Université d'Antananarivo **Faculté de Sciences**

Cours d'Algèbre 1

Andry Rabenantoandro et Christalin Razafindramahatsiaro

Table des matières

1 Théorie Naïve des Ensembles

1.1 Introduction et Définitions

Un `objet` est dit un `objet mathématiques` s'il a été formellement défini avec lequel on peut faire un raisonnement déductif et des preuves mathématiques. Ainsi, de manière naïve, on définit un `ensemble` comme une collection d'objets mathématiques rassemblés d'après, au moins, une propriété commune. Ces propriétés sont suffisants pour affirmer si un objet appartient ou pas à l'ensemble. Les objets sont appelés aussi `les éléments` de l'ensemble. Si x est un élément d'un ensemble E, on le notera tout simplement par : $x \in E$.
On notera aussi un ensemble en écrivant ses éléments séparés par des virgules entre deux accolades ou en indiquant les propriétés de ses éléments entre deux accolades. Ainsi, par exemple, on pourra noté l'ensemble des nombres entiers naturels pairs, soit par $\{0, 2, 4, 6, \ldots\}$, ou bien par $\{n \in \mathbb{N} | \text{n est pair}\}$.
Deux éléments d'un ensemble sont égaux s'il définissent le même objet mathématiques. Ainsi, l'ensemble

$$\{-3, 5, \{1, 2, 3\}, 2, 4, 2, \{2, 3, 1\}\}$$

définit le même ensemble que

$$\{-3, 5, 4, 2, \{2, 3, 1\}\}.$$

Exemples 1.1.1.
1. On désigne respectivement par $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ l'ensemble des entiers naturels, l'ensemble des entiers, l'ensemble des nombres rationnels, l'ensemble des nombres réels et l'ensemble des nombres complexes.
2. Considérons l'ensemble E des hommes fidèles et infidèles. Cet ensemble n'a pas d'élément puisqu'un tel homme n'existe pas. On appellera E l'ensemble vide, et on le notera par $\emptyset$, ou bien par $\{\}$.

Soient A et B deux ensembles. On dit que A est `inclus` dans B (qu'on notera par $A \subset B$) si tout élément de A est un élément de B. On dit aussi dans ce cas que l'ensemble A est `une partie ou sous-ensemble` de B. Ainsi, les deux ensembles sont égaux (qu'on notera par $A = B$) si $A \subset B$ et $B \subset A$.
Si E est un ensemble, on notera l'ensemble des parties de E par $\mathcal{P}(E)$.

Remarque 1.1.2. Soient E un ensemble quelconque et n un entier naturel.
1. L'ensemble vide est une partie de E;
2. Supposons de plus que l'ensemble E admet exactement n éléments : Alors l'ensemble $\mathcal{P}(E)$ admet exactement 2^n éléments.

Démonstration. Exercice à faire en cours. □

On définit l'ensemble $B \setminus A$ comme l'ensemble des éléments de B qui n'appartiennent pas à A. Si de plus, $A \subset B$, on notera l'ensemble $B \setminus A$ par C_B^A (ou tout simplement par A^c s'il n'y a pas de confusion). On appellera aussi l'ensemble C_B^A le complémentaire de A dans B.
Maintenant, on va introduire deux notions importants concernant les opérations sur les ensembles, à savoir : l'Intersection et l'Union.
L'ensemble qui ne contient que des éléments de A et B à la fois sera noté par $A \cap B$, tandis que l'ensemble qui ne contient, soit les éléments de A ou soit les éléments de B sera noté par $A \cup B$. Si

de plus, les ensembles A et B n'ont pas d'éléments en commun, on dit qu'ils sont `disjoints` et on a $A \cap B = \emptyset$.
Ainsi, on a les propriétés suivantes :

Proposition 1.1.3. *Soient A, B et C trois ensembles quelconques :*

1. $A \cap A = A \cup A = A$ *(Idempotente)* ;
2. $A \cap B = B \cap A, \quad A \cup B = B \cup A$ *(Commutativité)* ;
3. $A \setminus B = A \cap B^c$;
4. $(A \cup B)^c = A^c \cap B^c, \quad (A \cap B)^c = A^c \cup B^c$ *(Lois de Morgan)* ;
5. $A \cap (B \cap C) = (A \cap B) \cap C, \quad A \cup (B \cup C) = (A \cup B) \cup C$ *(Associativité)* ;
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(Distributivité)* ;
7. $B = \mathrm{C}_C^A \Leftrightarrow A \cup B = C$ *et* $A \cap B = \emptyset$.

Démonstration. Exercice. □

Soient A et B deux ensembles. L'ensemble produit définie par :

$$A \times B := \{(a, b) : \ a \in A, \ b \in B\}$$

est appelé `le produit cartésien` de A par B. Bien attendu, en général, on a $A \times B \neq B \times A$.
Enfin, si A et B sont deux parties d'un ensemble E, on dit que A et B sont `disjoints` si $A \cap B = \emptyset$.

Exercice 1 (Travaux dirigés). 1. Considérons les ensembles suivants : $A = \{1, 13, 25\}$; $B = \{\{1, 13\}, 25\}$; $C = \{\{1, 13, 25\}\}$; $D = \{\emptyset, 1, 13, 25\}$; $E = \{25, 1, 13\}$; $F = \{\{1, 13\}, \{25\}\}$; $G = \{\{25\}, \{1, 13\}, 25\}$; $H = \{\{1\}, \{13\}, 25\}$.

   a). Quelles sont les relations (d'égalité ou d'inclusion) qui existent entre ces ensembles ?

   b). Déterminer $A \cap B$; $\quad G \cup H$; $\quad E \setminus G$; $\quad \mathrm{C}_D^A$.

2. Soient A, B et C trois parties d'un ensemble E :

   a). Montrer que :

$$\begin{aligned} (A \cap B) \cup B^c &= A \cup B^c \\ (A \setminus B) \setminus C &= A \setminus (B \cup C) \\ A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C). \end{aligned}$$

   b). Simplifier : $(A \cup B)^c \cap (C \cup A^c)^c$; $\quad (A \cap B)^c \cup (C \cap A^c)^c$.

3. Démontrer la Proposition 1.3.

1.2 Applications

Dans cet section, considérons deux ensembles E et F.

Définition 1.2.1. Une application f de l'ensemble E dans l'ensemble F est une relation de correspondance qui à tout élément x de E, on associe un `unique` élément y de F. L'application f sera noté par :

$$\begin{aligned} f :& E \longrightarrow F \\ & x \longmapsto y{:=}f(x). \end{aligned}$$

Ainsi, si $y = f(x)$, on dit que l'élément y est `l'image` de x par f, tandis que x est `l'antécédent` de y par f. Bien attendu, les variables x et y sont muets. On pourra les notés par d'autres lettres. Par exemple, si e est un élément de E, $f(e)$ est l'image de e par f dans F.

Soit f une application de E dans F. Si A et B sont respectivement des sous-ensembles de E et F, les ensembles $f(A)$ et $f^{-1}(B)$ définies par :

$$f(A){:=}\{f(a) \in F : \quad a \in A\}, \quad f^{-1}(B){:=}\{a \in E : \quad \exists b \in B,\, b = f(a)\} = \{x \in E : \quad f(x) \in B\}$$

sont, respectivement, appelés `l'image de` A par f et `l'image réciproque de` B par f. En particulier, le sous-ensemble $f(E)$ de F sera noté par $\mathrm{Im}(f)$. Par définition, les ensembles $f(A)$ et $f^{-1}(B)$ sont respectivement des parties de F et E.
Soient f une application de E dans F et g une application de F dans G. On définit l'application (`la composée`) $g \circ f$ par :

$$\begin{aligned} g \circ f :& E \to G \\ & x \mapsto g(f(x)). \end{aligned}$$

Proposition 1.2.2. *Soit f une application de E dans F.*

1. *Soient A et B deux sous-ensembles de E, on a :*
   - *i).* $A \subset B \implies f(A) \subset f(B)$;
   - *ii).* $f(A \cup B) = f(A) \cup f(B)$;
   - *iii).* $f(A \cap B) \subset f(A) \cap f(B)$;
2. *Soient A et B deux sous-ensembles de F, on a :*
   - *i).* $A \subset B \implies f^{-1}(A) \subset f^{-1}(B)$;
   - *ii).* $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
   - *iii).* $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
   - *iv).* $f^{-1}(B \setminus A) = f^{-1}(B) \setminus f^{-1}(A)$.
3. *Soient $A \subset E$ et $B \subset F$. On a : $A \subset f^{-1}(f(A))$ et $f(f^{-1}(B)) = B \cap \mathrm{Im}(f)$.*
4. *Soit g une application de F dans G. Si A et B sont respectivement des parties de E et G, on a :*
   - *i).* $g \circ f(A) = g(f(A))$;
   - *ii).* $(g \circ f)^{-1}(B) = f^{-1}(g^{-1}(B))$.

Démonstration. Exercice. □

Définition 1.2.3. Soit f une application de E dans F. On dit que :

1. f est `injective` ou `une injection` si tout élément de $\mathrm{Im}(f)$ admet un unique antécédent, i.e, pour tout e_1 et e_2 éléments de E tels que $f(e_1) = f(e_2)$, on a, forcément $e_1 = e_2$;
2. f est `surjective` ou `une surjection` si $\mathrm{Im}(f) = F$, i.e, tout élément de F admet au moins un antécédent;
3. f est `bijective` ou `une bijection` si tout élément de F admet un unique antécédent, i.e, si elle est à la fois injective et bijective.

Exercice 2. Construisez des applications :

— Injective mais pas surjective;

— Surjective mais pas injective;

— Bijective;

— Ni injective ni surjective.

Solutions. A faire en classe. □

Proposition 1.2.4. *Soit f une application de E dans F. On a :*

1. *L'application f est injective si et seulement si pour tout partie A de E, $f^{-1}(f(A)) = A$;*
2. *L'application f est surjective si et seulement si pour tout partie B de F, $B = f(f^{-1}(B))$.*
3. *Considérons une application g de F dans G, on a :*
   - *i). Si f et g sont injectives, l'application $g \circ f$ est injective;*
   - *ii). Si f et g sont surjectives, l'application $g \circ f$ est surjective;*
   - *iii). Si $g \circ f$ est injective, l'application f est injective;*
   - *iii). Si $g \circ f$ est surjective, l'application g est surjective;*
   - *iv). Si l'application $g \circ f$ est bijective, l'application f est injective et l'application g est surjective.*

Démonstration. A faire en classe. □

Soit E un ensemble. L'application Id_E de E dans E qui à tout élément x de E, on associe $\mathrm{Id}_E(x) := x$ est appelée `l'application identique` de E.

Proposition 1.2.5. *Soit f une application de E dans F. L'application f est bijective si et seulement si il existe une application g de F dans E telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$. De plus, si f est une bijection, une telle application g est bijective et unique. Elle sera appelée `l'application inverse de` f. On la notera (par abus de notation) par f^{-1}.*

Démonstration. A faire en classe. □

Question 1.2.6. *Soit une application f de E dans F. La condition d'existence d'une application g telle que $g \circ f = \mathrm{Id}_E$ est -elle suffisante pour que f soit bijective? Si oui, donnez une preuve. Sinon, trouvez un contre exemple.*

Exercice 3 (Travaux dirigés). 1. Considérons les parties de $\mathbb{R}$ suivantes :

$$E = [0,1]\,;\ F = [-1,1]\,;\ G = [0,2]\,.$$

Soient f et g deux applications définies respectivement par :

$$\begin{aligned} f :& E \to G \\ & x \mapsto 2 - x; \\ g :& F \to G \\ & x \mapsto x^2 + 1. \end{aligned}$$

a). Déterminer $f(\{\frac{1}{2}\})$; $f^{-1}(\{0\})$; $g([-1,1])$; $g^{-1}([0,2])$.

b). Les applications f et g sont-elles bijectives ? Justifier votre réponse.

2. Démontrer la Proposition 1.5.
3. Question 1.9.

1.3 Dénombrabilité

Soit E un ensemble. On dit que E est `un ensemble fini` s'il possède un nombre fini d'éléments. Si ce n'est pas le cas, on dit que E est `infini`. Dans le cas où l'ensemble E est fini, on note le nombre d'éléments de E par $\#E$ ou par $\mathrm{Card}(E)$.

Proposition 1.3.1. *Soient E et F deux ensembles finis :*

1. *Le nombre d'applications de E dans F est $\#F^{\#E}$;*
2. *Soit f une application de E dans F :*
   - *i). Si f est injective, on a $\#E \leq \#F$. Le nombre d'applications injectives de E dans F est $\mathrm{A}_{\#F}^{\#E}$;*
   - *ii). Si f est surjective, on a $\#F \leq \#E$;*
   - *iii). Si f est bijective, on a $\#E = \#F$. Le nombre d'applications bijectives de E dans F est $(\#E)!$.*
3. *Il existe une application bijective de E dans F si et seulement si $\#E = \#F$.*

Démonstration. Exercice à faire en classe. □

Dans toute la suite, on notera par F^E l'ensemble des applications de E dans F.

Définition 1.3.2. Soit E un ensemble. On dit que E est `dénombrable` s'il existe une injection de E dans $\mathbb{N}$. Cela veut dire qu'on peut numéroter les éléments d'un ensemble dénombrable.

Exemples 1.3.3. L'ensemble des entiers naturels $\mathbb{N}$ est dénombrable. En particulier, les ensembles finis sont dénombrables.

Explications. A faire en cours. □

Proposition 1.3.4. *Soit E un ensemble dénombrable. L'ensemble E est infini si et seulement si il existe une bijection entre E et $\mathbb{N}$.*

Démonstration. A faire en classe. □

Exercice 4 (Travaux dirigés). 1. Montrer que $\mathbb{Z}$ est dénombrable.

