → à faire en exercice.
- la loi de soustraction n'est pas associative : $(2-3)-1 = -2 \neq 0 = 2-(3-1)$.
- la loi de division n'est pas associative non plus : $(4 \div 2) \div 2 = 1 \neq 4 = 4 \div (2 \div 2)$.
- la composition des applications $X \to X$ est associative et l'identité est un élément neutre.
- les lois qui suivent ne sont pas commutatives :
  - → la soustraction : $2-1 = 1 \neq -1 = 1-2$.
  - → le produit des matrices : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$
  - → la composition des applications : $X = \mathbb{R}$, $f(x) = x^2$ et $g(x) = \exp(x)$.
    $f \circ g(x) = \exp(x)^2 = \exp(2x) \neq \exp(x^2) = g \circ f(x)$.
  - → la division : $2 \div 1 = 2 \neq \frac{1}{2} = 1 \div 2$.
- les autres lois de **1.3** sont commutatives.

1.7 Proposition [unicité de l'élément neutre] : soit $e_1, e_2 \in E$ des éléments neutres pour une loi $* : E \times E \to E$. Alors $e_1 = e_2$.

Démonstration : $e_1 = e_1 * e_2 = e_2$.
(e_2 est un élément neutre ; e_1 est un élément neutre)
□

1.8 Proposition : si une loi $* : E \times E \to E$ est associative / commutative / possède un élément neutre, alors il en va de même pour la loi donnée par la Construction **1.4**.

Démonstration : laissée en exercice. □

1.9 Notation : Pour une loi $*$ associative, il n'est pas nécessaire de mettre des parenthèses lorsqu'on applique la loi de multiples fois. La notation $x*y*z$ n'est pas ambigue puisque $(x*y)*z = x*(y*z)$.

Groupes

On fixe désormais une loi de composition interne $*: E\times E \to E$ qui admet un élément neutre e.

1.10 Définition : Soit $x \in E$. Un inverse de x pour la loi $*$ est un élément $y \in E$ tel que $x*y = e = y*x$.

1.11 Proposition [Unicité de l'inverse] : Soient $y_1, y_2 \in E$ des inverses de $x \in E$. Si la loi $*$ est associative alors $y_1 = y_2$.

Démonstration : $y_1 = y_1 * e = y_1 * x * y_2 = e * y_2 = y_2$
($e = x*y_2$ car y_2 est un inverse de x ; $y_1 * x = e$ car y_1 est un inverse de x) □

L'unicité de l'inverse (dans le cas d'une loi associative) nous permet alors de le noter x^{-1} : $x*x^{-1} = e = x^{-1}*x$.
⚠ Dans le cas des lois commutatives notées $+$, on note l'élément neutre "0" et l'inverse "$-x$" : $x + (-x) = 0 = (-x) + x$.

1.12 ⚠ L'inverse n'existe pas nécessairement :
- Seuls 1 et -1 ont un inverse pour la loi $\times$ dans $\mathbb{Z}$.
- 0 n'a pas d'inverse pour la loi $\times$ dans $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- il y a des matrices qui ne sont pas inversibles pour la loi $\times$:
  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ évidemment, mais aussi : $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, ou encore $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.
  Rappel : une matrice est inversible si et seulement si son déterminant est non nul.

1.13 Définition : Un groupe est la donnée d'un ensemble muni d'une loi de composition interne associative possédant un élément neutre et telle que tout élément admet un inverse (on dit aussi est inversible).
Un groupe dont la loi est commutative est dit abélien.

Munis de la loi $+$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des groupes abéliens. L'existence d'un inverse étant une propriété préservée par la Construction 1.4 (exercice), il en va de même pour :
- $\mathbb{R}^n$ ($X = \{1, \dots, n\}$)
- l'ensemble des suites numériques ($X = \mathbb{N}$)
- l'ensemble des fonctions numériques d'une variable réelle ($X = \mathbb{R}$)
- l'ensemble des matrices de taille $n \times m$ ($X = \{1, \dots, n\} \times \{1, \dots, m\}$)
- etc...

1.14 Proposition : On suppose que la loi $*$ est associative.
(a) Si $x, y \in E$ sont inversibles, alors $x*y$ est inversible et $(x*y)^{-1} = y^{-1} * x^{-1}$.
(b) Par conséquent, la partie $G = \{x \in E \mid x \text{ inversible}\} \subset E$ est stable par $*$, et est donc un groupe lorsqu'on la munie de la restriction de $*$ à G.

