Algèbre Linéaire Avancée I
Math 110 (b)

Dr. Aline Zanardini

aline.zanardini@epfl.ch

Septembre 2025

AZ: Ces notes sont susceptibles de contenir des erreurs. Vous êtes libres de me signaler toute coquille et erreur par e-mail.

Table des matières

Cours 1 (8 septembre)

1.1 Que comprend l'algèbre linéaire et pourquoi l'étudie-t-on ?

L'algèbre est le domaine des mathématiques qui s'occupe d'étudier les **structures algébriques**, c.-à-d., les ensembles munis d'un certain nombre d'opérations sur leurs éléments, et parfois dépendant d'autres ensembles, qui satisfont quelques propriétés et qui sont liées. Dans l'univers de l'algèbre linéaire, c'est la structure **d'espace vectoriel** qui joue le rôle principal. En fait, le mot linéaire fait référence à deux **lois de composition** sur un ensemble (non vide), l'une interne et l'autre externe, qui sont compatibles entre elles et qui vérifient certains axiomes.

Cette structure nous permet de généraliser des concepts de géométrie (comme les droites, les plans, les volumes, . . .), des notions concrètes que nous pouvons visualiser, à une variété de cas beaucoup plus abstraits qui apparaissent dans différents domaines d'étude, notamment la physique. Par exemple, en mécanique quantique, l'espace des états d'un système est un espace vectoriel, dit un espace de Hilbert. On peut également citer tous les problèmes de la physique qui consistent en la résolution d'une équation différentielle linéaire. De toute façon, il y a aussi des applications concrètes de l'algèbre linéaire en ingénierie, en informatique, en économie, en chimie, en biologie, ...

AZ: Je vous propose de lire cet article (en anglais).

1.1.1 Une introduction aux espaces vectoriels

AZ: Cette petite introduction est basée sur une vidéo de la chaîne *Les maths en finesse* avec le même nom que je vous propose également de regarder.

Des espaces vectoriels peuvent donc contenir par leurs éléments des suites, des polynômes, des matrices, des fonctions, ou alors plus simplement des « vecteurs numériques » ou des « vecteurs géométriques » qui représentent un point dans le plan $\mathbb{R}^2$ ou dans l'espace $\mathbb{R}^3$, par exemple. Même si à première vue ces objets semblent très différents.

Pour introduire cette notion, considérons maintenant les ensembles suivants :

- $\mathbb{R}^2$,
- $\mathcal{S} := \{x = (x_n)_{n=0}^{\infty} \in \mathbb{R}^{\mathbb{N}} \mid x_{n+2} = x_{n+1} + x_n\}$, et
- $\mathcal{F} := \{f \in C^2(\mathbb{R}, \mathbb{R}) \mid \forall t \in \mathbb{R}, f''(t) + f(t) = 0\}$.

Quel est le lien entre ces trois ensembles ? On vérifie que dans les trois cas, les affirmations suivantes sont vraies.

(i) Les trois ensembles sont stables par **combinaisons linéaires** (réelles). Intuitivement, ça veut dire que si je prends deux éléments d'un de ces ensembles, il existe un moyen de les multiplier par des nombres réels et d'additionner le résultat de telle manière que nous obtenions un élément qui appartient au même ensemble. Plus précisément, nous avons que pour tous les nombres réels α et β

$$(x, y) \in \mathcal{S} \times \mathcal{S} \Rightarrow \alpha x + \beta y \in \mathcal{S},$$

où l'addition de deux suites est définie terme par terme, et la multiplication par les **scalaires** réels aussi. Le formalisme dans les deux autres cas est analogue.

(ii) Chaque élément de $\mathbb{R}^2$, de $\mathcal{S}$, ou de $\mathcal{F}$ est complètement déterminé par deux données. Par exemple, chaque point du plan est entièrement déterminé par son abscisse et par son ordonnée. Similairement, toute suite $x = (x_n)$ dans $\mathcal{S}$ est caractérisée par les termes x_0 et x_1. Et, de la même manière, des fonctions f qui appartiennent à $\mathcal{F}$ peuvent être reconstruites en utilisant les valeurs $f(0)$ et $f'(0)$.

AZ: Dans ce dernier cas, il peut être utile pour vous de faire le lien avec des systèmes physiques qui sont modélisés comme des oscillateurs harmoniques.

(iii) Tout élément de $\mathbb{R}^2$ s'écrit de manière unique comme une combinaison linéaire de deux éléments quelconques qui n'appartiennent pas à la même droite passant par l'origine. Par exemple, si $(x, y) \in \mathbb{R}^2$, alors

$$(x, y) = x \cdot (1, 0) + y \cdot (0, 1),$$

et il est évident que les nombres réels x et y que nous permettent d'écrire (x, y) comme une combinaison linéaire des éléments $(1, 0)$ et $(0, 1)$ sont uniques. Des affirmations analogues sont également vraies pour les ensembles $\mathcal{S}$ et $\mathcal{F}$.

1.1.2 Pour réfléchir chez-vous

Exercice 1.1.1. Vérifiez la véracité de l'affirmation du point (i) ci-dessus. Comment sont définies les opérations d'addition et de multiplication par un nombre réel dans chaque cas ?