2. Montrer que $\mathbb{N} \times \mathbb{N}$ est dénombrable. En déduire que le produit d'un nombre fini d'ensembles dénombrables est dénombrable.
3. Montrer que $\mathbb{Q}$ est dénombrable.
4. Soit $(E_n)_{n\in\mathbb{N}}$ une famille dénombrable de sous ensembles dénombrables d'un ensemble E. Montrer que la réunion $\cup_{n\in\mathbb{N}} E_n$ est dénombrable.
5. Montrer que l'ensemble des polynômes à coefficients entiers est dénombrable. En déduire que l'ensemble des sous-ensembles finis de $\mathbb{N}$ est dénombrable.
6. On dit qu'un nombre (réel ou complexe) est `algébrique` s'il est une racine d'un polynôme à coefficients entiers. Montrer que l'ensemble des nombres algébriques est dénombrable.
7. Existe-il une bijection entre $\mathbb{Q} \cap [0,1]$ et $\mathbb{Q} \cap]0,1[$?

Théorème 1.3.5 (Cantor)**.** *L'ensemble des nombres réels $\mathbb{R}$ n'est pas dénombrable. En particulier, l'ensemble des nombres irrationnels n'est pas dénombrable.*

Démonstration. A faire en classe. □

Corollaire 1.3.6. *Un nombre réel est dit `transcendant` s'il n'est pas algébrique. L'ensemble des nombres transcendants n'est pas dénombrable.*

Démonstration. A faire en classe. □

De manière générale,

Définition 1.3.7. Soient E et F deux ensembles. On dit que E et F sont `équipotents` s'il existe une bijection entre E et F.

Exemples 1.3.8. — Deux ensembles finis sont équipotents si et seulement si ils ont le même nombre d'éléments ;
— Deux ensembles dénombrables infinis sont toujours équipotents ;
— $\mathbb{Q}$ n'est pas équipotent à $\mathbb{R}$;

Proposition 1.3.9. *Tout intervalle non-réduit à un point est équipotent à $\mathbb{R}$.*

Démonstration. A faire en classe. □

Le résultat suivant permet la plus part du temps pour montrer que deux ensembles sont équipotents :

Théorème 1.3.10 (Cantor-Bernstein)**.** *Soient E et F deux ensembles. Si E est équipotent à un sous-ensemble de F et F est équipotent à un sous-ensemble de E, les ensembles E et F sont équipotents.*

Démonstration. On peut supposer que $E \subset F$ et qu'il existe un sous-ensemble A de E tel que A est équipotent à F.
Comme A est équipotent à F, il existe une bijection $f : F \to A$. Posons $C_0 := F \setminus E$. Alors, les ensembles $C_1 := f(C_0)$ et C_0 sont deux sous-ensembles disjoints de F. En effet, par définitions, $C_0 \subset F \setminus E$ et $C_1 \subset A \subset E$. De la même manière, on pose $C_2 := f(C_1)$. On a :

$$C_2 \subset f(A) \subset f(E) \subset A \subset E.$$

Or, par définition, les sous-ensembles C_1 et $f(E)$ sont disjoints. En effet, comme f est une bijection, on a $C_1 = f(F \setminus E) = f(F) \setminus f(E)$. Par conséquent, les ensembles C_0, C_1 et C_2 sont deux à deux disjoints. Ainsi, on construit une suite des sous-ensembles $(C_i)_{i\in\mathbb{N}}$ deux à deux disjoints de F définie par : $C_{i+1} = f(C_i)$. Posons :

$$C = \cup_{i\geq 0} C_i, \quad D = \cup_{i\geq 1} C_i.$$

La fonction f induit ainsi une bijection de C dans D. De plus, on a :

$$\begin{aligned} F \setminus C &= F \setminus (\cup_{i\geq 0} C_i) \\ &= F \cap (\cup_{i\geq 0} C_i)^c \\ &= F \cap (\cap_{i\geq 0} C_i^c) \\ &= (F \cap C_0^c) \cap (\cap_{i\geq 1} C_1^c) \\ &= (F \cap E) \cap (\cap_{i\geq 1} C_1^c) \\ &= E \setminus D. \end{aligned}$$

D'où, il existe bien une bijection de F dans E. □

Théorème 1.3.11 (Cantor)**.** *Soit E un ensemble. Les ensembles E et $\mathcal{P}(E)$ ne sont pas équipotents.*

Démonstration. Supposons par l'absurde qu'il existe une bijection $f : E \to \mathcal{P}(E)$. Considérons l'ensemble :

$$A := \{u \in E : \quad u \notin f(u)\}.$$

Par définition, l'ensemble A est une partie de E et qu'il existe alors un élément $p \in E$ tel que $A = f(p)$. Deux cas se présentent :

— Si $p \in A$: Alors, on a $p \in f(p)$. Or, par définition de A, c'est une contradiction ;

— Si $p \notin A$: Alors, on a aussi $p \notin f(p)$. Mais cela est aussi impossible.

D'où le résultat. □

Pour conclure cette section, on va énoncer la fameuse `hypothèse du continu.`
On sait qu'un sous ensemble de $\mathbb{N}$ qui n'est pas fini est équipotent à $\mathbb{N}$. Mais, est-ce qu'un sous-ensemble non dénombrable de $\mathbb{R}$, est-il équipotent à $\mathbb{R}$? La réponse affirmative à cette question est appelée `l'hypothèse du continu.` Cependant, on ne sait pas encore si c'est vraie ou fausse. En effet, notre théorie des ensembles est fondée principalement sur deux axiomes, à savoir : L'axiome du choix et l'axiome dit de Zermelo-Frenkel. C'est d'ailleurs la raison pour laquelle on a dit qu'on étudie plutôt la théorie naïve des ensembles. Avec ces deux axiomes, en 1963, Cohen a démontrer qu'il n'est pas possible de démontrer l'hypothèse du continu, ni son contraire.

Exercice 5 (Travaux dirigés).
1. En s'inspirant de la preuve du théorème 1.19, expliciter une bijection entre les intervalles $[a, b[$ et $]a, b[$.
2. Montrer que l'ensemble $\mathbb{N}^{\mathbb{N}}$ des suites d'entiers est équipotent à $\mathbb{R}$.
3. Montrer que l'ensemble des parties de $\mathbb{R}$ n'est ni dénombrable, ni équipotent à $\mathbb{R}$.
4. Montrer que l'ensemble $\mathbb{R}^{\mathbb{R}}$ n'est ni dénombrable, ni équipotent à $\mathbb{R}$.

1.4 Relations binaires sur un ensemble

Jusqu'à maintenant, on a globalement traité les ensembles par sa "taille" (sa cardinalité). On a quelques propriétés pour pouvoir comparer deux ensembles. Dans cette sous-section, on va regarder "plus à l'intérieur" d'un ensemble.
On sait depuis plusieurs années qu'on peut "comparer" tout les éléments de l'ensemble des entiers naturels $\mathbb{N}$. Cela veut dire qu'il existe une "relation" ($\leq$) entre deux entiers quelconques. Avec cette relation, on en déduit plus de propriétés de l'ensemble $\mathbb{N}$. Ainsi, notre but ici est de généraliser, puis formaliser cet idée d'existence possible d'une relation entre les éléments d'un ensemble. C'est le début de l'étude de ce qu'on appellera "un structure algébrique" dans un ensemble.
Soient E et F deux ensembles. Soient x et y deux éléments respectifs de E et F. Une correspondance entre x et y est appelée une `relation binaire` $\mathcal{R}$ entre x et y que l'on note par $x\mathcal{R}y$. Autrement dit, Une relation binaire $\mathcal{R}$ entre E et F est définie par une partie $\mathcal{G}$ du produit cartésien $E \times F$ telle que :

$$\mathcal{G} := \{(x, y) \in E \times F : \ x\mathcal{R}y\}.$$

En particulier, une relation binaire $\mathcal{R}$ sur l'ensemble E est une partie $\mathcal{G}$ de $E \times E$ telle que :

$$\mathcal{G} := \{(x, y) \in E \times E : \ x\mathcal{R}y\}.$$

Exemples 1.4.1.
1. L'inégalité $\leq$ est une relation binaire sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$;
2. L'orthogonalité et le parallélisme sont des relations binaires sur l'ensemble des droites de $\mathbb{R}^2$ ou $\mathbb{R}^3$;
3. L'inclusion $\subset$ est une relation binaire sur l'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E;
4. Le graphe d'une fonction numérique est une relation binaire sur $\mathbb{R}$.

Voici quelques caractéristiques d'une relation binaire sur un ensemble :

Définition 1.4.2. Soient E un ensemble et $\mathcal{T}$ une relation binaire sur E. On dit que :

i). $\mathcal{T}$ est `réflexive` si pour tout z élément de E, on a $z\mathcal{T}z$;

ii). $\mathcal{T}$ est `symétrique` si pour tout a et b éléments de E tels que $a\mathcal{T}b$, on a $b\mathcal{T}a$;

iii). $\mathcal{T}$ est `transitive` si pour tout x, y et z élément de E tels que $x\mathcal{T}y$ et $y\mathcal{T}z$, on a $x\mathcal{T}z$;

iv). $\mathcal{T}$ est `antisymétrique` si pour tout n et m élément de E tels que $n\mathcal{T}m$ et $m\mathcal{T}n$, on a $n = m$.

Soient $\mathcal{R}$ une relation sur un ensemble E et x un élément de E. Le sous-ensemble $\mathrm{Cl}_{\mathcal{R}_g}(x)$ (resp. $\mathrm{Cl}_{\mathcal{R}_d}(x)$) de E défini par :

$$\mathrm{Cl}_{\mathcal{R}_g}(x) := \{a \in E : \ x\mathcal{R}a\} \ (\text{resp. } \mathrm{Cl}_{\mathcal{R}_d}(x) := \{a \in E : \ a\mathcal{R}x\})$$

est appelé `le sous-ensemble de classe à gauche` (resp. `le sous-ensemble de classe à droite`) de l'élément x.

Remarque 1.4.3. Si la relation $\mathcal{R}$ est symétrique, on a $\mathrm{Cl}_{\mathcal{R}_g}(x) = \mathrm{Cl}_{\mathcal{R}_d}(x)$. Dans ce cas, on le note tout simplement par $\mathrm{Cl}_{\mathcal{R}}(x)$ ou par $\dot{x}$ ou par $\overline{x}$ et sera appelé `la classe d'équivalence` de l'élément x.

1.4.1 Relations d'équivalence

Définition 1.4.4. Une relation d'équivalence $\mathcal{R}$ sur un ensemble E est dite une relation d'équivalence si elle est à la fois réflexive, symétrique et transitive.

Exemples 1.4.5.
1. L'égalité sur un ensemble est une relation d'équivalence ;
2. Le parallélisme est une relation d'équivalence sur l'ensemble des droites de $\mathbb{R}^2$ ou de $\mathbb{R}^3$;
3. Soit f une application de E vers F. Le sous ensemble de E^2 défini par :

$$\left\{(a,b) \in E^2 : \ f(a) = f(b)\right\}$$

définit une relation d'équivalence sur E.

Définition 1.4.6. Soit E un ensemble non vide. `Une partition` de E est une famille de sous-ensembles non vides de E, deux à deux disjoints, dont la réunion est égal à E.

Proposition 1.4.7. *Soit $\mathcal{F}$ une relation d'équivalence sur un ensemble E. Si x et y deux éléments de E, on a :*

1. $x \in \mathrm{Cl}_{\mathcal{F}}(x)$;
2. $\dot{x} = \dot{y}$ *si et seulement si* $y \in \dot{x}$;
3. *Si* $y \notin \dot{x}$, *on a* $\dot{x} \cap \dot{y} = \emptyset$.

Démonstration. A faire en classe. □

Corollaire 1.4.8. *Soit E un ensemble non vide. L'ensemble des classes d'équivalence de E forme une partition de E. Inversement, toute partition d'un ensemble définit une relation d'équivalence.*

Démonstration. A faire en classe. □

Définition 1.4.9. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. L'ensemble $E/\mathcal{R}$ des classes d'équivalences défini par :

$$E/\mathcal{R} := \{\dot{y} : \ y \in E\}$$

est appelé `ensemble quotient` de E par $\mathcal{R}$. Ainsi, on en déduit une application de E vers $E/\mathcal{R}$ qui a $x \in$ E, on associe la classe $\dot{x}$. Cette application est appelé `la projection (ou surjection) canonique` de E dans $E/\mathcal{R}$.

En voici un exemple fondamental concernant les relations d'équivalences : Les congruences.
Soit n un entier naturel non nul. Pour tout entier a et b, on dit que a est `congruent` à b `modulo` n s'il a le même reste que b après division euclidienne par n. Autrement dit, a est congruent à b modulo n si n divise $a - b$. Si c'est le cas on écrit :

$$a \equiv b \bmod n.$$

cette relation est dite `la relation de congruence modulo` n. Elle sera notée par $n\mathbb{Z}$.

Proposition 1.4.10. *La relation binaire $n\mathbb{Z}$ est une relation d'équivalence sur $\mathbb{Z}$.*

Démonstration. A faire en classe. □

Soit a un entier. Par définition, la classe $\dot{a}$ est

$$\dot{a} := \{b \in \mathbb{Z} \mid a \equiv b \bmod n\} = a + n\mathbb{Z}.$$

Ainsi :

$$a \equiv b \bmod n \quad \text{si et seulement si} \quad \dot{a} = \dot{b}.$$

Finalement, l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est définie par :

$$\mathbb{Z}/n\mathbb{Z} := \{\dot{a} \mid a \in \mathbb{Z}\}.$$

Comme les restes possibles après division euclidienne par n sont : $0, 1, 2, \ldots, n-1$, on conclut que :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}.$$

Maintenant on va munir $\mathbb{Z}/n\mathbb{Z}$ de deux opérations binaires, à savoir l'addition et la multiplication, induites par celles de $\mathbb{Z}$. D'après les propriétés ci-dessus, on conclut qu'on a, pour tout $\dot{a}$ et $\dot{b}$ dans $\mathbb{Z}/n\mathbb{Z}$:

— $\overline{a} + \overline{b} = \overline{a+b}$;

— $\overline{a} \cdot \overline{b} = \overline{ab}$.