On dit qu'une partie $F \subset E$ est stable par $*$ si : $\forall x, y \in F,\ x*y \in F$.
La restriction de la loi $*$ à F est la loi $*_F : F\times F \to F$ définie par $x *_F y = x * y$.

Démonstration de la Proposition : (a) il suffit de calculer :
$y^{-1} * x^{-1} * x * y = y^{-1} * e * y$ (car $x^{-1}*x = e$, et on peut omettre les parenthèses grâce à l'associativité)
$= y^{-1} * y = e$
De la même manière $x*y*y^{-1}*x^{-1} = x*e*x^{-1} = x*x^{-1} = e$.
Nous avons donc montré que $y^{-1}*x^{-1}$ est un inverse de $x*y$.

(b) d'après (a), si $x, y \in G$ alors $x*y \in G$. On peut donc restreindre la loi $*$ à la partie $G \subset E$. Cette loi est évidemment associative (puisqu'on l'a supposée telle sur E) :
$\forall x, y, z \in G,\ (x *_G y) *_G z = (x*y)*z = x*(y*z) = x *_G (y *_G z)$.

⚠ Le plus difficile dans la démonstration de (b) est de comprendre ce qu'il y a à démontrer.

Dans un premier temps, il est primordial de bien différencier $*_G$ et $*$. Par

Dans un premier temps, il est primordial de bien différencier $*_G$ et $*$. Par la suite, lorsque vous serez plus à l'aise, vous pourrez utiliser le même symbole pour les deux.

$$\forall x,y,z \in G,\ (x *_G y) *_G z = (x*y)*z = x*(y*z) = x *_G (y *_G z).$$

L'élément neutre de $*$ appartient à G et est l'élément neutre de $*_G$: en effet, $e \in G$ car l'élément neutre est toujours inversible (il est son propre inverse : $e*e=e$), et pour tout $x \in G$, $x *_G e = x*e = x = e*x = e *_G x$.

Finalement, pour tout $x \in G$, l'inverse x^{-1} pour $*$ (qui existe par définition de G) est aussi un inverse pour $*_G$: $x *_G x^{-1} = x*x^{-1} = e = x^{-1}*x = x^{-1} *_G x$. □

Comme conséquence immédiate de cette Proposition, nous obtenons les exemples de groupes qui suivent :
- $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, munis de la multiplication $\times$.
- $\{-1,+1\}$, muni de la multiplication $\times$ (dans $\mathbb{Z}$, les seuls éléments inversibles pour $\times$ sont ± 1).
- $\{+1\}$, muni de la multiplication $\times$ (dans $\mathbb{N}$, le seul élément inversible pour $\times$ est 1).
- l'ensemble $Bij(X)$ des bijections d'un ensemble X dans lui-même, muni de la composition des applications (dans $E = X^X$, les éléments inversibles pour la composition sont les bijections).
- l'ensemble $GL_n(\mathbb{R})$ des matrices $n \times n$ à coefficients dans $\mathbb{R}$ qui sont inversibles, muni du produit matriciel.

1.15 **Définition** : deux groupes $(G, *_G, e_G)$ et $(H, *_H, e_H)$ sont dits **isomorphes** si il existe une bijection $\varphi : G \to H$ telle que $\varphi(e_G) = e_H$ et $\varphi(x *_G y) = \varphi(x) *_H \varphi(y)$ quels que soient $x, y \in G$. On dit alors que φ est un **isomorphisme**.

Il suit immédiatement de la définition que $\varphi(x^{-1}) = \varphi(x)^{-1}$ → à démontrer en exercice.

1.16 **Exemple** : le groupe des bijections de l'ensemble $\{1,2\}$ (muni de la loi "$\circ$") est isomorphe au groupe $\{-1,+1\}$ (muni de la loi "$\times$"). En effet, posons $\varphi : Bij(\{1,2\}) \longrightarrow \{-1,+1\}$, $f \longmapsto f(2) - f(1)$.