Exercice 1.1.2. Trouvez deux autres éléments $u = (u_1, u_2)$ et $v = (v_1, v_2)$ dans $\mathbb{R}^2$ tels que tout autre point du plan $(x, y) \in \mathbb{R}^2$ peut être écrit de manière unique comme une combinaison linéaire de ceux-ci, c'est-à-dire que de la façon suivante :

$$(x, y) = \alpha u + \beta v = \alpha \cdot (u_1, u_2) + \beta \cdot (v_1, v_2),$$

où α et β sont des nombres réels. Que se passera-t-il si nous remplaçons $\mathbb{R}^2$ par $\mathbb{R}^3$? Et dans le cas des ensembles $\mathcal{S}$ et $\mathcal{F}$, pouvez-vous trouver deux bons éléments « **générateurs** » ?

1.2 Lois de composition

Un ensemble est simplement une collection d'objets, sans condition particulière. Mais ils peuvent souvent être associés les uns aux autres (additionnés ou multipliés, par exemple), et on parle alors de lois de composition. Selon les règles que ces lois vérifient, elles permettent de définir des structures algébriques ; autrement dit, les ensembles correspondants portent des structures algébriques (de groupe, d'anneau, de corps, d'espace vectoriel, ...). Les définitions sont les suivantes.

Définition 1.2.1. Une **loi de composition interne**, ou loi interne, sur un ensemble $E \neq \emptyset$ est une application (une fonction) de $E \times E$ dans E.

AZ: ⚠ Dans ce cours, les mots application, fonction et transformation seront utilisés de manière interchangeable.

Autrement dit, une loi interne sur un ensemble E associe à deux éléments de E un élément de E. Donc, une loi de composition interne sur un ensemble E est une opération binaire par laquelle E est

stable. Elle peut être notée par $*$, par $\circ$, par $\otimes$, ... L'addition et la multiplication usuelles dans les ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ sont des exemples classiques de lois de composition internes.

Il est important de noter que pour que la fonction considérée soit effectivement une loi de composition interne, il faut qu'elle soit définie partout. À deux éléments quelconques de E la fonction associe un troisième (élément), unique, et toujours dans E.

Définition 1.2.2. Une **loi de composition externe**, ou loi externe, sur un ensemble $E \neq \emptyset$ est une application de $F \times E$ dans E, où F est un autre ensemble a priori différent de E. Les éléments de F sont appelés des opérateurs ou des scalaires.

L'exemple typique est la multiplication d'un point du plan, un élément de $E = \mathbb{R}^2$, par un nombre réel ($F = \mathbb{R}$). Géométriquement, on peut considérer les points du plan comme des vecteurs géométriques, c'est-à-dire représentés par un segment orienté (une flèche) dont les extrémités sont un point de départ, l'origine, et un point d'arrivée. L'opération dont nous parlons consiste à étirer ou à rétrécir un vecteur, ou bien évidemment à ne rien faire.

Remarque 1.2.3. Si $F = E$ dans la Définition 1.2.2, on a une loi interne. Donc, une loi interne, c'est un cas particulier d'une loi externe.

1.2.1 Quelques propriétés

Soit E un ensemble non vide et soit $* : E \times E \to E$ une loi interne sur E. On dit que la loi $*$ est

(P1) associative si

$$(a * b) * c = a * (b * c) \qquad \forall (a, b, c) \in E^3 = E \times E \times E,$$

(P2) commutative si

$$a * b = b * a \quad \forall (a, b) \in E^2 = E \times E,$$

De plus,

- si $\circ : E \times E \to E$ est une autre loi sur E, on dit que $*$ est distributive à gauche sur $\circ$ si :

$$\forall (a, b, c) \in E^3 ; \; a * (b \circ c) = (a * b) \circ (a * c).$$

  Similairement, on dit que $*$ est distributive à droite sur $\circ$ si :

$$\forall (a, b, c) \in E^3 ; \; (b \circ c) * a = (b * a) \circ (c * a).$$

- Un **élément neutre** pour $*$ est un élément $e \in E$ tel que :

$$\boxed{e * a = a * e = a} \qquad \forall a \in E.$$

- Si E possède un élément neutre e pour $*$, on dit qu'un élément $b \in E$ est un **inverse** de $a \in E$ si $\boxed{a * b = b * a = e}$. Un élément $a \in E$ qui admet un inverse est dit inversible (pour $*$).

Remarque 1.2.4. On peut parler aussi d'éléments neutres à gauche ou à droite et également des inverses à droite et à gauche. Lorsque la loi $*$ en considération est associative, l'existence d'un implique l'existence de l'autre. On va laisser tout ça de côté dans ce cours, cf. Section 2.1 ci-dessous.