S'il n'y a pas de confusion, on pourra omettre la barre sur les entiers. Mais, l'étudiant doit se souvenir toujours dans quel ensemble il travaille.

Exemples 1.4.11. Pour $n = 6$, on a les tables suivantes :
Pour l'addition :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Pour la multiplication :

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Soit a un entier. On dit que $\overline{a}$ est `inversible` dans $\mathbb{Z}/n\mathbb{Z}$ s'il existe un entier u tel que

$$\overline{u} \cdot \overline{a} = \overline{1}$$

C'est à dire :

$$au \equiv 1 \bmod n.$$

Si c'est le cas, on dit que $\overline{u}$ est `l'inverse` de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$. Noter bien que $\overline{u}$ est aussi inversible et que $\overline{a}$ est son inverse.
L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté par $(\mathbb{Z}/n\mathbb{Z})^\times$. D'après la table de multiplication ci-dessus, on a par exemple :

$$(\mathbb{Z}/6\mathbb{Z})^\times = \left\{\overline{1}, \overline{5}\right\}.$$

L'inverse de $\overline{1}$ est lui-même, de même pour $\overline{5}$.

Théorème 1.4.12. *Soit a un entier. L'élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a et n sont premiers entre eux. C'est à dire :*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(a, n) = 1\}.$$

Preuve. Supposons que $\overline{a}$ est inversible. Donc, il existe un entier u tel que $au \equiv 1 \bmod n$. C'est à dire, il existe un entier v tel que $au = 1 + nv$. D'après le théorème de Bézout, comme $au - nv = 1$, où u et v sont des entiers, alors $\text{pgcd}(a, n) = 1$. Supposons maintenant que $\text{pgcd}(a, n) = 1$. D'après Bézout encore, ils existent deux entiers u et v tels que $au + nv = 1$. Dans, $\mathbb{Z}/n\mathbb{Z}$, on a $\overline{au + nv} = \overline{au} + \overline{nv} = \overline{au} = \overline{1}$ car $\overline{nv} = 0$. D'où $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. □

Ainsi, pour vérifier si un élément $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de calculer le pgcd de a et n. S'ils sont premiers entre eux, on conclut que $\overline{a}$ est inversible. Pour calculer l'inverse, on cherche un couple d'entier (u, v) tel que

$$au + nv = 1$$

en utilisant l'algorithme d'Euclide. Ainsi, l'inverse de $\overline{a}$ est $\overline{u}$.

1.4.2 Relations d'ordre

Définition 1.4.13. Soit $\mathcal{R}$ une relation sur un ensemble E. On dit que $\mathcal{R}$ est une `relation d'ordre` si elle est à la fois réflexive, antisymétrique et transitive. Deux éléments x et y de l'ensemble E sont dits `comparables` si $x\mathcal{R}y$ ou $y\mathcal{R}x$. Si de plus tout les éléments de E sont deux à deux comparables, on dit que l'ordre est `totale`. Sinon, l'ordre est dit `partiel`.

Exemples 1.4.14.
1. L'ordre usuelle $\leq$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou sur $\mathbb{R}$ est une relation d'ordre (Ordre total) ;
2. L'inclusion sur l'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E est une relation d'ordre (Ordre partiel) ;
3. La divisibilité sur l'ensemble des entiers $\mathbb{Z}$ est une relation d'ordre (Ordre partiel).

Noter bien que dans la plus part des cas, par abus, on notera une relation d'ordre par $\leq$.
Soient $(E, \leq)$ un ensemble ordonné et A une partie de E :

— Un élément M de E est appelé `un majorant` de A si pour tout élément x de A, on a $x \leq M$;

— Un élément m de E est appelé `un minorant` de A si pour tout élément x de A, on a $m \leq x$;

— Un élément de A est appelé `le plus grand élément` de A s'il majore tous les éléments de A et est noté par $\max(A)$;

— Un élément de A est appelé `le plus petit élément` de A s'il minore tous les éléments de A et est noté par $\min(A)$;

— Si l'ensemble des majorants de A admet un plus grand élément, cet élément est appelé `borne supérieure` et est noté $\sup(A)$;

— Si l'ensemble des majorants de A admet un plus grand élément, cet élément est appelé `borne inférieure` et est noté $\inf(A)$.

— Si A admet une borne supérieure, on dit que la partie A est `majorée`. Si A admet une borne inférieure, on dit que la partie A est `minorée`. Si de plus, elle est minorée et majorée, on dit que A est `bornée`.

Remarque 1.4.15. Si la partie A admet un maximum, elle admet une borne supérieure et on a $\max(A) = \sup(A)$. De même, si A admet un minimum, elle admet une borne inférieure et on a $\min(A) = \inf(A)$.

Exercice 6 (Travaux dirigés).

1. Montrer que les relations suivantes sont des relations d'équivalences :
   i). Le parallélisme sur l'ensemble des droites de $\mathbb{R}^2$ ou de $\mathbb{R}^3$;
   ii). Sur $\mathbb{R}^2$, $(x,y)\mathcal{R}(x',y')$ si et seulement si $x+y = x'+y'$.
2. Montrer que les relations suivantes sont des relations d'ordres partiels :
   i). L'inclusion sur l'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E;
   ii). La divisibilité sur l'ensemble des entiers $\mathbb{Z}$;
   iii). Sur $\mathbb{R}^2$, $(x,y)\mathcal{T}(x',y')$ si et seulement si $|x'-x| \leq y'-y$.
3. Soit $E = \mathbb{R}^2 \setminus \{(0,0)\}$. Considérons la relation binaire $\mathcal{R}$ sur E définie comme suit : Pour tout a et b dans E, $a\mathcal{R}b$ si et seulement si a et b appartiennent à une droite passant par $(0,0)$.
   i). Soient (x,y) et (x',y') deux éléments de E. Montrer que $(x,y)\mathcal{R}(x',y')$ si et seulement si il existe un nombre réel non nul λ tel que $(x,y) = \lambda(x',y')$.
   ii). Montrer que $\mathcal{R}$ est une relation d'équivalence.
   iii). Notons par $[x,y]$ la classe d'équivalence d'un élément (x,y) de E. Vérifier qu'on a $[x,1] = [y,1]$ si et seulement si $x = y$.
   iv). Montrer qu'on a : $E/\mathcal{R} = \{[x,1] : x \in \mathbb{R}\} \cup \{[1,0]\}$
4. (**Important.**) Soit f une application d'un ensemble E dans un ensemble F. On sait que la relation $\mathcal{R}$ définie pour tout a et b dans E, par :

$$a\mathcal{R}b \Leftrightarrow f(a) = f(b)$$

   est une relation d'équivalence.
   i). Montrer que l'application $\overline{f}$ de $E/\mathcal{R}$ dans F définie par $\overline{f}(\dot{a}) = f(a)$ est bien définie et est injective.
   ii). En déduire qu'on a $f = \overline{f} \circ g$ où l'application g est la projection canonique de E dans $E/\mathcal{R}$.
   iii). Montrer que si f est surjective, alors il existe une bijection entre $E/\mathcal{R}$ et F.

2 Equations Linéaires et Matrices

2.1 Vecteurs : Introduction

Avant de définir en general ce que c'est qu'un espace vectoriel, nous nous proposons dans cette section de traiter la notion de vecteur. Ceci nous fournit un exemple concret d'espace vectoriel et en même temps une motivation pour l' étude abstraite des espaces vectoriels plus tard.
Dans tout ce qui suivra $\mathbb{R}$ et $\mathbb{C}$ sont respectivement l'ensemble des nombres réels et l'ensemble des nombres complexes.

2.1.1 Vecteurs dans $\mathbb{R}^n$

Généralités

L'ensemble de tous les n-tuples ordonnés de nombres réels est noté $\mathbb{R}^n$ et est appelé *espace à n dimensions*. Tout élément $u = (u_1, u_2, \cdots, u_n) \in \mathbb{R}^n$ (écriture en ligne) est appelé *vecteur* (ou *point*) et les u_i sont appelés les *composantes* ou *coordonnées* de u. Graphiquement, pour $n = 2$ ou $n = 3$, un vecteur $u = (u_1, u_2, \cdots, u_n)$ est représenté dans le plan $\mathbb{R}^n$ par une flêche qui part de l'origine [1] $\mathbf{0} = (0, 0, \cdots, 0)$ et qui a pour sommet le point de coordonnées $(u_1, u_2, \cdots, u_n)$. PRENEZ GARDE à ne pas confondre avec la notion de vecteur $\overrightarrow{AB}$ introduit en classe de 3^{eme}, où A et B sont deux points quelconque, et qui est représenté graphiquement par une flêche qui part de A vers B.
Dans toute la suite, on développera la théorie dans le cas général où $n \in \mathbb{N}$ est un entier naturel fixé au préalable. Il est tout de même préférable d'avoir à notre disposition des interprétations graphiques sur lesquelles nos intuitions puissent se reposer. Ce qui est seulement possible quand $n = 2$ ou $n = 3$. On adoptera donc la convention suivante :

Les interprétations graphiques se feront dans le cas $n = 2$, i.e. dans le plan $\mathbb{R}^2$.

Définition 2.1.1 (Opérations sur les vecteurs)**.** Etant donnés deux vecteurs $u = (u_1, u_2, \cdots, u_n)$ et $v = (v_1, v_2, \cdots, v_n) \in \mathbb{R}^n$, et un élément $k \in \mathbb{R}$, on définit les opérations suivantes :

- **Addition** : $u + v = (u_1 + v_1, u_2 + v_2, \cdots, u_n + v_n)$.
- **Multiplication par un scalaire** : $ku = (ku_1, ku_2, \cdots, ku_n)$.

Dans ce cas, l'élément $k \in \mathbb{R}$ est appelé un *scalaire*.

On verra plus tard que $(\mathbb{R}^n, +, \cdot)$ où $\cdot$ représente la multiplication par un scalaire, forme une structure qu'on appelle espace vectoriel. Plus précisément, $(\mathbb{R}^n, +, \cdot)$ est un espace vectoriel sur $\mathbb{R}$ ou un $\mathbb{R}$-*espace vectoriel* où le $\mathbb{R}$ se réfère au corps des scalaires (on définira plus tard ce qu'est un corps).
On dit que l'addition el la multiplication par un scalaire se font composante par composante.

Définition 2.1.2 (Combinaison linéaire)**.** Etant donnés r vecteurs $u_1, u_2, \cdots, u_r$, une *combinaison linéaire* de $u_1, u_2, \cdots, u_2$ est une somme de la forme $k_1u_1 + k_2u_2 + \cdots + k_ru_r$ où les k_i sont des scalaires.

Exemples 2.1.3. Considérons le cas $n = 2$. On a $(1, 3) + (0, 2) = (1 + 0, 3 + 2) = (1, 5)$ et $\pi(1, 3) = (\pi, 3\pi)$. Le vecteur $\frac{1}{2}(1, 3) + (-2)(0, 2) = (\frac{1}{2}, \frac{3}{2}) + (0, -4) = (\frac{1}{2}, -\frac{5}{2})$ est une combinaison linéaire des vecteurs $(1, 3)$ et $(0, 2)$.

1. Indépendamment de n, l'origine sera toujours noté $\mathbf{0}$.

Interprétations graphique

— La somme $u + v$ est représenté par la flêche qui part de l'origine et dont le sommet forme un parallélogramme avec l'origine et les sommets de u et v.

— L'ensemble des points ku où u est un vecteur et k parcours $\mathbb{R}$ est la droite dirigée par le vecteur u.

— Etant donnés deux vecteurs non nulls u et v de $\mathbb{R}^2$. Quelle est l'ensemble de toutes les combinaisons linéaires $cu + dv$ de u et v ? Si u et v sont parallèles c'est une droite, sinon c'est tout le plan $\mathbb{R}^2$. Qu'en est-it de l'ensemble des combinaisons linéaires de trois vecteurs, quatre vecteurs, etc ? On verra que deux vecteurs suffisent pour "générer" $\mathbb{R}^2$.

MILA ASIANA SARY.

Le théorème suivant nous fournit les propriétés essentielles des opérations dans $\mathbb{R}^n$. Ce sont les propriétes que nous allons abstraire quand on étudiera les espaces vectoriels de manière abstraites.

Théorème 2.1.4. *Quels que soient les vecteurs $u, v, w \in \mathbb{R}^n$ et quels que soient les scalaires $k, l \in \mathbb{R}$, on a :*

(i) $(u + v) + w = u + (v + w)$ *(Associativité de l'addition)*

(ii) $u + v = v + u$ *(Commutativité de l'addition)*

(iii) $u + \mathbf{0} = u$ *($\mathbf{0}$ est l' élément neutre de l'addition)*

(iv) $u + (-u) = \mathbf{0}$ *($-u$ est l'inverse additive de u)*

(v) $k(u + v) = ku + kv$ *(Distributivité de la multiplication par un scalaire par rapport à l'addition)*

(vi) $(k + l)u = ku + lu$ *(La première addition est l'addition dans $\mathbb{R}$ tandis que la seconde est celle dans $\mathbb{R}^n$)*

(vii) $(kl)u = k(lu)$

(viii) $1u = u$.