- vérifions que φ est bien défini et est une bijection : $Bij(\{1,2\})$ n'a que deux éléments, qui sont l'identité "id" et la permutation "σ" de 1 et 2. On a $\varphi(id) = id(2) - id(1) = 2-1 = 1$. et $\varphi(\sigma) = \sigma(2) - \sigma(1) = 1 - 2 = -1$.
- On voit en particulier que φ envoie l'élément neutre de $Bij(\{1,2\})$ (qui est id) sur l'élément neutre de $\{-1,+1\}$ (qui est $+1$).
- Il reste à vérifier que φ préserve le produit : la seule chose non évidente à vérifier est que $\varphi(\sigma \circ \sigma) = \varphi(\sigma) \times \varphi(\sigma)$. Vérifions : $\varphi(\sigma \circ \sigma) = \varphi(id) = 1 = (-1) \times (-1) = \varphi(\sigma) \times \varphi(\sigma)$.

Deux remarques avant de poursuivre : 1) en fait, tous les groupes à deux éléments sont isomorphes (vous pouvez essayer de le démontrer si vous vous sentez à l'aise)

2) Le groupe $Bij(\{1,\dots,n\})$ des bijections de l'ensemble à n éléments $\{1,\dots,n\}$ s'appelle le groupe des permutations de n éléments, et se note S_n.

Sous-groupes

Il peut être fastidieux de devoir vérifier tous les axiomes de la définition d'un groupe (et ça sera pire avec les espaces vectoriels). La notion de sous-groupe permet de vérifier à peu de frais qu'une partie d'un groupe est encore un groupe : c'est une notion pratique et économe pour les démonstrations (et ça sera encore plus flagrant lorsqu'on verra les sous-espaces vectoriels).

1.17 **Définition** : soit $(G, *, e)$ un groupe. Un **sous-groupe** de G est une partie non-vide $H \subset G$ qui est stable par $*$ ($\forall x,y \in H,\ x*y \in H$) et par passage à l'inverse ($\forall x \in H,\ x^{-1} \in H$).

⚠ N'oubliez pas la condition "non-vide" (que beaucoup de personnes oublient).

1.18 **Proposition** : soit $(G, *, e)$ un groupe et $H \subset G$ un sous-groupe. Alors, muni de la restriction $*_H$ de la loi $*$, H est un groupe.

Démonstration : La démonstration ressemble beaucoup à la démonstration du (b) de la Proposition 1.14.

① Montrons que la loi $*_H$ est associative.
$\forall x,y,z \in H$, $(x *_H y) *_H z = (x*y)*z = x*(y*z) = x *_H (y *_H z)$.

② Montrons que $e \in H$ et que c'est l'élément neutre de $*_H$.
Soit $x \in H$ (un tel x existe car H est supposé non-vide), alors $x^{-1} \in H$ et $e = x * x^{-1} \in H$.
(stabilité par passage à l'inverse ; stabilité par $*$)

Quel que soit $y \in H$, $y *_H e = y*e = y = e*y = e *_H y$.

Donc $e \in H$ est l'élément neutre de $*_H$.

③ Montrons finalement que pour tout $x \in H$, son inverse x^{-1} (pour $*$) est un inverse pour $*_H$.
$x *_H x^{-1} = x * x^{-1} = e = x^{-1} * x = x^{-1} *_H x$. □

1.19 Exemples [racines de l'unité] : Soit $N \geq 1$ un entier. On note $\mu_N = \{ z \in \mathbb{C} \mid z^N = 1 \}$. C'est un sous-groupe de $\mathbb{C}^\times$.
(a) $\mu_N \subset \mathbb{C}^\times$: $\forall z \in \mu_N$, $z \times z^{N-1} = z^{N-1} \times z = z^N = 1$. Donc z admet un inverse (dans $\mathbb{C}$).
(b) $\mu_N \neq \emptyset$: $1 \in \mu_N$.
(c) μ_N est stable par $\times$: si $z, \xi \in \mu_N$ alors $(z \times \xi)^N = z^N \times \xi^N = 1 \times 1 = 1$.
(d) μ_N est stable par passage à l'inverse : si $z \in \mu_N$ alors $(z^{-1})^N = (z^N)^{-1} = (1)^{-1} = 1$.

[matrices inversibles et bijections linéaires] : on note $M_n(\mathbb{R})$ l'ensemble des matrices $n \times n$ à coefficients dans $\mathbb{R}$.
On considère l'application $\Psi : M_n(\mathbb{R}) \longrightarrow (\mathbb{R}^n)^{\mathbb{R}^n}$ définie comme suit :
Si on note les éléments de $\mathbb{R}^n$ comme des vecteurs colonne, on a $\Psi(A)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := A \times \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.
Exercice : montrer que $\Psi(A \times B) = \Psi(A) \circ \Psi(B)$.
Remarque : l'image de Ψ est l'ensemble des applications linéaires $\mathbb{R}^n \to \mathbb{R}^n$.
De plus, Ψ est injective (à démontrer en exercice).
Donc $M_n(\mathbb{R})$ est en bijection avec l'ensemble des application linéaires $\mathbb{R}^n \to \mathbb{R}^n$.
Conséquence : le groupe $GL_n(\mathbb{R})$ est isomorphe au sous-groupe de $Bij(\mathbb{R}^n)$ constitué des bijections linéaires.