AZ: ⚠ Lorsque la loi en question est associative et commutative, on adopte souvent la notation additive : on la désigne par $+$, l'inverse d'un élément $a \in E$ devient $-a$, et on parle d'élément opposé. On parle également d'élément nul, plutôt que d'élément neutre, généralement noté O_E ou simplement 0. Même si 0 n'est pas forcément le nombre zéro. D'un autre côté, il est aussi parfois utile d'adopter la notation multiplicative... Je voudrais donc vous avertir que je ferai probablement tout cela très souvent pendant ce cours, car c'est quelque chose de très naturel pour moi. Il faut toujours faire attention.

Nous pouvons prouver ce qui suit à propos de ces notions.

Proposition 1.2.5. *Soit E un ensemble non vide et $\star : E \times E \to E$ une loi de composition interne. Si E possède un élément neutre pour la loi $\star$, alors cet élément est unique. Par ailleurs, si $\star$ est associative et E possède un élément neutre, alors chaque élément inversible de E a un unique inverse.*

Démonstration. Soient E et $\star$ comme dans l'énoncé du théorème. Supposons que E possède un élément neutre $e \in E$ (pour $\star$). Si $\tilde{e} \in E$ est un autre élément neutre, alors

$$e = e \star \tilde{e} = \tilde{e}. \tag{1}$$

AZ: Notez que dans la première égalité dans (1) ci-dessus nous avons utilisé le fait que $\tilde{e}$ est un élément neutre, et la deuxième égalité découle du fait que e est un élément neutre.

Supposons maintenant que $\star$ est associative et choisissons un élément a qui appartient à E et qui est inversible. Soient b et $\tilde{b}$ deux inverses de a. Alors,

$$\begin{aligned}
\tilde{b} &= \tilde{b} \star e && (e \text{ est élément neutre}) \\
&= \tilde{b} \star (a \star b) && (b \text{ est un inverse de } a) \\
&= (\tilde{b} \star a) \star b && (\star \text{ est associative}) \\
&= e \star b && (\tilde{b} \text{ est un inverse de } a) \\
&= b. && (e \text{ est élément neutre})
\end{aligned}$$

□

1.2.2 Quelques exemples

Exemple 1.2.6 (Réunion et intersection)**.** Si X est un ensemble non vide quelconque, la réunion $(A, B) \mapsto A \cup B$ et l'intersection $(A, B) \mapsto A \cap B$ sont des lois de composition interne sur l'ensemble $\mathcal{P}(X)$ de toutes les parties de X.

Exemple 1.2.7 (Composition de fonctions)**.** Si X est un ensemble non vide quelconque, nous pouvons considérer l'ensemble $\mathcal{F}(X, X)$ de toutes les applications de X dans X. La composition usuelle $(f, g) \mapsto f \circ g$ est une loi de composition sur cet ensemble.

Exemple 1.2.8 (Produit vectoriel)**.** Sur l'ensemble $\mathbb{R}^3$ nous pouvons considérer une loi $\wedge : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ qui est définie par

$$(a, b, c) \wedge (d, e, f) = \begin{vmatrix} \hat{\mathbf{i}} & \hat{\mathbf{j}} & \hat{\mathbf{k}} \\ a & b & c \\ d & e & f \end{vmatrix} = (bf - ce, cd - af, ae - bd).$$

1.2.3 Pour réfléchir chez-vous

Exercice 1.2.9. Les lois des exemples ci-dessus sont-elles commutatives ? Sont-elles associatives ? Est-ce qu'elles admettent un élément neutre ?

Exercice 1.2.10. Donnez un exemple[1] d'un ensemble E et d'une loi interne $* : E \times E \to E$ qui n'est pas commutative. Est-ce que vous connaissez un exemple de loi qui n'est pas associative ?

AZ: Je vous invite à lire cet article (en français).

Exercice 1.2.11. Si $*$ est une loi associative/commutative, sur un ensemble E, et $A \subset E$ est stable par $*$, alors convainquez-vous que la loi $*$, vue comme une loi interne sur A, est bien sûr encore associative/commutative.

Exercice 1.2.12. Soit $E \neq \emptyset$ un ensemble et $\clubsuit : E \times E \to E$ une loi de composition sur E qui est associative. Supposons que E possède un élément neutre $e \in E$ (pour $\clubsuit$). Démontrez que le sous-ensemble

$$A = \{a \in E \mid a \text{ est inversible}\}$$

est stable par $\clubsuit$. Si $a, b \in A$, quel est l'inverse de $a \clubsuit b$?

La définition de partie stable est la suivante.

Définition 1.2.13. Soit E un ensemble non vide, soit $A \subset E$ un sous-ensemble (une partie) et soit $\diamond : E \times E \to E$ une loi interne sur E. On dit que A est **stable** par $\diamond$ si pour chaque couple (x, y) d'éléments de A on a $x \diamond y \in A$. On dit aussi que $\diamond$ induit une loi interne sur la partie A.

1. Différent des exemples ci-dessus.

Cours 2 (10 septembre)

2.1 Groupes

La structure de groupe est fondamentale en mathématiques et dans ce cours nous l'utiliserons pour définir les espaces vectoriels de manière rigoureuse.