Démonstration. Exercice facile laissé aux étudiants. □

2.1.2 Produit Scalaire, Norme et Distance

Définition 2.1.5 (Produit scalaire)**.** Soient $u = (u_1, u_2, \cdots, u_n)$ et $v = (v_1, v_2, \cdots, v_n)$ deux vecteurs de $\mathbb{R}^n$. Le produit scalaire de u et v est le scalaire défini par

$$u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

Définition 2.1.6. Deux vecteurs u et v sont dits *orthogonaux* ou *perpendiculaires* si $u \cdot v = 0$.

En effet, graphiquement, pour $n = 2$ ou $n = 3$, deux vecteurs non nulls sont orthogonaux si et seulement si leur produit scalaire est null. La notion d'orthogonalité n' est donc qu'une généralisation en dimension supérieure de la notion usuelle de perpendicularité.

Exemples 2.1.7. Les vecteurs $\mathbf{i} = (1, 0)$ et $\mathbf{j} = (0, 1)$ sont orthogonaux car $\mathbf{i} \cdot \mathbf{j} = 0 + 0 = 0$.

Nous donnons ensuite les propriétés remarquables du produit scalaire dans $\mathbb{R}^n$.

Théorème 2.1.8. *Soient $u, v, w \in \mathbb{R}^n$ et soit $k \in \mathbb{R}$.*

(i) $(u+v)\cdot w = u\cdot w + v\cdot w$

(ii) $(ku)\cdot v = k(u\cdot v)$

(iii) $u\cdot v = v\cdot u$

(iv) $u\cdot u \geq 0$

(v) $u\cdot u = 0$ *si et seulement si* $u = \mathbf{0}$.

Démonstration. Voir exercices. □

On dit que l'espace vectoriel $\mathbb{R}^n$ muni du produit scalaire est un *espace euclidien* de dimension n.

Définition 2.1.9. Soient deux vecteurs $u = (u_1, \cdots, u_n)$ et $v = (v_1, \cdots, v_n) \in \mathbb{R}^n$. La *distance* entre u et v est définie par $d(u,v) = \sqrt{(u_1-v_1)^2 + \cdots + (u_n-v_n)^2}$. La *norme* (ou *longueur*) du vecteur u est définie par $\|u\| = \sqrt{u\cdot u} = \sqrt{u_1^2 + \cdots + u_n^2}$. Un vecteur w appelé un vecteur *unitaire* si $\|w\| = 1$.

On observe que $d(u,v) = \|u - v\|$ et que pour tout vecteur $w \neq \mathbf{0}$, le vecteur $\frac{w}{\|w\|}$ est unitaire et de même direction que w. On rappelle que le cercle centré à l'origine et de rayon de longueur 1 est appelé le *cercle unité*.
En dimension 2, si nous considérons deux vecteurs $p = (a,b)$ et $q = (c,d)$, on voit facilement que $\|p\| = \sqrt{a^2+b^2}$ représente la longueur de la flêche représentant le vecteur p et $d(p,q) = \sqrt{(a-c)^2+(b-d)^2}$ représente la distance euclidienne qui sépare les pointes des flêches représentant p et q respectivement. On invite le lecteur a réfléchir sur le cas de la dimension 3.

MILA ASIANA SARY.

Exemples 2.1.10. Les vecteurs **i** et **j** sont unitaires. Compte tenu de la relation $\cos^2\theta_0 + \sin^2\theta_0 = 1$ pour tout $\theta_0 \in \mathbb{R}$, tout vecteur unitaire du plan xy s'écrit sous la forme $(\cos\theta, \sin\theta)$ où θ est l'angle que fait le vecteur par rapport à l'axe des x.
Le vecteur $u = (2,2,1)$ est de longueur 3 et $\frac{u}{\|u\|} = (\frac{2}{3}, \frac{2}{3}, \frac{1}{3})$ est unitaire (à vérifier).
Soit $v = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. On a $v\cdot v = \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 1$. Soit $w = (1,1,1,1)$, on a $\|w\| = 2$ donc $v = \frac{w}{\|w\|}$.

Proposition 2.1.11. *Si u et $v \in \mathbb{R}^n$ son orthogonaux, alors $\|u\|^2 + \|v\|^2 = \|u-v\|^2$.*

Démonstration. Voir exercices. □

Le théorème suivant nous fournit une inégalité fondamentale reliant le produit scalaire et la norme.

Théorème 2.1.12 (Cauchy-Schwarz)**.** *Quels que soient les vecteurs $u = (u_1, \cdots, u_n)$ et $v = (v_1, \cdots, v_n)$ de $\mathbb{R}^n$, on a :*

$$|u\cdot v| \leq \|u\|\|v\|.$$

Démonstration. Si $u = \mathbf{0}$ ou $v = \mathbf{0}$, l'inégalité est triviale. On peut donc supposer que $u \neq \mathbf{0}$ et $v \neq \mathbf{0}$. Le lecteur vérifiera que pour tout nombres réels a et b, on a $|a+b| \leq |a| + |b|$. Donc, il vient que

$$|u \cdot v| = |\sum_{i=1}^{n} u_i v_i| \leq \sum_{i=1}^{n} |u_i v_i|. \tag{1}$$

D'un autre côté, on invite le lecteur a vérifier que pour tout nombres réels a et b on a l'inégalité $ab \leq \frac{1}{2}(a^2 + b^2)$. Donc,

$$\begin{aligned} \frac{\sum_{i=1}^{n} |u_i v_i|}{\|u\|\|v\|} &= \sum_{i=1}^{n} \frac{|u_i||v_i|}{\|u\|\|v\|} \\ &\leq \sum_{i=1}^{n} \left[\frac{1}{2} \left(\frac{|u_i|^2}{\|u\|^2} + \frac{|v_i|^2}{\|v\|^2} \right) \right] \\ &= \frac{1}{2} \left(\sum_{i=1}^{n} \frac{|u_i|^2}{\|u\|^2} + \sum_{i=1}^{n} \frac{|v_i|^2}{\|v\|^2} \right) \\ &= 1. \end{aligned} \tag{2}$$

On a le résultat en combinant les inégalités (1) et (2). □

Le Théorème de Cauchy-Schwarz entraine que $-1 \leq \frac{u \cdot v}{\|u\|\|v\|} \leq 1$, donc il existe un unique $\theta \in [0, \pi]$ tel que $\cos\theta = \frac{u \cdot v}{\|u\|\|v\|}$. Ceci nous permet de généraliser la notion d'angle entre deux vecteurs de $\mathbb{R}^2$.

Définition 2.1.13. On définit l'angle θ entre deux vecteurs non null u et $v \in \mathbb{R}^n$ par :

$$\cos\theta = \frac{u \cdot v}{\|u\|\|v\|}.$$

Vérifiez qu'en dimension 2, θ est bien l'angle entre u et v.

MILA ASIANA SARY.

Proposition 2.1.14. *Quels que soient les vecteurs $u, v \in \mathbb{R}^n$ et quel que soit le scalaire $k \in \mathbb{R}$, la norme dans $\mathbb{R}^n$ satisfait les propriétés suivantes :*

(i) $\|u\| \geq 0$.

(ii) $\|u\| = 0$ *si et seulement si* $u = \mathbf{0}$.

(iii) $\|ku\| = |k|\|u\|$.

(iv) $\|u + v\| \leq \|u\| + \|v\|$ *(Inégalité triangulaire*[2]*).*

Démonstration. Voir exercices. □

2. Aussi connue sous le nom Inégalité de Minkowski.

2.2 Vecteurs dans $\mathbb{C}^n$

On rappelle qu'un nombre complexe $z \in \mathbb{C}$ est un nombre de la forme $a + ib$ où $a, b \in \mathbb{R}$ (la partie réelle et la partie imaginaire de z respectivement) et i vérifie $i^2 = -1$. Le *conjugué* de z est le nombre complexe $\bar{z} = a - ib$. Le *module* de z est le nombre réel positif $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$. Tout comme les nombres réels qui sont représentés par les points d'une droite, les nombres complexes peuvent être représentés dans le plan. En particulier, $z = a + ib$ est représenté par le point (a, b) du plan et le module $|z|$ est la distance du point z à l'origine.

MILA ASIANA SARY.

Nous rappellons les propriétés élémentaires suivantes.

Proposition 2.2.1. *Quels que soient $z, \omega \in \mathbb{C}$, on a :*

(i) $\overline{z + \omega} = \bar{z} + \overline{\omega}$.

(ii) $\overline{z\omega} = \bar{z}\,\overline{\omega}$.

(iii) $\bar{\bar{z}} = z$.

(iv) $|z\omega| = |z||\omega|$.

(v) $|z + \omega| \leq |z| + |\omega|$.

Démonstration. Voir exercices. □

Nous allons maintenant rapidement refaire ce qu'on a fait dans la section précédente. Dans toute la suite $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'*espace complexe* à n dimensions $\mathbb{C}^n$ est en effet à la fois un espace vectoriel sur $\mathbb{R}$ et un espace vectoriel sur $\mathbb{C}$. Bien que l'ensemble sous-jacent soit le même, on verra plus tard qu'il y a des différences entre les structures d'espace vectoriel sur $\mathbb{R}$ et sur $\mathbb{C}$.
Comme dans le cas réel, les éléments de $\mathbb{C}^n$ sont appelés *vecteurs* (ou *points*) et les éléments de $\mathbb{K}$ sont appelés *scalaires*. L'*addition* de deux vecteurs et la *multiplication par un scalaire* se font composante par composante comme dans le cas réel. Dans le cas complexe, le produit scalaire et la norme se définissent d'une manière légèrement différente du cas réel.

Définition 2.2.2 (Produit scalaire)**.** Soient $z = (z_1, \cdots, z_n)$ et $\omega = (\omega_1, \cdots, \omega_n)$ deux vecteurs de $\mathbb{C}^n$. On définit le produit scalaire de z et ω par :

$$z \cdot \omega = z_1\overline{\omega_1} + \cdots + z_n\overline{\omega_n}.$$

Il est facile de voir qu'avec cette définition $z \cdot z$ est un nombre réel positif, ce qui permet de définir la norme.

Définition 2.2.3 (Norme)**.** Soit $z = (z_1, \cdots, z_n) \in \mathbb{C}^n$, la *norme* de z est définie par :

$$\|z\| = \sqrt{z \cdot z} = \sqrt{|z_1|^2 + \cdots + |z_n|^2}.$$

Les notions d'orthogonalité et de distance se définissent de la même manière que dans le cas réel.

Exercice 7 (Travaux dirigés). 1. a). Déterminez si le vecteur $(1, 3, 5) \in \mathbb{R}^3$ est une combinaison linéaire de $(0, 1, 0)$, $(1, 4, 1)$ et $(1, 0, 1)$.

b). Déterminez si le vecteur $(1,1) \in \mathbb{R}^2$ est une combinaison linéaire de $(0,1),(1,4)$ et $(1,0)$. Dans le cas où la réponse est affirmative, est-ce que la représentation en tant que combinaison linéaire est unique ?

2. Décrivez le sous-ensemble de $\mathbb{R}^3$ formé par toutes les combinaisons linéaires des vecteurs $u = (1,1,0)$ et $v = (0,1,1)$. Trouvez un vecteur qui n'est pas combinaison linéaire de u et v.
3. Soient $u = (\pi, 0)$ et $v = (0,2)$. Décrivez les sous ensembles de $\mathbb{R}^2$ suivants :
   a). $\{cu | c \in \mathbb{N}\}$.
   b). $\{cu | c \geq 0\}$.
   c). $\{cu + dv | c \in \mathbb{N} \text{ et } d \in \mathbb{R}\}$.
4. Est-ce que le vecteur $w = (1,0)$ est une combinaison linéaire des vecteurs $u = (2,-1)$ et $v = (-1,2)$?
5. Si $u + v = (\frac{1}{2}, 4, 1)$ et $u - 2v = (1,0,2)$, calculez u et v.
6. Montrez que pour tout vecteur u, $0u = \mathbf{0}$.
7. Démontrez Théorème 2.1.4.
8. Démontrez Proposition 2.1.8.
9. Démontrez Proposition 2.1.11.
10. Pour deux vecteurs u et $v \in \mathbb{R}^2$, quand est-ce qu'on a l'égalité $|u \cdot v| = \|u\|\|v\|$? l'égalité $\|u + v\| = \|u\| + \|v\|$?
11. Démontrez Proposition 2.1.14. Pour l'inégalité triangulaire on pourra utiliser le Théorème de Cauchy-Schwarz.
12. Démontrez Proposition 2.2.1.
13. Montrez que pour $z, \omega \in \mathbb{C}^n$ et $k \in \mathbb{K}$ on a :
    a). $z \cdot \omega = \overline{\omega \cdot z}$.
    b). $(kz) \cdot \omega = z \cdot (k\omega)$.
    c). $z \cdot (k\omega) = \overline{k}(z \cdot \omega)$.

    (Comparer avel le cas réel).
14. a). Soient $u = (a,b)$ et $v = (c,d)$ deux vecteurs du plan. Trouver une condition nécessaire et suffisante pour que tout élément de $\mathbb{R}^2$ soit une combinaison linéaire de u et v.
    c). Trouver quatre vecteurs de $\mathbb{R}^4$ tels que tout vecteur de $\mathbb{R}^4$ soit une combinaison linéaire de ces vecteurs.
15. Si $\|u\| = 5$ et $\|v\| = 3$, quelles sont la plus petite et la plus grande valeurs de $\|u - v\|$? Même question pour $u \cdot v$.
16. Est-il possible d'avoir trois vecteurs du plan dont les produits scalaires (deux à deux) sont tous strictement négatifs ? Quand est-il dans $\mathbb{R}^3$?
17. Soient x, y et z trois nombres réels tels que $x + y + z = 0$. Trouver l'angle que les vecteurs $u = (x,y,z)$ et $v = (z,x,y)$ font entre eux.
18. Reprendre les résultats (théorèmes, propositions, lemmes, corollaires) de la section 2.1.1 et vérifiez si ils restent vrai ou deviennent faux (dans quel cas, fournir des contre-exemples) dans le cas complexe.