[isométries] : on considère le produit scalaire usuel sur $\mathbb{R}^n$, donné par
$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle := (x_1 \cdots x_n) \times \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i=1}^{n} x_i y_i .$$

Une isométrie de $\mathbb{R}^n$ est une application $f : \mathbb{R}^n \to \mathbb{R}^n$ telle que : $\forall \underline{x}, \underline{y} \in \mathbb{R}^n$, $\langle f(\underline{x}), f(\underline{y}) \rangle = \langle \underline{x}, \underline{y} \rangle$.
On peut montrer que toute isométrie est linéaire (on admettra ce résultat), et peut donc être représentée de manière unique par une matrice A.
La condition d'isométrie se traduit sur A par $A^T A = A A^T = Id = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.
Donc A est inversible et $A^{-1} = A^T$. En particulier, toute isométrie de $\mathbb{R}^n$ est bijective.
Montrons que l'ensemble des isométries de $\mathbb{R}^n$ est un sous-groupe du groupe des bijections (linéaires) de $\mathbb{R}^n$.
(a) l'identité est une isométrie. L'ensemble est donc non-vide.
(b) si $f, g : \mathbb{R}^n \to \mathbb{R}^n$ sont deux isométries, alors $\langle g \circ f(\underline{x}), g \circ f(\underline{y}) \rangle = \langle f(\underline{x}), f(\underline{y}) \rangle = \langle \underline{x}, \underline{y} \rangle$ (car g est une isométrie ; car f est une isométrie).
(c) si $f : \mathbb{R}^n \to \mathbb{R}^n$ est une isométrie,
$\langle \underline{x}, \underline{y} \rangle = \langle f \circ f^{-1}(\underline{x}), f \circ f^{-1}(\underline{y}) \rangle = \langle f^{-1}(\underline{x}), f^{-1}(\underline{y}) \rangle$.
(car f^{-1} est l'inverse de f ; car f est une isométrie)

Exercice : refaire cette démonstration en termes matriciels. Les matrices des isométries de $\mathbb{R}^n$ s'appellent les matrices orthogonales et on note leur ensemble $O(n)$.

[permutations et matrices de permutations] : on note $S_n := Bij(\{1, \dots, n\})$, dont les éléments sont appelées les permutations de n éléments. On considère l'application $\Psi : S_n \longrightarrow Bij(\mathbb{R}^n)$
$\sigma \longmapsto \left[\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix} \right]$
Montrons que Ψ est ...

les permutations de n éléments. On considère l'application $\varphi : S_n \longrightarrow Bij(\mathbb{R}^n)$

$$\sigma \longmapsto \left[\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix} \right]$$

On vérifie facilement que φ est injective,

Exercice : montrer que $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$.

On en déduit que S_n est isomorphe au sous-groupe de $Bij(\mathbb{R}^n)$ constitué des bijections qui permutent les coordonnées.

On remarque finalement qu'une permutation des coordonnées est une application linéaire, de sorte que $S_n \subset GL_n(\mathbb{R})$.

Exercice : on note $e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots, 0)$. Montrer que $\varphi(\sigma)(e_i) = e_{\sigma(i)}$.
Quelle est la matrice de l'application linéaire $\varphi(\sigma)$?

Anneaux et corps

1.20 Définition : un anneau est un groupe abélien $(A, +, 0_A)$ muni d'une loi $\times : A \times A \to A$ associative, possédant un élément neutre 1_A, qui est distributive par rapport à l'addition :

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

Un anneau est dit commutatif si la loi $\times$ est commutative.

1.21 Exemples : • $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis des lois $+$ et $\times$ habituelles, sont des anneaux commutatifs.

• L'ensemble $M_n(\mathbb{R})$, muni de la somme et du produit des matrices, est un anneau qui n'est pas commutatif !