Définition 2.1.1. Un **groupe** est un ensemble muni d'une loi de composition interne associative, admettant un élément neutre et telle que tout élément est inversible. Autrement dit, un groupe est un ensemble G muni d'une application $* : G \times G \to G$, qui envoie $(a, b) \mapsto a * b$, tel que les axiomes suivants sont verifiées :

(G1) (associativité) On a $a * (b * c) = (a * b) * c$ por tous $a, b, c \in G$;

(G2) (existence de l'élément neutre) il existe $e \in G$ tel que $e * g = g * e = g$ pour tout $g \in G$; et

(G3) (existence des inverses) pour tout $g \in G$, il existe $g^{-1} \in G$ tel que $g^{-1} * g = g * g^{-1} = e$.

Définition 2.1.2. Un groupe $(G, *)$ dans lequel la loi de composition $*$ est commutative est appelé **groupe abélien**.

AZ: ⚠ On écrira souvent ab pour $a * b$ dans un groupe où la loi n'est pas précisée.

AZ: ⚠ Si le groupe G est abélien j'utiliserai parfois la notation additive : $+$ pour désigner la loi de composition, 0 pour l'élément neutre, et $-g$ pour l'inverse/opposé de $g \in G$.

AZ: ⚠ Les mathématicien.ne.s aiment désigner l'élément neutre d'un groupe $(G, *)$ par e_G.

Remarque 2.1.3. Notez que dans un groupe G, les inverses sont uniques. Nous avons prouvé ce fait dans la Proposition 1.2.5. C'est pour ça qu'on utilise la notation g^{-1} pour désigner l'inverse d'un élément $g \in G$.

Voici quelques conséquences directes de la définition de groupe.

Proposition 2.1.4. *Soit $(G, *)$ un groupe avec élément neutre $e \in G$. Les affirmations suivantes sont vraies.*

(i) Pour tous $a, b, c \in G$, on a

$$a * b = a * c \Rightarrow b = c. \qquad \textit{(simplification à gauche)}$$

De même,

$$a * b = c * b \Rightarrow a = c \qquad \textit{(simplification à droite)}$$

(ii) Pour tous $a, b \in G$, on a

$$(a * b)^{-1} = b^{-1} * a^{-1} \quad \textit{et} \quad (a^{-1})^{-1} = a.$$

Démonstration.

(i) Por tous $a, b, c \in G$ on a

$$\begin{aligned} a * b = a * c &\Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c) \\ &\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c && \text{(Associativité)} \\ &\Rightarrow e * b = e * c && \text{(Définition de l'inverse)} \\ &\Rightarrow b = c && (e \text{ est élément neutre}) \end{aligned}$$

et de même,

$$\begin{aligned} a * b = c * b &\Rightarrow (a * b) * b^{-1} = (c * b) * b^{-1} \\ &\Rightarrow a * (b * b^{-1}) = c * (b * b^{-1}) && \text{(Associativité)} \\ &\Rightarrow a * e = c * e && \text{(Définition d'inverse)} \\ &\Rightarrow a = c && (e \text{ est élément neutre}) \end{aligned}$$

(ii) Pour tous $a, b \in G$, on a

$$\begin{aligned} (a * b) * \left(b^{-1} * a^{-1}\right) &= \left((a * b) * b^{-1}\right) * a^{-1} && \text{(Associativité)} \\ &= \left(a * (b * b^{-1})\right) * a^{-1} && \text{(Associativité)} \\ &= (a * e) * a^{-1} && \text{(Définition de l'inverse)} \\ &= a * a^{-1} && (e \text{ est élément neutre}) \\ &= e. && \text{(Définition de l'inverse)} \end{aligned}$$

AZ: Notez qu'à ce moment, nous venons de prouver que $b^{-1} * a^{-1}$ est un inverse à droite de $a * b$ et la preuve n'est pas finie. Pourquoi ?

De la même façon, nous pouvons montrer que $(b^{-1} * a^{-1}) * (a * b) = e$. Donc, par définition de l'inverse, on a $b^{-1} * a^{-1} = (a * b)^{-1}$.
Enfin, l'égalité $(a^{-1})^{-1} = a$ est une tautologie. Comme dans un groupe des inverses sont uniques (regardez Remarque 2.1.3 et Proposition 1.2.5), on a que $(a^{-1})^{-1}$ est le seul élément de G satisfaisant les égalités suivantes :

$$(a^{-1})^{-1} * (a^{-1}) = (a^{-1}) * (a^{-1})^{-1} = e.$$

Donc ça suffit de noter que

$$a * (a^{-1}) = (a^{-1}) * a = e.$$

En tout cas, nous pouvons également argumenter comme suit (comparez avec la preuve de la Proposition 1.2.5).

$$\begin{aligned} (a^{-1})^{-1} &= (a^{-1})^{-1} * e && (e \text{ est élément neutre}) \\ &= (a^{-1})^{-1} * (a^{-1} * a) && (a^{-1} \text{ est l'inverse de } a) \\ &= \left((a^{-1})^{-1} * a^{-1}\right) * a && (* \text{ est associative}) \\ &= e * a && ((a^{-1})^{-1} \text{ est l'inverse de } a^{-1}) \\ &= a && (e \text{ est élément neutre}) \end{aligned}$$

□

2.1.1 Exemples

Il existe une variété d'exemples de groupes. En fait, vous connaissez déjà, par exemple, $(\mathbb{Z}, +)$ (ou $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}+), \dots$) et $(\mathbb{R}\backslash\{0\}, \cdot)$. Nous listons ici quelques autres qui sont pertinents pour ce cours.