Résoudre des systèmes d'équations linéaires est l'un des problèmes les plus importants en algèbre. Dans cette section, on développera une méthode générale en utilisant des objets qui seront au centre de notre cours : `Les Matrices.`
Pour commencer, considérons le système d'équations, qu'on va résoudre dans $\mathbb{R}^2$, suivant :

$$\begin{cases} 2x - y &= 5 \\ 3x + 2y &= 4 \end{cases}.$$

On peut voir ce système de deux manières différentes :
1^{er} **point de vue :**
Ce système représente deux droites dans $\mathbb{R}^2$ d'équations respectives :

$$2x - y - 5 = 0, \quad 3x + 2y - 4 = 0.$$

Les deux droites ne sont pas parallèles, la solution est donc les coordonnées du point d'intersection qui est $(x = 2, y = -1)$.
2^{e} **point de vue :**
résoudre ce système est équivalent à répondre à la question suivante : Trouver la combinaison linéaire des vecteurs $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ et $\begin{pmatrix} -1 \\ 2 \end{pmatrix}$ qui donne le vecteur $\begin{pmatrix} 5 \\ 4 \end{pmatrix}$, i.e, trouver x et y, nombres réels, tels que :

$$x \begin{pmatrix} 2 \\ 3 \end{pmatrix} + y \begin{pmatrix} -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 4 \end{pmatrix}.$$

C'est dans ce deuxième point de vue qu'on va voir les choses la plus part du temps.

2.3 Matrices

Considérons les trois vecteurs de $\mathbb{R}^3$ suivants :

$$u = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad v = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \quad w = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Une combinaison linéaire de ces trois vecteurs est de la forme :

$$x_1 u + x_2 v + x_3 w = \begin{pmatrix} x_1 \\ x_2 - x_1 \\ x_3 - x_2 \end{pmatrix}$$

où x_1, x_2 et x_3 sont des scalaires.
Maintenant, on va réecrire cette combinaison en utilisant l'un des plus importants objets en algèbre linéaire : `Les Matrices.`
On va mettre les trois vecteurs dans `les colonnes de la matrice` A comme suit :

$$A := (u \quad v \quad w) = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}.$$

Posons $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3$. Ainsi, on définit le produit $A \cdot x$ (noté par Ax) comme suit :

$$Ax = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_1 u + x_2 v + x_3 w = \begin{pmatrix} x_1 \\ x_2 - x_1 \\ x_3 - x_2 \end{pmatrix}.$$

Par conséquent, Ax est un vecteur de $\mathbb{R}^3$ qui est une combinaison linéaire des vecteurs u, v et w.
De plus, si $b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$ est un vecteur de $\mathbb{R}^3$, `l'équation linéaire`

$$Ax = b$$

est un système de trois équations linéaires. La solution de ce système est :

$$\begin{cases} x_1 &= b_1 \\ x_2 &= b_1 + b_2 \\ x_3 &= b_1 + b_2 + b_3 \end{cases}.$$

Ainsi,

$$x = b_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + b_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = Sb,$$

où

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Remarque 2.3.1. Considérons l'équation linéaire dans $\mathbb{R}$:

$$ax = b$$

où a et b sont donnés et x est l'inconnu. La solution est :

$$x = \frac{b}{a} = a^{-1} b$$

si a est non nul.
De la même manière, pour résoudre l'équation $Ax = b$, on suggère de trouver une méthode pour trouver A^{-1}. On verra plus tard les conditions d'existence de la matrice A^{-1}. Ici,

$$A^{-1} = S.$$

Et, on dit dans ce cas que S est `l'inverse` de A. Par analogie, A est l'inverse de S.

Notons par u', v' et w' les vecteurs colonnes de la matrice S. On a :

$$Au' = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad Av' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad Aw' = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Ainsi, on obtient la matrice :

$$I_3 = (Au' \quad Av' \quad Aw') = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pour tout vecteur x de $\mathbb{R}^3$, on a :

$$I_3 x = x.$$

On appellera la matrice I_3, `la matrice identité de dimension` 3. Cela nous donne une idée assez clair sur comment on va faire la multiplication de deux matrices. Dans notre exemple, on a :

$$AS = (u \quad v \quad w)(u' \quad v' \quad w') = (Au' \quad Av' \quad Aw') = I_3$$

et

$$SA = (u' \quad v' \quad w')(u \quad v \quad w) = (Su \quad Sv \quad Sw) = I_3.$$

Avant de décrire les règles d'opérations sur les matrices, noter bien aussi la remarque suivante :

Remarque 2.3.2. Jusqu'à maintenant, on n'a adopté que le deuxième point de vue : "Le point de vue des colonnes". Bien évidemment, on peut voir aussi les matrices sur les lignes (Le premier point de vue). Posons :

$$x = (1, 0, 0), \quad y = (-1, 1, 0), \quad z = (0, -1, 1).$$

On a :

$$A = (u \quad v \quad w) = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Ainsi :

$$A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x \cdot (x_1, x_2, x_3) \\ y \cdot (x_1, x_2, x_3) \\ z \cdot (x_1, x_2, x_3) \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 - x_1 \\ x_3 - x_2 \end{pmatrix}.$$

Cela nous donne une deuxième façon de calculer $A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, ainsi que le produit de deux matrices.

2.3.1 Règles des Opérations pour les Matrices

Dans toute la suite, sauf mention explicite du contraire, m et n désignent deux entiers naturels non tous nuls.

Définition 2.3.3. Soient I et J deux ensembles d'indices. Une matrice A est une application :

$$\begin{aligned} A : & I \times J \longrightarrow \mathbb{K} \\ & (i, j) \longmapsto a_{ij} \end{aligned}$$

où $\mathbb{K}$ est l'ensemble de scalaires. Dans toute la suite, sauf mention explicite du contraire, les ensembles I et J sont finis et sont respectivement $\{1,2,\ldots,m\}$ et $\{1,2,\ldots,n\}$. Dans ce cas, on représentera la matrice A comme un tableau rectangulaire de dimension $m \times n$ dont les mn éléments sont des scalaires. Les nombres des lignes et des colonnes sont respectivement m et n. On note A par :

$$A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$$

où a_{ij} sont des scalaires ; ou simplement par

$$A = (a_{ij})$$

s'il n'y a pas de confusion. Le scalaire a_{ij} se trouve ainsi sur la i-ème ligne et la j-ème colonne de la matrice A. Les $n-$tuplets $(a_{i1} \quad \ldots \quad a_{in})$ sont appelés les vecteurs lignes de A tandis que les vecteurs de $\mathbb{K}^m$, $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ sont appelés les vecteurs colonnes de A.
Si de plus, $n = m$, on dit que la matrice A est une *matrice carrée* de dimension n. On notera par $M_n(\mathbb{K})$ l'ensemble des matrices carrées de dimension n (à coefficients dans $\mathbb{K}$).

Par définition, on peut considérer comme des matrices, les éléments de $\mathbb{R}^n$ ou $\mathbb{C}^n$. Ainsi, les vecteurs colonnes de $\mathbb{R}^n$ ou $\mathbb{C}^n$ sont des matrices de dimension $n \times 1$, tandis que les vecteurs lignes sont de dimension $1 \times n$. Comme dans le cas de ces vecteurs, on a l'addition et la multiplication par un scalaire entre les matrices. Par exemple :

$$\begin{pmatrix} 0 & 1 \\ 2 & 1 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 2 & 1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \\ 2 & 4 \end{pmatrix}; \quad -2 \begin{pmatrix} 0 & 1 \\ 2 & 1 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ -4 & -2 \\ -2 & -6 \end{pmatrix}.$$

Par conséquent :

Définition 2.3.4 (Addition de deux matrices et Multiplication par un scalaire). L'addition de deux matrices est bien définie si les deux matrices ont la même dimension. Ainsi, si $A = (a_{ij})$ et $B = (b_{ij})$ sont des matrices de dimension $m \times n$, on définit $A + B$ par :

$$A + B = (a_{ij} + b_{ij}).$$

Si k est un scalaire, on définit kA par :

$$kA = (ka_{ij}).$$

Définition 2.3.5 (Multiplication de deux Matrices). Soient A et B deux matrices de dimensions respectives $m \times n$ et $q \times p$. La multiplication $A \times B$ ou simplement AB est bien définie si le nombre de colonnes de A est égal au nombre de ligne de B, i.e, $n = q$. Ainsi, on définit AB par :

$$AB = (A\mathbf{b}_1 \quad \ldots \quad A\mathbf{b}_p)$$

Ou bien :

$$AB = \left(\mathbf{a}_i \cdot \mathbf{b}_j\right)_{1\leq i\leq m, 1\leq j\leq p}$$

où $A = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_m \end{pmatrix}$ avec $\mathbf{a}_i$ $(1 \leq i \leq m)$ sont les vecteurs lignes de A.

On remarque ainsi que chaque vecteur colonne de AB est une combinaison linéaire des colonnes de A. Mais encore, on a :

$$\big(\text{i-ème ligne de AB}\big) = \big(\text{i-ème ligne de A}\big) \times B$$

et

$$\big(\text{j-ème colonne de AB}\big) = \text{A} \times \text{(j-ième colonne de B)}.$$

Proposition 2.3.6 (Linéarité de la multiplication par une matrice)**.** *Soit A une matrice dans $M_n(\mathbb{K})$. Considérons trois vecteurs colonnes u, v et w de $\mathbb{K}^n$ tels que $w = au + bv$ où a et b sont des scalaires. Alors on a :*

$$Aw = aAu + bAv.$$

Preuve. Exercice. □

Proposition 2.3.7. *Soient A, B et C trois matrices et k un scalaire. On a :*

$$\begin{aligned}
A + B &= B + A && (\textit{Commutativité de l'addition}) \\
k(A + B) &= kA + kB && (\textit{Distributivité de la multiplication par un scalaire}) \\
A + (B + C) &= (A + B) + C && (\textit{Associativité de l'addition}) \\
AB &\neq BA && (\textit{Non commutativité de la multiplication}) \\
C(A + B) &= CA + CB && (\textit{Distributivité à gauche de la multiplication}) \\
(A + B)C &= AC + BC && (\textit{Distributivité à droite de la multiplication}) \\
A(BC) &= (AB)C && (\textit{Associativité de la multiplication})
\end{aligned}$$

Preuve. Exercice. □

Définition 2.3.8. La matrice de $M_n(\mathbb{K})$, qu'on notera par I_n (ou par I s'il n'y a pas de confusion), définie par :

$$I_n = (a_{ij})$$

où

$$a_{ij} = \begin{cases} 1 & \text{si } i = j; \\ 0 & \text{sinon.} \end{cases}$$

est appelée la matrice identité.

Remarque 2.3.9. On remarque que la matrice I commute avec toutes les matrices dans $M_n(\mathbb{K})$, i.e, pour toute matrice A dans $M_n(\mathbb{K})$, on a :

$$IA = AI.$$

Ainsi, si k est un scalaire, la matrice kI commute, elle aussi, avec toute les éléments de $M_n(\mathbb{K})$.

D'où la question suivante :

Question 2.3.10. *Peut-on trouver d'autres matrices (autres que kI) qui pourraient commuter avec toute les éléments de $M_n(\mathbb{K})$?*

Réponse. Exercice. □

Une dernière chose (importante) concernant la multiplication des matrices est ce qu'on appelle la *décomposition d'une matrice en blocs.* Considérons par exemple une décomposition de la matrice A en blocs suivante :

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & B \\ 0 & 0 & 1 & \\ \hline & O & & C \end{array}\right)$$

où

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad O = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Proposition 2.3.11. *Soient A et B deux matrices décomposées en blocs des matrices. Si le nombre des blocs sur une ligne de A est égal au nombre des blocs sur une colonne de B, la multiplication de $A \times B$ peut se faire blocs par blocs (suivant la règle de multiplication de deux matrices).*

Preuve. Exercice. □

Ainsi, on obtient une troisième manière de multiplier deux matrices qui suit :

Corollaire 2.3.12. *Soient A et B deux matrices tels que AB est bien défini. Pour tout $i = 1, 2, \ldots, n$, notons respectivement par a_i et b_i les vecteurs colonnes de A et les vecteurs lignes de B. Alors, on a :*

$$AB = a_1 b_1 + \ldots + a_n b_n.$$

Preuve. Exercice à faire pendant le cours. □

Voici un exemple :

$$\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} -3 & 3 \\ -1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 0 & 1 \end{pmatrix}.$$

2.3.2 Inverses

Soit A une matrice dans $M_{m\times n}(\mathbb{K})$. On dit que la matrice A admet *un inverse à gauche* (resp. *à droite*) s'il existe une matrice G (resp. une matrice D) dans $M_{n\times m}(\mathbb{K})$ tel que :

$$GA = I_n \text{ (resp. } AD = I_m).$$

Noter qu'en général (dans le cas où $m \neq n$), on peut vérifier que $G \neq D$.

Proposition 2.3.13. *Soit A une matrice inversible dans $M_n(\mathbb{K})$. Notons respectivement par G et D un inverse à gauche et un inverse à droite de A. Alors :*

$$G = D.$$

De plus, l'inverse de A est unique qu'on notera par A^{-1}. Ainsi, A est l'inverse de A^{-1}.