Remarque : dans cet exemple, les coefficients des matrices auraient pu être dans $\mathbb{Z}$ ($M_n(\mathbb{Z})$ est un anneau), $\mathbb{Q}$ ou encore $\mathbb{C}$.

• On se rappelle que l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites numériques est un groupe abélien pour la loi $+$ donnée par l'addition terme à terme. Nous allons définir une loi $\times$ "originale" sur l'ensemble $\mathbb{R}^{\mathbb{N}}$:

étant données deux suites $u = (u_n)_{n \in \mathbb{N}}$ et $v = (v_n)_{n \in \mathbb{N}}$, on pose $(u \times v)_n := \sum_{i=0}^{n} u_i v_{n-i}$.

→ vérifiez que cette loi définit une structure d'anneau sur $\mathbb{R}^{\mathbb{N}}$.

Intuition : on peut écrire formellement la somme $u_0 + u_1 X + u_2 X^2 + \dots + u_n X^n + \dots$

On a $(u_0 + u_1 X + u_2 X^2 + \dots) \times (v_0 + v_1 X + v_2 X^2 + \dots) = u_0 v_0 + (u_0 v_1 + u_1 v_0) X + (u_0 v_2 + u_1 v_1 + u_2 v_0) X^2 + \dots$

Le coefficient devant X^n est précisément $(u \times v)_n$.

1.22 Définition : Soit $(A, +, 0, \times, 1)$ un anneau. Une partie $B \subset A$ est un sous-anneau si :

1] B est un sous-groupe de $(A, +, 0)$.
2] B est stable par $\times$ et $1 \in B$.

Comme pour les sous-groupes, on peut vérifier aisément que si B est un sous-anneau de A, alors les lois induites de A sur B font de B un anneau. → à vérifier en exercice.

1.23 Exemple : Considérons le sous-ensemble de $\mathbb{R}^{\mathbb{N}}$ constitué des suites presques nulles (une suite $(u_n)_{n \in \mathbb{N}}$ est presque nulle si elle est nulle à partir d'un certain rang : $\exists N \in \mathbb{N}, \forall n \geq N, \ u_n = 0$).

L'ensemble des suites presques nulles est un sous-groupe pour la loi $+$ donnée par la somme terme à terme :

→ en effet, si $u_n = 0$ lorsque $n \geq N_1$ et $v_n = 0$ lorsque $n \geq N_2$ alors $u_n + v_n = 0$ lorsque $n \geq \max(N_1, N_2)$.

! il faut aussi vérifier que c'est non-vide et stable par passage à l'opposé. Mais ces deux conditions sont évidemment satisfaites

Cette partie est également stable par la loi $\times$ définie en 1.21 :

en effet, si $u_n = 0$ lorsque $n \geq N_1$ et $v_n = 0$ lorsque $n \geq N_2$ alors $\sum_{i=0}^{n} u_i v_{n-i} = 0$ lorsque $n \geq N_1 + N_2$.

Enfin, l'élément neutre pour la loi $\times$ est la suite $(1, 0, 0, 0, \dots)$, qui est bien presque nulle.

⇒ On obtient un anneau, qui n'est rien d'autre que l'anneau des polynômes !!!

Dans l'exemple qui précède (comme dans celui des matrices), on peut remplacer $\mathbb{R}$ par $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, ou même n'importe quel autre anneau A.

1.24 Notation : • s'il n'y a pas d'ambiguïté, on a tendance à noter xy pour $x \times y$ lorsque $x, y \in A$ anneau.

• on écrira aussi x^n pour $\underbrace{x \times \dots \times x}_{n \text{ fois}}$. Stricto sensu, il faut définir x^n par récurrence : $x^0 = 1$ et $x^{n+1} = x \times x^n$.

1.25 Proposition [calcul dans un anneau] : Soit A un anneau et soient $x, y \in A$ deux éléments qui commutent (ce qui signifie que $xy = yx$). Alors :

1.25 **Proposition [calcul dans un anneau]** : Soit A un anneau et soient $x, y \in A$ deux éléments qui commutent (ce qui signifie que $xy = yx$). Alors :

(a) $(xy)^n = x^n y^n$ quel que soit $n \in \mathbb{N}$.

(b) $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$.

(c) $x^n - y^n = (x-y)\left(\sum_{i=0}^{n-1} x^i y^{n-1-i}\right) = \left(\sum_{i=0}^{n-1} x^i y^{n-1-i}\right)(x-y)$

Corollaire : si A est un anneau et $x \in A$ est tel que $x^n = 0$ pour un certain $n \geq 1$, alors $1-x$ est inversible d'inverse $(1-x)^{-1} = \sum_{i=0}^{n-1} x^i = 1 + x + \cdots + x^{n-1}$.