Notez que l'ensemble $\mathbb{N}$ muni de l'addition usuelle n'est pas un groupe. Pourquoi ?

AZ: Je vous invite à parcourir cet article (en français) pour trouver plus d'exemples qui sont relevant pour les physicien.ne.s.

Exemple 2.1.5 (Le plus petit groupe)**.** Soit G un ensemble quelconque avec un seul élément noté e. Si on définit une loi interne $* : G \times G \to G$ sur G, alors nécessairement $e * e = e$ et $(G, *)$ est un groupe.

Exemple 2.1.6. Nous verrons qu'un espace vectoriel est, en particulier, un groupe abélien avec l'addition vectorielle. Nous reviendrons sur cette affirmation lors de la troisième semaine du cours.

Exemple 2.1.7. Soit X un ensemble non vide et considérez l'ensemble $:= \mathrm{Bij}(X)$ de toutes les applications bijectives de X dans X. Si $\circ : \mathrm{Bij}(X) \times \mathrm{Bij}(X) \to \mathrm{Bij}(X)$ note la composition de fonctions, alors on peut vérifier que $(\mathrm{Bij}(X), \circ)$ est un groupe.

AZ: On appelle ce groupe le groupe des permutations de l'ensemble X ou le groupe symétrique de X.

Un cas particulier qui est très important, c'est celui où X est fini. Si $X = \{1, 2, \dots, n\}$, n étant un entier naturel positif, on appelle $\mathrm{Bij}(X)$ le **groupe symétrique de degré** n, noté $\mathfrak{S}_n$, Sym_n, ou simplement S_n. Pour $\sigma \in S_n$ on écrit souvent

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Par exemple, si $n = 3$ et $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ est la bijection telle que $1 \mapsto 2, 2 \mapsto 1$ et $3 \mapsto 3$, on écrit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Exemple 2.1.8 (Les entiers modulo n)**.** Fixons un nombre naturel n non nul. On définit une relation d'équivalence sur $\mathbb{Z}$ de la façon suivante : pour tous $a, b \in \mathbb{Z}$, on dit que $a \sim b$ si et seulement si n divise $b - a$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $b - a = k \cdot n$. On écrit $\mathbb{Z}/n\mathbb{Z}$ pour désigner l'ensemble des classes d'équivalence de $\mathbb{Z}$ par rapport à cette relation et on munit $\mathbb{Z}/n\mathbb{Z}$ d'une loi de composition qui lui donnera la structure de groupe abélien. Si on note $\overline{a}$ la classe d'équivalence de $a \in \mathbb{Z}$, c.-à-d. $\overline{a} := \{b \in \mathbb{Z} \mid a \sim b\}$, alors pour $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ on pose $\overline{x} + \overline{y} := \overline{x + y}$.

Exemple 2.1.9 (Matrices)**.** Une matrice $n \times m$ à coefficients dans $\mathbb{R}$ (ou plus généralement dans un corps K) est un tableau à n lignes et m colonnes constituées d'éléments de $\mathbb{R}$ (ou K) :

On va voir la définition dans le troisième cours.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

On appelle des a_{ij} les coefficients de la matrice A. On écrit $A = (a_{ij})$ et on note $\mathbb{M}_{n\times m}(\mathbb{R})$ (ou $\mathbb{M}_{n\times m}(K)$) l'ensemble des matrices $n \times m$ à coefficients dans $\mathbb{R}$ (ou K). Sur cet ensemble, on peut définir une loi interne $+ : \mathbb{M}_{n\times m}(\mathbb{R}) \times \mathbb{M}_{n\times m}(\mathbb{R}) \to \mathbb{M}_{n\times m}(\mathbb{R})$ donnée par $\big(A = (a_{ij}), B = (b_{ij})\big) \mapsto A + B$, où la matrice $(A+B)$ est telle que son coefficient trouvé dans la ligne i et la colonne j est égal à $a_{ij} + b_{ij}$ pour tous $1 \leq i \leq n$ et $1 \leq j \leq m$. On vérifie que $(\mathbb{M}_{n\times m}(\mathbb{R}), +)$ est un groupe abélien. Quel est l'élément neutre ?

Exemple 2.1.10 (Matrices inversibles)**.**

Définition 2.1.11.

(i) Soient $A \in \mathbb{M}_{n\times m}(\mathbb{R})$ et $B \in \mathbb{M}_{m\times \ell}(\mathbb{R})$. On définit le produit AB comme étant la matrice $C \in \mathbb{M}_{n\times \ell}(\mathbb{R})$ avec $C = (c_{ij})$ et telle que $c_{ij} = \sum_{k=1}^{m} a_{ik}b_{kj}$ pour tous $1 \leq i \leq n$ et $1 \leq j \leq \ell$.