Preuve. Par définition, on a $GA = I_n$. En multipliant cet égalité à droite par D, on a $(GA)D = D$. Puisque la multiplication des matrices est associative, on a $(GA)D = G(AD) = G(I_n) = G$. D'où, $G = D$.
Maintenant, soient B_1 et B_2 deux inverses (à droite et à gauche) de A. D'après le résultat précédent, on peut considérer B_1 comme inverse à droite et B_2 comme inverse à gauche. D'après ce même résultat, on conclut que $B_1 = B_2$.

□

Dans toute la suite, quand on parle des inverses de matrices, on ne s'intéressera qu'au cas où la matrice est carrée. Ainsi, on notera par $\mathrm{GL}_n(\mathbb{K})$, le (sous-) ensemble des matrices inversibles de $M_n(\mathbb{K})$.

Proposition 2.3.14. *Soient A et B des matrices dans $\mathrm{GL}_n(\mathbb{K})$. On a :*

- *La matrice AB est aussi dans $\mathrm{GL}_n(\mathbb{K})$ (Stabilité par la multiplication) ;*
- *L'inverse de AB est $B^{-1}A^{-1}$.*

Preuve. Exercice. □

Une question s'impose :

Question 2.3.15. *Si A et B deux matrices inversibles, est-ce que $A + B$ est aussi inversible ?*

Réponse. Exercice. □

Proposition 2.3.16. *Soit A une matrice dans $M_n(\mathbb{K})$. La matrice A est inversible si et seulement si pour tout vecteur b de $\mathbb{K}^n$, il existe un unique solution dans $\mathbb{K}^n$ de l'équation :*

$$Ax = b.$$

Preuve. Supposons que A est inversible. Soit $b \in \mathbb{K}^n$ et considérons l'équation $Ax = b$. Donc, le vecteur $x = A^{-1}b$ est une solution. Si x' est une solution de l'équation, on a $Ax' = b$. En multipliant cet équation par A^{-1}, on a $x' = A^{-1}b = x$. Puisque A^{-1} est unique, d'où l'unicité de la solution.
Inversement, supposons maintenant que pour tout vecteur b de $\mathbb{K}^n$, il existe un unique solution dans $\mathbb{K}^n$ de l'équation :

$$Ax = b.$$

Pour tout $i = 1, 2, \ldots, n$, notons par b_i le i-ième colonne de la matrice identité I_n. Par hypothèse, il existe un unique x_i dans $\mathbb{R}^n$, solution de l'équation

$$Ax = b_i$$

pour tout $i = 1, 2, \ldots, n$. D'où :

$$A^{-1} = (x_1 \quad x_2 \quad \cdots \quad x_n)$$

est l'inverse de A. □

Remarque 2.3.17. On a, dans la preuve de la proposition précédente, une méthode pour calculer l'inverse d'une matrice.

On verra plus tard dans ce cours, des critères pour qu'une matrice soit inversible, ainsi que d'autres méthodes pour calculer l'inverse d'une matrice.

2.3.3 Dépendances et Indépendances

On a vu au tout début de ce cours, la définition d'une combinaison linéaire. Soient $u_1, u_2, \ldots, u_r$, r vecteurs de $\mathbb{K}^n$, on se demandait si un vecteur w dans $\mathbb{K}^n$ est une combinaison linéaire de ces r vecteurs. Maintenant, en particulier, on se demande s'il existe (au moins) un vecteur parmi les u_i qui soit (ou non) une combinaison linéaire des autres.

Définition 2.3.18. Soient $u_1, u_2, \ldots, u_r$, r vecteurs de $\mathbb{K}^n$. On dit que ces vecteurs sont *linéairement dépendants* s'ils existent $x_1, x_2, \ldots, x_r$ scalaires non tous nuls tels que :

$$x_1u_1 + x_2u_2 + \ldots + x_ru_r = 0.$$

Ils sont dits *linéairement indépendants* dans le cas contraire.

Proposition 2.3.19. *Soit A une matrice dans $M_n(\mathbb{K})$. La matrice A est inversible si et seulement si les vecteurs colonnes de A sont linéairement indépendants.*

Preuve. Pour tout $i = 1, 2, \ldots, n$, notons par u_i le i-ième colonne de A. D'après Proposition 2.3.16, l'équation $Ax = x_1u_1 + x_2u_2 + \ldots + x_nu_n = 0$ admet un unique solution. Or, le vecteur nul dans $\mathbb{K}^n$ est une solution de cet équation. D'où le résultat. □

Théorème 2.3.20. *Soit A une matrice dans $M_n(\mathbb{K})$. Les vecteurs colonnes de A sont linéairement indépendants si et seulement si les vecteurs lignes de A le sont aussi.*

Preuve. Notons par $u_1, u_2, \ldots, u_n$ les vecteurs lignes de A. Supposons que les vecteurs colonnes de A sont linéairement indépendants. D'après la proposition 2.3.19, la matrice A est inversible. Ainsi, en multipliant à droite par A^{-1}, l'équation

$$xA = x_1u_1 + x_2u_2 + \ldots + x_nu_n = 0$$

où $x = (x_1, x_2, \ldots, x_n)$ admet un unique solution (qui est le vecteur nul). D'où les vecteurs lignes sont aussi linéairement indépendants. La réciproque se démontre de la même manière.

□

Proposition 2.3.21. *Soit $A \in \mathrm{M}_n(\mathbb{K})$. L'équation*

$$Ax = 0$$

admet plusieurs (au moins deux) solutions si et seulement si A n'est pas inversible. Dans ce cas, on dit que la matrice A est `singulière`*.*

Preuve. Exercice. □

2.3.4 Transpositions et Permutations

Dans ce paragraphe, on va introduire deux opérateurs (importants) opérant sur les matrices à savoir : la Transposition et la Permutation.

Définition 2.3.22. Soit A une matrice. La matrice dont les colonnes sont respectivement les vecteurs lignes de A est appelée la `transposée` de A (qu'on notera par A^{T}). Plus précisément :

$$(A^{\mathrm{T}})_{ij} = A_{ji}.$$

En particulier, si $A \in \mathrm{M}_{m\times n}(\mathbb{K})$, la matrice A^{T} est dans $\mathrm{M}_{n\times m}(\mathbb{K})$.

Exemples 2.3.23. Si $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, la transposée de A est $A^{\mathrm{T}} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$.

Proposition 2.3.24. *Soient A et B deux matrices. Alors :*

i). $(A+B)^{\mathrm{T}} = A^{\mathrm{T}} + B^{\mathrm{T}}$;

ii). $(AB)^{\mathrm{T}} = B^{\mathrm{T}}A^{\mathrm{T}}$;

iii). Si A est inversible, alors A^{T} est aussi inversible avec $(A^{\mathrm{T}})^{-1} = (A^{-1})^{\mathrm{T}}$.

iv). $((A)^{\mathrm{T}})^{\mathrm{T}} = A$.

Preuve. Exercice.

□

Remarque 2.3.25. Soient A une matrice dans $\mathrm{M}_n(\mathbb{K})$ et x un vecteur colonne de $\mathbb{K}^n$. Le vecteur Ax est une combinaison linéaire des vecteurs colonnes de A tandis que $x^{\mathrm{T}}A$ est celle des vecteurs lignes de A.

Dans toute la suite, sauf mention explicite du contraire, tout vecteur de $\mathbb{K}^n$ sera considérer comme un vecteur colonne.

Remarque 2.3.26. Soient x et y deux vecteurs de $\mathbb{K}^n$. Alors on a :

$$x \cdot y = x^{\mathrm{T}}y.$$

Si de plus, A est une matrice dans $\mathrm{M}_n(\mathbb{K})$, on a :

$$(Ax)^{\mathrm{T}}y = x^{\mathrm{T}}(A^{\mathrm{T}}y).$$

Maintenant on va introduire quelques importantes classes de matrices.

Définition 2.3.27. Soient A une matrice dans $\mathrm{M}_n(\mathbb{K})$. On dit que A est `une matrice triangulaire supérieure` (resp. `inférieure`) si $a_{ij} = 0$ pour $i > j$ (resp. pour $i < j$).

Il est important de souligner que les matrices triangulaires (supérieures ou inférieures) joueront un très grand rôle dans la résolution des équations linéaires du type :

$$Ax = b$$

où A une matrice carrée, b un élément de $\mathbb{K}^n$ et x dans $\mathbb{K}^n$ est l'inconnu.

Remarque 2.3.28. Si A est une matrice triangulaire supérieure, sa transposée A^{T} est une matrice triangulaire inférieure, et inversement.

La classe des matrices suivante est l'une des plus importantes :

Définition 2.3.29. Soit $A = (a_{ij})$ une matrice dans $\mathrm{M}_n(\mathbb{K})$. La matrice est dite `symétrique` si $A^{\mathrm{T}} = A$, i.e, $a_{ij} = a_{ji}$.

Il est clair que si A est une matrice symétrique et inversible, alors l'inverse est aussi une matrice symétrique.

Proposition 2.3.30. *Soit A une matrice dans $\mathrm{M}_{m\times n}(\mathbb{K})$. La matrice $A^{\mathrm{T}}A$ dans $\mathrm{M}_n(\mathbb{K})$ est une matrice symétrique.*

Définition 2.3.31. Soit $A = (a_{ij})$ une matrice dans $\mathrm{M}_n(\mathbb{K})$. La matrice est dite `antisymétrique` si $A^{\mathrm{T}} = -A$, i.e, $a_{ij} = -a_{ji}$.

On verra plus tard (plus loin) l'importance de ces classes de matrices.
Soit A une matrice dans $\mathrm{M}_n(\mathbb{K})$. Notons par $u_1, u_2, \ldots, u_n$ les vecteurs ligne de A. Une question que l'on peut se poser est la suivante : Existe-t-il une matrice P qui permute (ou échange) deux ou plusieurs vecteurs lignes de A en la multipliant par P ? La réponse est OUI !
Par définition, la matrice identité I_n ne change rien sur A, i.e, $I_nA = A$. Par contre si P_{21} est la matrice qu'on obtient en permutant la première et la deuxième ligne de la matrice I_n, on a :

$$P_{21}A = \begin{pmatrix} u_2 \\ u_1 \\ u_3 \\ u_4 \\ \vdots \\ u_n \end{pmatrix}.$$

De manière générale, la matrice P_{ij} obtenue de la matrice identité après avoir permuté la i-ème ligne et la j-ème ligne permute la i-ème et la j-ème ligne de la matrice A. Ainsi :

Définition 2.3.32. Une matrice P est dite `une matrice de permutation` si P est le produit de matrices de type P_{ij}. L'ensemble des matrices de permutations dans $\mathrm{M}_n(\mathbb{K})$ est noté par P_n.

Proposition 2.3.33. *Soit P une matrice dans P_n. Alors :*

i). La matrice P est inversible avec $P^{-1} = P^{\mathrm{T}}$. En particulier, P^{-1} est aussi une matrice de permutation ;

ii). $P^n = I_n$;

iii). Le cardinal de l'ensemble P_n est $n!$.

Preuve. Exercice. □

2.4 Equations Linéaires

Avant de passer aux choses sérieuses, illustrons cette section avec l'un des fondations (Si ce n'est la fondation) de l'algèbre linéaire à savoir : La résolution d'un système d'équations linéaires.
Considérons le système suivant :

$$\begin{cases} 2x - y + z &= 1 \\ x + y + z &= 0 \\ x + y - 2z &= -1 \end{cases}$$

où $(x, y, z) \in \mathbb{K}^3$ est l'inconnu. En utilisant la méthode d'élimination, on peut avoir le système réduit (qui est plus facile à résoudre) qui suit :

$$\begin{cases} 2x - y + z &= 1 \\ -3y - z &= 1 \\ -6z &= -2 \end{cases}.$$

D'où :

$$\begin{cases} x &= \frac{1}{9} \\ y &= -\frac{4}{9} \\ z &= \frac{1}{3} \end{cases}.$$

.
Maintenant l'idée est de "revisiter" cette méthode en utilisant les matrices. La méthode est bien connue sous le nom : La méthode de pivot de Gauss.
Reprenons l'exemple ci-dessus :
Considérons l'équation linéaire suivante :

$$Ax = b$$

où $x \in \mathbb{K}^3$ est l'inconnu avec :

$$A = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -2 \end{pmatrix}; \quad b = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}.$$

Définition 2.4.1. Soit $A = (a_{ij})$ une matrice dans $\mathrm{M}_n(\mathbb{K})$. Une matrice E_{ij} vérifiant les deux propriétés suivantes :

i). La multiplication à gauche de A par E_{ij} ne change que la i-ième ligne de A;

ii). La (i, j) position de la matrice $E_{ij}A$ est zéro;

est appelée `une matrice d'élimination` du coefficient a_{ij} de A.

Proposition 2.4.2. *Soient $A = (a_{ij})$ une matrice dans $\mathrm{M}_n(\mathbb{K})$ et i, j et k trois entiers entre 1 et n avec $k < i$. Supposons que a_{kj} et a_{ij} sont non nuls. Alors, la matrice déduite de la matrice identité I_n en remplaçant seulement la (i, k) position par $-\frac{a_{ij}}{a_{kj}}$, est une matrice d'élimination du coefficient a_{ij} de A. On notera cette matrice par E_{ij}. De plus, La i-ième ligne de la matrice $E_{ij}A$ est égal à $-\frac{a_{ij}}{a_{kj}}L_k + L_i$ où L_k et L_i sont respectivement la k-ième ligne et la i-ième ligne de la matrice A.*

Preuve. Exercice. □

Proposition 2.4.3. *Les matrices d'éliminations sont inversibles. De plus, si $E = (e_{kl})$ est une matrice d'élimination de la (i, j) position d'une matrice donnée, la matrice inverse E^{-1} se déduit de la matrice E en remplaçant seulement la (i, j) position par $-e_{ij}$.*

Preuve. Exercice. □

En revenant à notre exemple, l'équation peut se réduire à :

$$A'x = b'$$

où

$$A' = E_{32}E_{31}E_{21}A = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3/2 & 1/2 \\ 0 & 0 & -3 \end{pmatrix}; \quad b' = E_{32}E_{31}E_{21}b = \begin{pmatrix} 1 \\ -1/2 \\ -1 \end{pmatrix}$$

avec

$$E_{21} = \begin{pmatrix} 1 & 0 & 0 \\ -1/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad E_{31} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1/2 & 0 & 1 \end{pmatrix}; \quad E_{32} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}.$$

Par conséquent, on retrouve le résultat :

$$\begin{cases} x &= \frac{1}{9} \\ y &= -\frac{4}{9} \\ z &= \frac{1}{3} \end{cases}.$$

.