Dans un anneau il y a deux lois ($+$ et $\times$). Tout élément x a un inverse pour la loi $+$ (on a un groupe abélien) qu'on appelle opposé et qu'on note $-x$. Lorsqu'on parle d'invertibilité et d'inverse on se réfère toujours à la loi $\times$ (et on note comme d'habitude l'inverse x^{-1}).

Démonstration du Corollaire : on applique le (c) de la Proposition et on trouve que
$(1-x)(1+x+\cdots+x^{n-1}) = 1 - x^n = 1 = (1+x+\cdots+x^{n-1})(1-x)$. □

Éléments de démonstration de la Proposition :

- (a) C'est évident, mais si on veut faire une démonstration rigoureuse il faut d'abord démontrer par récurrence que si x et y commutent alors x et y^n commutent pour tout n.
- (b) Ici il faut utiliser la formule du triangle de Pascal : $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. On rappelle que $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$.

→ à faire en exercice, en regardant bien à quel moment on utilise que x et y commutent !

- (c) Ici il faut développer le produit et faire une somme télescopique :

$$(x-y)\left(\sum_{i=0}^{n-1} x^i y^{n-1-i}\right) = \sum_{i=0}^{n-1} x^{i+1} y^{n-1-i} - \sum_{i=0}^{n-1} y\, x^i y^{n-1-i} = x^i y^{n-i}$$

$$= \sum_{i=1}^{n} x^i y^{n-i} - \sum_{i=0}^{n-1} x^i y^{n-i} = x^n y^0 - x^0 y^n = x^n - y^n. \quad \square$$

1.26 **Définition** : un corps est un anneau commutatif non nul dans lequel tout élément non nul est inversible.

(l'anneau nul n'a qu'un élément qui est le neutre à la fois de $+$ et $\times$.)

Par exemple, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. Mais il existe des corps qui vous sont moins familiers, comme par exemple le corps $\mathbb{F}_2$ à deux éléments : $\mathbb{F}_2 := \{\bar{0}, \bar{1}\}$ (vous pouvez penser à $\bar{0}$ = "pair" et $\bar{1}$ = "impair") est muni de deux lois $+$ et $\times$: $\bar{0}+\bar{0} = \bar{0}$, $\bar{0}+\bar{1} = \bar{1} = \bar{1}+\bar{0}$, $\bar{1}+\bar{1} = \bar{0}$.

$\bar{0}\times\bar{0} = \bar{0} = \bar{1}\times\bar{0} = \bar{0}\times\bar{1}$, $\bar{1}\times\bar{1} = \bar{1}$.

Remarque : on n'a aucune liberté pour les lois du corps à deux éléments. La loi $+$ est déterminée uniquement car on a vu que tous les groupes à deux éléments sont isomorphes.

Ensuite, dans un anneau, $0 \times a = 0$ (en effet : $0 \times a = (0+0) \times a = 0 \times a + 0 \times a$, donc $0 = 0 \times a$).

1.27 **Observation finale** : la plupart des calculs que vous êtes habitués à effectuer dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sont valides dans un corps quelconque, mais pas tous !

Par exemple : • dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, $\underbrace{1+\cdots+1}_{n \text{ fois}} \neq 0$ quel que soit $n \in \mathbb{N} \setminus \{0\}$.

On dit que ce sont des corps de caractéristique 0.

• dans $\mathbb{F}_2$, $\bar{1}+\bar{1} = \bar{0}$. $\mathbb{F}_2$ est un corps de caractéristique non nulle (sa caractéristique est 2).

1.28 **Une dernière Définition** : un sous-corps d'un corps $\mathbb{K}$ est un sous-anneau $\mathbb{K}' \subset \mathbb{K}$ qui est aussi un corps.

On peut montrer facilement qu'un sous-anneau $A \subset \mathbb{K}$ d'un corps si et seulement si $A \setminus \{0\}$ est stable par passage à l'inverse → à démontrer en exercice.

On peut montrer facilement qu'un sous-anneau $A \subset \mathbb{K}$ d'un corps si et seulement si $A \setminus \{0\}$ est stable par passage à l'inverse → à démontrer en exercice.

Exemples : $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est un sous-corps de $\mathbb{C}$.