Il faut faire attention ici car le produit est défini uniquement lorsque le nombre de colonnes de A est égal au nombre de lignes de B.

(ii) Une matrice $A \in \mathbb{M}_{n\times n}(\mathbb{R})$ est dite inversible s'il existe $B \in \mathbb{M}_{n\times n}(\mathbb{R})$ telle que

$$AB = \underbrace{\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}}_{:= I_n} = BA.$$

(iii) On note $\mathrm{GL}(n, \mathbb{R})$ l'ensemble des matrices $n \times n$ (à coefficients dans $\mathbb{R}$) qui sont inversibles. Avec la multiplication de matrices, $\mathrm{GL}(n, \mathbb{R})$ est un groupe.

AZ: Ce dernier exemple est fondamental. En fait, beaucoup d'autres exemples intéressants sont des sous-groupes (Définition 2.2.1) de $\mathrm{GL}(n, \mathbb{R})$. On verra aussi que dans l'algèbre linéaire le calcul matriciel est très important. Je vous propose de regarder la vidéo « But what is a neural network ? » sur la chaîne *3Blue1Brown*. Je vous invite aussi à lire cet article (en anglais).

Remarque 2.1.12 (⚠ À lire en fin de semestre)**.** Soit K un corps et considérons le groupe $\mathrm{GL}(n, K)$. On peut définir une loi de composition externe sur l'ensemble $\mathbb{M}_{n\times n}(K)$ de la façon suivante :

$$\begin{aligned} \mathrm{GL}(n, K) \times \mathbb{M}_{n\times n}(K) &\to \mathbb{M}_{n\times n}(K) \\ (P, A) &\mapsto PAP^{-1} \end{aligned}$$

Bien sûr qu'on peut parler aussi des matrices inversibles à coefficients dans un corps...

Notez qu'en utilisant la notation de l'Exemple 1.2.7 on peut aussi considérer cette loi comme une application

$$\begin{aligned} \mathrm{GL}(n, K) &\to \mathcal{F}(\mathbb{M}_{n\times n}(K), \mathbb{M}_{n\times n}(K)) \\ P &\mapsto (f_P : A \mapsto PAP^{-1}) \end{aligned}$$

telle que pour chaque $P \in \mathrm{GL}(n, K)$ la fonction $f_P : \mathbb{M}_{n\times n}(K) \to \mathbb{M}_{n\times n}(K)$ est bijective. Pouvez-vous voir pourquoi ? Ceci est donc un exemple d'action de groupe. Alors, on peut utiliser cette loi-là pour définir une relation d'équivalence sur l'ensemble $\mathbb{M}_{n\times n}(K)$. Pouvez-vous décrire les classes d'équivalence lorsque $n = 2$ et $K = \mathbb{R}$ ou $\mathbb{C}$?

AZ: Bien comprendre Remarque 2.1.12 à la fin du semestre est l'un des objectifs de ce cours.

2.1.2 Pour réfléchir chez-vous

Exercice 2.1.13. Si $(G, *)$ est un groupe fini (c.-à-d. que l'ensemble G est fini) on peut décrire $*$ à travers un tableau (ou matrix) : on place les éléments de G dans un ordre fixe $g_1 = e, g_2, \ldots, g_n$ et on pose que l'entrée a_{ij} du tableau soit l'élément $g_i g_j \in G$ (et que doit être l'un des g_k), cf. Exemple 2.2.6. Montrez que dans ce cas G est abélien si et seulement si le tableau donne une matrice symétrique (la transposée est égale à la matrice originale).

la matrice transposée (ou la transposée) d'une matrice $A \in \mathbb{M}_{n\times m}(K)$ est la matrice $A^t \in \mathbb{M}_{m\times n}(K)$, obtenue en échangeant les lignes et les colonnes de A.

Exercice 2.1.14. Soit $(G, *)$ un groupe avec élément neutre e et tel que $g^2 = g * g = e$ pour tout $g \in G$. Montrez que G est abélien.

Exercice 2.1.15. Considérez l'ensemble $\mathcal{H}$ de toutes les matrices $H \in \mathbb{M}_{3\times 3}(\mathbb{R})$ de la forme :

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Montrez que $\mathcal{H}$ est un groupe avec le produit des matrices. Ce groupe est appelé le groupe de Heisenberg et son origine est trouvée dans la mécanique quantique.

2.2 Sous-groupes

Définition 2.2.1. Soit $(G, *)$ un groupe. Un sous-ensemble $H \subset G$ est un **sous-groupe** de G si la loi $*$ restreinte à H munit H d'une structure de groupe. Si tel est le cas, on écrit $H \leq G$.

Nous constatons que cette définition n'est pas très pratique. Nous démontrons donc ce qui suit.

Proposition 2.2.2. *Soit $(G, *)$ un groupe et $H \subset G$ un sous-ensemble. Alors H est un sous-groupe de G si et seulement si les trois conditions suivantes sont vérifiées.*

(i) H est non vide,

(ii) pour tous $a, b \in H$, on a $a * b \in H$, et

(iii) pour tout $h \in H$, on a $h^{-1} \in H$.

Démonstration.