Remarquons ainsi que, A se factorise comme suit :

$$A = LU$$

où L et U sont respectivement une matrice triangulaire inférieure et une matrice triangulaire supérieure, avec :

$$L = E_{21}^{-1}E_{31}^{-1}E_{32}^{-1}$$

où

$$E_{21}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad E_{31}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1/2 & 0 & 1 \end{pmatrix}; \quad E_{32}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Remarque 2.4.4. En général, dans le procédé de la méthode d'élimination de la Proposition 2.4.2, si le coefficient a_{ij} qu'on veut éliminer est déjà zéro, on ne fait rien, on passe au suivant qui est généralement $a_{(i+1)j}$ ou $a_{(i+1)(j+1)}$. Mais, plus important encore, on peut pas éliminer si $a_{kj} = 0$. Si c'est le cas, on permute les lignes de A jusqu'à ce qu'on obtienne un premier coefficient qui est non nul. On commence souvent par a_{11}.

D'où le résultat suivant :

Théorème 2.4.5 (Factorisation LU)**.** *Soit A une matrice carrée. Alors il existe une matrice de permutation P tel que A se factorise comme suit :*

$$PA = LU$$

où L et U sont respectivement une matrice triangulaire inférieure et une matrice triangulaire supérieure.

Preuve. Une explication sera donnée en cours magistral.

□

Remarque 2.4.6. Maintenant, on sait que toute matrice carré A peut s'écrire de la forme :

$$PA = LU$$

comme l'indique le précédent théorème. Si de plus, la matrice A est inversible, il sera facile de trouver son inverse en utilisant cette factorisation en utilisant le fait qu'il est "facile" de trouver les inverses des matrices d'élimination ainsi que les matrices triangulaires.

Exercice 8 (Travaux dirigés). Dans toute la suite, sauf mention explicite du contraire, $\mathbb{K}$ désignera le corps des nombres réels $\mathbb{R}$ ou le corps des nombres complexes $\mathbb{C}$.

1. Ecrire les deux problèmes suivants sous la forme $Ax = b$ où A est une matrice 2×2, puis donner une solution à chaque problème :
   a). Alice est deux fois plus jeune que Bob et la somme de leur age est 33 ;
   b). Les deux points $(2, 5)$ et $(3, 7)$ appartiennent à une droite d'équation $y = mx + c$. Trouver m et c.
2. Pour chacune des matrices suivantes, trouver le scalaire a pour que la matrice soit singulière (non inversible) :

$$\begin{pmatrix} 1 & 3 & 5 \\ 1 & 2 & 4 \\ 1 & 1 & a \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 & a \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}; \quad \begin{pmatrix} a & a & a \\ 2 & 1 & 5 \\ 3 & 3 & 6 \end{pmatrix}$$

3. Soit A une matrice dans $\mathrm{M}_3(\mathbb{K})$ telle qu'il existe un vecteur colonne non nul x dans $\mathbb{K}^3$ vérifiant $Ax = 0$.
   a). Montrer que les vecteurs colonnes de A forment un plan P dans $\mathbb{K}^3$.
   b). Montrer que P et x sont perpendiculaires.
4. Soit un système d'équations linéaires dans $\mathbb{K}^3$.
   a). Montrer que ce système ne peut pas avoir exactement deux solutions.
   b). Si (x, y, z) et (u, v, w) sont deux solutions du système, pouvez vous trouver un autre ?
5. Trouver les matrices matrices E et L telles que l'on ait :

$$EP_3 = P_2; \quad LP_3 = I_4$$

où

$$P_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix}; \quad P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

6. Considérons les matrices suivantes :

$$E_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & d & 1 & 0 \\ 0 & e & 0 & 1 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & f & 1 \end{pmatrix}.$$

Montrer que :

$$L = E_1E_2E_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & d & 1 & 0 \\ c & e & f & 1 \end{pmatrix}.$$

7. Calculer les inverses de trois matrices suivantes :

$$A = \begin{pmatrix} 1 & -a & 0 & 0 \\ 0 & 1 & -b & 0 \\ 0 & 0 & 1 & -c \\ 0 & 0 & 0 & 1 \end{pmatrix}; \quad B = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}; \quad K = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Calculer $4K^{-1}$ et $7K^{-1}$.

8. Soit A et B deux matrices carrées de même dimension.
   a). Montrer que $A(I + BA) = (I + AB)A$.
   b). En déduire que $I + BA$ est inversible si et seulement si $I + AB$ l'est aussi.
9. Un sous ensemble de $\mathrm{M}_n(\mathbb{K})$ est appelé *un groupe de matrices* si pour toutes A et B deux matrices de l'ensemble, on a : le produit AB et l'inverse de chaque élément sont dans l'ensemble.
   a). Montrer que si G est un groupe de matrices, la matrice identité I_n est automatiquement dans G;
   b). Montrer que : l'ensemble des matrices triangulaires inférieures telles que $a_{ii} = 1$; l'ensembles des matrices symétriques ; l'ensemble des matrices de permutations sont des groupes de matrices.
   c). Donner plus de groupes de matrices.
10. Ecrire une matrice dans $\mathrm{M}_3(\mathbb{K})$ de votre choix.
    a). Trouver deux matrices B et C telles que : $A = B + C$ et B et C soient respectivement symétrique et anti-symétrique.
    b). Ré-écrire B et C en fonction de A et A^{T}.
11. Factoriser les matrices suivantes (de la forme $A = LU$ ou $PA = LU$) :

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 & 2 \\ 0 & 3 & 8 \\ 2 & 1 & 1 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 2 & 3 & 4 \end{pmatrix}; \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix}.$$

3 Espaces Vectoriels et Sous-Espaces Vectoriels

Dans ce chapitre, nous allons étudier l'une des structures mathématiques fondamentales, étroitement liées à l'algèbre linéaire : *les espaces vectoriels*. Les espaces vectoriels fournissent un cadre général, et plus abstrait, pour l'étude des équations linéaires, des applications linéaires et des matrices entre autres. Dans le premier chapitre, on a vu quelques exemples d'espaces vectoriels, notemment $\mathbb{R}^n$ et $\mathbb{C}^n$, ainsi que quelques propriétés de ces derniers. Certaines de ces propriétés vont nous servir comme point de départ pour définir abstraitement ce qu'est un espace vectoriel (cf. Théorème 2.1.4), et de ce fait formeront les axiomes de base d'un espace vectoriel.
Dans tout ce chapitre, on fixe un "corps" des scalaires $\mathbb{K}$ (pour l'instant, $\mathbb{R}$ ou $\mathbb{C}$).

3.1 Espaces Vectoriels

Soit $V \neq \emptyset$ un ensemble non vide. Une *loi de composition interne* sur V est une application $\oplus : V \times V \to V$ qui à chaque pair d'éléments (u, v) de V associe un élément $\oplus(u, v)$ de V, que l'on notera $u \oplus v$. La loi $\oplus$ sera appelée *l'addition de* V. On dit que V est munie d'une *multiplication par les scalaires* de $\mathbb{K}$ s'il existe une application $\odot : \mathbb{K} \times V \to V$ qui à tout pair d'éléments (k, v) de $\mathbb{K} \times V$ associe un élément $\odot(k, v)$ de V, que l'on notera $k \odot v$.

Définition 3.1.1. Un *espace vectoriel sur* $\mathbb{K}$ ou $\mathbb{K}$-*espace vectoriel* est un ensemble non vide V possédant un élément spécial $\mathbf{0}$ qu'on apellera naturellement *le zéro* de V, muni d'une loi de composition interne $\oplus$ et d'une multiplication par les scalaires de $\mathbb{K}$ $\odot$, satisfaisant les axiomes suivantes : quels que $u, v, w \in V$ et quels que soient $k, l \in \mathbb{K}$, on a

(i) $(u \oplus v) \oplus w = u \oplus (v \oplus w)$ (Associativité de l'addition)

(ii) $u \oplus v = v \oplus u$ (Commutativité de l'addition)

(iii) $u \oplus \mathbf{0} = \mathbf{0} \oplus u = u$ ($\mathbf{0}$ est l' élément neutre de l'addition)

(iv) Il existe un élément $-u \in V$ tel que $u \oplus (-u) = \mathbf{0}$ ($-u$ est l'inverse additive de u)

(v) $k \odot (u + v) = k \odot u + k \odot v$ (Distributivité de la multiplication par un scalaire par rapport à l'addition)

(vi) $(k + l) \odot u = (k \odot u) \oplus (l \odot u)$ (La première addition est l'addition dans $\mathbb{K}$ tandis que la seconde est celle dans V)

(vii) $(kl) \odot u = k \odot (l \odot u)$

(viii) $1 \odot u = u$.

Remarque 3.1.2. Il faut prendre garde à ne pas confondre le zéro du corps de base $\mathbb{K}$, qu'on écrira $0_{\mathbb{K}}$ ou simplement 0, avec le zéro de V que l'on écrira $\mathbf{0}$ (le chiffre 0 en gras).

Remarque 3.1.3. Dans la définition précédente, on a utilisé les notations $\oplus$ et $\odot$ pour que l'on comprenne que l'addition dans un espace vectoriel n'est pas toujours l'addition usuelle ans $\mathbb{R}$ ou $\mathbb{C}$, de même pour la multiplication par les scalaires. Cependant, pour la commodité, on convient dans toute la suite d'écrire $u + v$ au lieu de $u \oplus v$ et kv au lieu de $k \odot v$ du moment qu'aucune confusion n'est á craindre.

Les quatres premiers axiomes font de $(V, \oplus)$ ce qu'on appelle un *groupe abélien* ou *groupe commutatif*. L'axiome d'associativité de l'addition nous permet d'écrire une somme quelconque d'éléments de V de la forme

$$u_1 + u_2 + \cdots + u_n$$

sans écrire les parenthèses, et la commutativité implique que l'ordre de sommation n'est pas important.

Proposition 3.1.4. *L'élément neutre* $\mathbf{0}$ *est unique et pour tout* $u \in \mathbb{K}$*, l'opposé* $-u$ *de* u *est unique.*

Preuve. Exercice. □

On peut donc définir la soustraction dans V par : $u - v = u + (-v)$.

Corollaire 3.1.5 (Régularité de l'addition)**.** *Soient* $u, v, w \in \mathbb{K}$ *tels que* $u + v = u + w$*, donc* $v = w$*.*

Preuve. Exercice. □

On a les propriétés simple suivantes

Théorème 3.1.6. *Soit* V *un* $\mathbb{K}$*-espace vectoriel.*

(i) Pour tout $k \in \mathbb{K}$*,* $k\mathbf{0} = \mathbf{0}$*.*

(ii) Pour tout $u \in V$*,* $0u = \mathbf{0}$*.*

(iii) Si $ku = 0$ *avec* $k \in \mathbb{K}$ *et* $u \in V$*, alors* $k = 0$ *ou* $u = \mathbf{0}$*.*

(iv) Pour tout $k \in \mathbb{K}$ *et pour tout* $u \in V$*,* $(-k)u = k(-u) = -(ku)$*.*

Preuve. (i) Soit $k \in \mathbb{K}$, on a $k\mathbf{0} = k(\mathbf{0} - \mathbf{0}) = k\mathbf{0} - k\mathbf{0} = \mathbf{0}$.

(ii) Soit $u \in V$, on a $0u = (0 - 0)u = 0u - 0u = \mathbf{0}$.

(iii) Soient $k \in \mathbb{K}$ et $u \in V$ tels que $ku = \mathbf{0}$. Si $k \neq 0$, alors $\frac{1}{k}(ku) = \frac{1}{k}\mathbf{0} = \mathbf{0}$. De plus, on a $(\frac{1}{k}k)u = 1u = u$. Donc $u = 0$.

(iv) Il suffit d'appliquer l'axiome (vii) avec $l = -1$ et utiliser la commutativité de la multiplication dans $\mathbb{K}$.

□

Nous allons maintenant voir quelques exemples d'espace vectoriels.

Exemples 3.1.7. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ (ou un corps quelconque). On vérifie facilement que l'ensemble $\mathbb{K}^n$ des n-tuples d'éléments de $\mathbb{K}$ muni de l'addition et de la multiplication par les scalaires fait composantes par composantes est un espace vectoriel. Lélément neutre de l'addition est $\mathbf{0} = (0, 0, \cdots, 0)$ et bien sur $-(a_1, a_2, \cdots, a_n) = (-a_1, -a_2, \cdots, -a_n)$.

Exemples 3.1.8. On vérifie que $\mathrm{M}_{m\times n}(\mathbb{K})$ muni de l'addition des matrices et de la multiplication des matrices par un scalaire est un espace vectoriel. La matrice nulle où toutes les entrées sont 0 est lélément $\mathbf{0}$ et l'opposé se déduit facilement.

Exemples 3.1.9. Soit $V = \mathbb{K}[X] := \{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n | \ n \in \mathbb{N}, a_0, \cdots, a_n \in \mathbb{K}\}$ l'ensemble des polynômes en la variable X et á coefficients dans $\mathbb{K}$. Alors V muni de l'addition des polynômes (on additionne les coefficients correspondant aux mêmes puissances de X) et de la multiplication par un scalaire (multiplier les coefficients par le scalaire) est un espace vectoriel.