$\boxed{\Rightarrow}$ Tout d'abord, supposons que H soit un sous-groupe de G. Alors, H possède un élément neutre e_H et est donc non vide. En plus, *(ii)* s'ensuit, puisque la loi de composition sur G se restreint à une loi

sur H. On a aussi que l'élément neutre de H, e_H, est égal à e, l'élément neutre de G. En effet,

$$\underbrace{e_H * e}_{\substack{\uparrow \\ e_H \in G \\ e \text{ est élément neutre de } G}} = e_H \overset{\substack{\downarrow \\ e_H \in H \\ e_H \text{ est élément neutre de } H}}{=} e_H * e_H \quad \Rightarrow \quad \boxed{e = e_H}. \qquad \begin{matrix} \uparrow \\ \text{simplification à gauche} \end{matrix}$$

Maintenant, montrons que (iii) est valide. Si $h \in H$, il existe $\tilde{h} \in H$ tel que $h * \tilde{h} = \tilde{h} * h = e_H$. Alors, puisque $e_H = e$, par l'unicité des inverses, on obtient que $\tilde{h} = h^{-1}$ et donc $h^{-1} \in H$.

$\boxed{\Leftarrow}$ Supposons maintenant que les conditions (i), (ii) et (iii) soient vérifiées. Alors, (ii) nous dit que l'image de tout couple $(a, b) \in H \times H$ sous la loi $*$ appartient à H, c.-à-d. que la restriction de $*$ à $H \times H$ définit bien une loi de composition sur H. La loi est associative car elle est déjà dans G (cf. Exercice 1.2.11). En plus, par (i) il existe $h \in H$ et par la combinaison de (iii) et (ii) on a $h * h^{-1} = e \in H$. Autrement dit, H possède un élément neutre, notamment e, l'élément neutre de G. Enfin, il résulte de (iii) que tout élément de H possède un inverse. En conclusion, les conditions (G1), (G2) et (G3) dans la Définition 2.1.1 sont vérifiées et $(H, *)$ est un groupe. □

2.2.1 Exemples

Exemple 2.2.3. Si G est un groupe quelconque, alors $H = \{e\}$ et $H = G$ sont des sous-groupes de G.

Exemple 2.2.4. $\{1, -1\} \leq (\mathbb{R}\backslash\{0\}, \cdot)$.

Exemple 2.2.5. Si $G = \mathbb{Z}/6\mathbb{Z}$, alors $H = \{\overline{0}, \overline{2}, \overline{4}\}$ est un sous-groupe.

Exemple 2.2.6. Le groupe $G = S_3$ a six éléments : l'élément neutre $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

On note que $\sigma_1\sigma_2 = \sigma_4 \neq \sigma_5 = \sigma_2\sigma_1$, et donc S_3 n'est pas abélien. En plus, $H = \{e, \sigma_4, \sigma_5\} \leq S_3$. En effet, on a

$\circ$	e	σ_4	σ_5
e	e	σ_4	σ_5
σ_4	σ_4	σ_5	e
σ_5	σ_5	e	σ_4

2.2.2 Pour réfléchir chez-vous

Exercice 2.2.7. Soit $(G, *)$ un groupe abélien avec élément neutre e et posons

$$G_2 = \{g \in G \mid g^2 = g * g = e\}.$$

Montrer que G_2 est un sous-groupe de G. Dans le cas particulier du groupe $(\mathbb{Z}/4\mathbb{Z}, +)$, trouver G_2.

Exercice 2.2.8. Plus généralement, soient $(G, *)$ un groupe abélien et $n \in \mathbb{N}$ un nombre naturel supérieur ou égal à deux. Montrez que $H \coloneqq \{g \in G\,;\, g^n = e\}$ est un sous-groupe de G. Ici $g^n = \underbrace{g * \ldots * g}_{n}$.

Est-ce que vous pouvez décrire H lorsque $(G, *) = (\mathbb{C}\backslash\{0\}, \cdot)$?

Exercice 2.2.9. On dit qu'une matrice $A \in \mathbb{M}_{n\times n}(\mathbb{R})$ est orthogonale si $A^t = A^{-1}$, c'est-à-dire que $A^tA = I_n = AA^t$. L'ensemble de toutes ces matrices orthogonales est noté $O(n, \mathbb{R})$.

Montrez que $O(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{R})$.

Ici A^t note la transposée de A.

2.3 Morphismes de groupes

Il n'est pas très utile de définir de nouveaux objets mathématiques si on ne sait pas comment les comparer entre eux. La notion qui permet de le faire pour les groupes est celle d'homomorphisme des groupes.

Définition 2.3.1. Soient $(A, *)$ et $(B, \circ)$ des groupes.

(i) Un **homomorphisme** (ou simplement morphisme) de groupes de A dans B est une application $\varphi : A \to B$, telle que pour tous $x, y \in A$ on a

$$\varphi(x * y) = \varphi(x) \circ \varphi(y).$$

($*$: loi sur A ; $\circ$: loi sur B)

(ii) Un **isomorphisme**, s'il existe, entre A et B est un homomorphisme bijectif. Si tel est le cas, nous disons que A et B sont isomorphes, ou que A est isomorphe à B (et vice versa), et on écrit $A \simeq B$.

Voici quelques propriétés qui suivent directement de la Définition 2.3.1.

Lemme 2.3.2. *Soit $\varphi : A \to B$ un morphisme de groupes de $(A, *)$ dans $(B, \star)$, et soit encore $a \in A$. Alors*

(i) $\varphi(e_A) = e_B$,

(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$

(iii) et plus généralement pour tout $n \in \mathbb{Z}$ on a $\varphi(a^n) = \varphi(a)^n$.

Démonstration. Comme déjà mentionné, la preuve découle directement de la Définition 2.3.1 (i) et est laissée en exercice. □

La notion de morphisme de groupes nous permet aussi d'introduire deux autres exemples de sous-groupes qui sont très importants.

Définition 2.3.3. Le **noyau** d'un homomorphisme de groupes $\varphi : A \to B$ est l'ensemble

$$\ker(\varphi) := \{a \in A \mid \varphi(a) = e_B\} \subset A.$$

(e_B : l'élément neutre de B)

On désigne l'image de φ par $\mathrm{im}(\varphi) := \{\varphi(a) \mid a \in A\} \subset B$.

Proposition 2.3.4. *Si $\varphi : A \to B$ est un morphisme de groupes de $(A, *)$ dans $(B, \star)$, alors* $\ker(\varphi) \leq A$ *et* $\mathrm{im}(\varphi) \leq B$.

Démonstration.

- Montrons que $\ker(\varphi) \leq A$ en utilisant la Proposition 2.2.2. Par Lemme 2.3.2 (i), $e_A \in \ker(\varphi)$ et donc $\ker(\varphi)$ est non vide. Maintenant, prenons $x, y \in \ker(\varphi)$. Alors

$$\varphi(x * y) \underset{\text{Définition 2.3.1 (i)}}{=} \varphi(x) \star \varphi(y) \overset{x,\, y \in \ker(\varphi)}{=} e_B \star e_B = e_B \underset{\text{Définition 2.3.3}}{\Rightarrow} x * y \in \ker(\varphi)$$

  et, également, par Lemme 2.3.2 (ii) on a

$$\varphi(a^{-1}) = \underbrace{\varphi(a)}_{=e_B}{}^{-1} = e_B.$$

- Je vous laisse comme exercice de montrer que $\mathrm{im}(\varphi) \leq B$.

□

2.3.1 Exemples

Exemple 2.3.5. Soit G un groupe quelconque. Alors l'application identité $\mathrm{id} : G \to G$ est un morphisme de groupes, tout comme l'application constante $\varphi : G \to \{e\}$.

Exemple 2.3.6. Soit $H = \{e, \sigma_4, \sigma_5\} \leq S_3$ comme dans l'Exemple 2.2.6. On définit $\varphi : \mathbb{Z}/3\mathbb{Z} \to H$ par $\varphi(\overline{0}) = e$, $\varphi(\overline{1}) = \sigma_4$ et $\varphi(\overline{2}) = \sigma_5$. On vérifie que φ est un isomorphisme de groupes.

Exemple 2.3.7. Soit $n \in \mathbb{N}$, $n \geq 1$ et soit $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ le morphisme défini par $a \mapsto \overline{a}$. Alors $\ker(\varphi) = \{a \in \mathbb{Z} \mid \overline{a} = \overline{0}\} = \{a \in \mathbb{Z} \mid n \text{ divise } a\} = n\mathbb{Z}$. Est-ce qu'il y a d'autres sous-groupes de $(\mathbb{Z}, +)$?

Exemple 2.3.8. Soit $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right\} \leq \mathrm{GL}(2, \mathbb{R})$ et considérons l'application $\varphi : H \to \mathbb{R}$ donnée par $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mapsto a$. On peut vérifier que φ est un isomorphisme de groupes de H (avec la multiplication des matrices) dans $(\mathbb{R}, +)$.

2.3.2 Pour réfléchir chez-vous

Exercice 2.3.9. Trouvez un sous-groupe $H \leq S_3$ tel qu'il existe un isomorphisme de groupes $\mathbb{Z}/2\mathbb{Z} \to H$. Décrivez explicitement l'isomorphisme. Combien de sous-groupes de ce type existe-t-il ?

Exercice 2.3.10. Soit S^1 le cercle unité dans $\mathbb{R}^2$, i.e. $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. On définit la loi de composition $*$ sur S^1 par

$$(a, b) * (c, d) = (ac - bd,\ \ ad + bc)$$

pour $a, b, c, d \in \mathbb{R}$. On sait que $(S^1, *)$ est un groupe. Soit $f : \mathbb{R} \to S^1$ l'application définie par $f(x) = (\cos(2\pi x), \sin(2\pi x))$ pour $x \in \mathbb{R}$.

(a) Montrer que f est un homomorphisme de groupes entre $(\mathbb{R}, +)$ et $(S^1, *)$.

(b) Montrer que f est surjective et déterminer son noyau $\ker(f)$. L'application f est-elle un isomorphisme de groupes ?