Exemples 3.1.10. Soit E un ensemble non vide et soit $\mathcal{F}(E, \mathbb{K})$ l'ensemble de toutes les applications de E dans $\mathbb{K}$. On munit $\mathcal{F}(E, \mathbb{K})$ de l'addition des applications et de la multiplication par un scalaire comme suit : pour tout $f, g \in \mathcal{F}(E, \mathbb{K})$ et $k \in \mathbb{K}$, on définit $f + g$ par

$$(f + g)(x) = f(x) + g(x)$$

et kf par

$$(kf)(x) = kf(x).$$

Lélément $\mathbf{0}$ est l'application nulle qui à chaque $x \in E$ associe 0.

La vérification de ces exemples est un exercice facile laissé aux étudiants.

3.2 Sous-Espaces Vectoriels

Définition 3.2.1. Un sous-ensemble non vide $W \subseteq V$ contenant $\mathbf{0}$ est un *sous-espace vectoriel* de V si W lui-même est un espace vectoriel par rapport aux lois d'addition et de multiplication par un scalaire de V.

Théorème 3.2.2. *$W \subseteq V$ est un sous-espace vectoriel de V si et seulement si :*

(i) $W \neq \emptyset$,

(ii) *W est fermé pour l'addition : $v, w \in W$ implique $v + w \in W$,*

(iii) *W est fermé pour la multiplication par un scalaire : $w \in W$ et $k \in \mathbb{K}$ implique $kw \in W$.*

Preuve. Exercice. □

Corollaire 3.2.3. *W est un sous-espace vectoriel de V si et seulement si*

(i) *$\mathbf{0} \in W$ (ou bien $W \neq \emptyset$) et*

(ii) *Pour tout $v, w \in W$ et pour tout $k, l \in \mathbb{K}$, $vk + wl \in W$.*

Preuve. Exercice. □

En particulier, $\{\mathbf{0}\}$ et V sont des sous-espaces vectoriels de V dites triviaux.
On laisse le soin de vérifier les quelques exemples suivant aux lecteurs :

Exemples 3.2.4. Soit le $\mathbb{R}$-espace vectoriel $V = \mathbb{R}^3$. L'ensemble W des vecteurs dont la dernière composante est 0 est un sous-espace vectoriel de V.

Exemples 3.2.5. L'ensemble des matrices symfriques de $M_n(\mathbb{K})$ est un sous-espace vectoriel de $M_n(\mathbb{K})$.

Exemples 3.2.6. Soit $V = \mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Le sous-ensemble des polynômes de degré inférieur ou égale à n est un sous-espace vectoriel de V.

Théorème 3.2.7. *L'intersection se sous-espaces vectoriels d'un espace vectoriel V est un sous-espace vectoriel de V. En particulier, toute intersection finie.*

Preuve. Exercice à faire en classe. □

Remarque 3.2.8. La réunion de deux sous-espaces vectoriels n'est pas forcément un espace vectoriel.

3.3 Combinaisons Linéaires et Générateurs

On a déja vu la notion de combinaison linéaire dans $\mathbb{K}^n$, il s'avère que cette notion peut se généraliser dans le cas d'un espace vectoriel quelconque. Soit V un $\mathbb{K}$-espace vectoriel et $v_1, v_2, \cdots, v_n \in V$. Un vecteur de la forme $a_1v_1 + a_2v_2 + \cdots + a_nv_n$ où les $a_i \in \mathbb{K}$ est appelé une *combinaison linéaire* de $v_1, v_2, \cdots, v_n$.

Définition 3.3.1. Soit $S \neq \emptyset$ un sous-ensemble non vide de V. Le plus petit sous-espace vectoriel de V contenant S, qu'on notera désormais $L(S)$ (une autre notation est Vect(S)), est appelé le sous-espace de V `engendré par` S. On dit que S est un `système générateur` ou une `famille génératrice` de $L(S)$, ou encore, que les éléments de S sont des `générateurs` de $L(S)$.

Lorsque $S = \{u_1, u_2, \cdots, u_m\}$, on écrira $L(S) = L(u_1, u_2, \cdots, u_m)$ s'il n'y a pas risque de confusion. On convient que $L(\emptyset) = \{\mathbf{0}\}$.

Définition 3.3.2 (Espace vectoriel de type fini)**.** Un espace vectoriel V est dit `de type fini` s'il peut être engendré par un nombre fini d'éléments.

Théorème 3.3.3. *Soit $S \subseteq V$ un sous-ensemble. Alors $L(S)$ est l'ensemble de toutes les combinaisons linéaires des éléments de S.*

Preuve. Soit W_S l'ensemble de toutes les combinaisons linéaires des éléments de S. D'une part,il est clair que $\mathbf{0} = 0\ s \in W_S$ $(s \in S)$. Aussi, on vérifie facilement que l'addition de deux combinaisons linéaires d' éléments de W_S est un élément de W_S. De même, la multiplication par un scalaire d'une combinaison linéaire d' éléments de W_S est un élément de W_S. Donc, W_S est un sous-espace vectoriel de V contenant S. Comme $L(S)$ est le plus petit sous-espace vectoriel de V contenant S, on a $L(S) \subseteq W_S$. D'autre part, $L(S)$ étant un sous-espace contenant S, donc $L(S)$ contient toute combinaison linéaire d'éléments de S. Donc, $W_S \subseteq L(S)$. Finalement, on a alors $L(S) = W_S$. □

Théorème 3.3.4. *Soit $S \subseteq V$ un sous-ensemble. Alors, $L(S)$ est l'intersection de toutes les sous-espaces vectoriels de V contenant S.*

Preuve. Exercice. □

Exemples 3.3.5. Soit le $\mathbb{R}$-espace vectoriel $V = \mathbb{R}^2$ et $v \in \mathbb{R}^2 \setminus \{\begin{pmatrix}0\\0\end{pmatrix}\}$. On peut se demander quel est le sous-espace engendré par v, ou $L(\{v\})$. D'après Théorème 3.3.3, $L(v) = \{\lambda v |\ \lambda \in \mathbb{R}\}$. C'est donc la droite passant par l'origine et v. Soit $w \notin L(v)$ un autre élément non null de V. On peut montrer que $L(v, w) = \mathbb{R}^2$ (que l'on fera plus tard).

Exemples 3.3.6. D'une manière similaire à l'exemple précédent, en prenant l'espace vectoriel $V = \mathbb{R}^3$, on peut montrer que si $v, w \in \mathbb{R}^3 \setminus \{\begin{pmatrix}0\\0\\0\end{pmatrix}\}$ tel que $w \notin L(v)$ alors $L(v, w)$ est le plan passant par l'origine et contenant v et w.

Exemples 3.3.7. Soit le $\mathbb{R}$-espace vectoriel $V = \mathbb{R}^n$. Les vecteurs $e_i = (0, \cdots, 1, \cdots, 0)$ où la i^{eme} est composante 1 et les autres 0, pour $i = 1, 2, \cdots, n$, engendrent V. En effet, tout élément $(a_1, a_2, \cdots, a_n) \in \mathbb{R}^n$ s'écrit $a_1e_1 + a_2e_2 + \cdots + a_ne_n$. Le sous-ensemble $\{e_1, \cdots, e_n\}$ s'appelle *la base canonique* de $\mathbb{R}^n$ (on y reviendra plus tard).

Exemples 3.3.8. Soit le $\mathbb{R}$-espace vectoriel $V = \mathbb{C}$). On sait que tout él'ement de $\mathbb{C}$ s'écrit sous la forme $a + ib$ où $a, b \in \mathbb{R}$. Donc, $\{1, i\}$ est un système générateur de $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel.

Exemples 3.3.9. Soit $V = \mathbb{K}[X]$. Les polynômes $1, t, t^2, \cdots$ engendrent V.

3.4 Espace Colonne d'une Matrice

Dans le chapitre précédent, on s'est intéressé en particulier à la résolution de systèmes de m équations linéaires à n inconnues. A un tel système on associe une matrice $A \in \mathrm{M}_{m\times n}(\mathbb{K})$, et on s'intéresse aux solutions de l'équation $Ax = b$, où $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ est l'inconnu et $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{K}^n$.
Rapellons que si A admet un inverse à gauche, alors l' équation admet au moins une solution en multipliant les membres de l'équation par une inverse de A (si $m = n$, alors A est inversible (avec une inverse unique) si et seulement si $Ax = b$ admet une solution unique). Une question importante s'impose : que se passe-t-il quand A n'est pas inversible ?
En général, le système peut être résolue pour certaines valeurs de b et ne peut pas être résolue pour les autres. On veut caractériser les valeurs de b pour lesquelles ce systême est résoluble, d'où l'importance de l'espace colonne de A.

Définition 3.4.1. L'*espace colonne* de la matrice $A \in \mathrm{M}_{m\times n}(\mathbb{K})$, qu'on écrira $\mathrm{C}(A)$, est le sous-espace de $\mathbb{K}^m$ engendré par les vecteurs colonnes de A. C'est donc l'ensemble de toutes les combinaisons linéaires possible des vecteurs colonnes de A.

En effet, on sait que $Ax = b$ implique que b est une combinaison linéaire des colonnes de A.

Proposition 3.4.2. *Le système $Ax = b$ est résoluble si et seulement si $b \in \mathrm{C}(A)$.*

Preuve. Si x est une solution, donc $b \in \mathrm{C}(A)$. Inversement, si $b \in \mathrm{C}(A)$, alors b est une combinaison linéaire des colonnes de A et les coefficients de cette combinaison linéaire nous fournit un solution x du système $Ax = b$. □

Exemples 3.4.3. L'espace colonne $C(A)$ de la matrice $A = \begin{pmatrix} 3 & 0 \\ 4 & 1 \\ 2 & 1 \end{pmatrix}$ est le sous-espace de R^3 engendré par $\begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, i.e. le plan contenant ces deux vecteurs. Notez bien que $A \in M_{3\times 2}(\mathbb{R})$ et que $C(A) \subseteq \mathbb{R}^3$.

Il est clair que $\mathbf{0} \in \mathrm{C}(A)$, ce qui indique en particulier que l'équation $Ax = \mathbf{0}$ admet au moins une solution, à savoir au moins la solution $x = \mathbf{0}$. Les sous-espaces vectoriels formés par les solutions de telles equations tiennent une place importante dans la théorie des espaces vectoriels. On y reviendra un peu plus tard.

3.5 Espace Ligne d'une Matrice

D'une manière analogue au cas des espaces colonnes, on a

Définition 3.5.1. L'*espace ligne* de la matrice $A \in \mathrm{M}_{m\times n}(\mathbb{K})$, qu'on écrira $\mathrm{R}(A)$, est le sous-espace de $\mathbb{K}^n$ engendré par les vecteurs lignes de A. C'est donc l'ensemble de toutes les combinaisons linéaires possible des vecteurs lignes de A.

Remarque 3.5.2. La notation $\mathrm{R}(A)$ vient de l'anglais "row" qui signifie "ligne". Aussi, la notation $L(\cdot)$ est réservé aux sous-espaces engendrés par des éléments de l'espace vectoriel en question.

Théorème 3.5.3. *Soient $A = (a_{ij}) \in \mathrm{M}_n(\mathbb{K})$, P_n une matrice de permutation et E_{ij} une matrice d'élimination de la composante a_{ij} de A. Alors,* $\mathrm{R}(P_nA) = \mathrm{R}(E_{ij}A) = \mathrm{R}(A)$.

Preuve. Exercice. □

3.6 Espace Nulle d'une Matrice

Soit $A = (a_{ij}) \in \mathrm{M}_{m\times n}(\mathbb{K})$ une matrice $m \times n$.

Définition 3.6.1. L'`espace nulle` de A, que l'on écrira $\mathrm{N}(A)$, est l'ensemble des vecteurs colonnes $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ de $\mathbb{K}^n$ tels que $Ax = \mathbf{0}$.

L'espace nulle $\mathrm{N}(A)$ est donc l'ensemble des solutions d'un système homogène (tous les monômes ont même degré) d'equations linéaires, comme on le voit

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Théorème 3.6.2. *L'espace nulle* $\mathrm{N}(A)$ *est un sous-espace vectoriel de* $\mathbb{K}^n$.

Preuve. Il est clair que $\mathrm{N}(A) \neq \emptyset$ car $\mathbf{0} \in \mathrm{N}(A)$. Il suffit alors de montrer la stabilité par addition et par multiplication par un scalaire. Soient $x, y \in \mathrm{N}(A)$. On a $A(x+y) = Ax + Ay = \mathbf{0} + \mathbf{0} = \mathbf{0}$, donc $x + y \in \mathrm{N}(A)$. Soit $k \in \mathbb{K}$ et $x \in \mathrm{N}(A)$. On a $A(kx) = (kA)x = k(Ax) = k\mathbf{0} = \mathbf{0}$, donc $kx \in \mathrm{N}(A)$. □

Une méthode, entre autres, pour montrer qu'un sous-ensemble de $\mathbb{K}^n$ est donc un sous-espace vectoriel est de montrer que le sous-ensemble en question est l'espace nulle d'une matrice. En général, tout sous-espace vectoriel de $\mathbb{K}^n$ est l'espace nulle d'une matrice. Pour l'instant, on n'a pas assez de matériels pour prouver cette derniére assertion.

Exemples 3.6.3. Considérons le plan de $\mathbb{R}^3$ déquation : $2x + y - 3z = 0$. On remarque que cette équation est équivalente à $\begin{pmatrix} 2 & 1 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, i.e. que le plan en question est l'espace nulle de la matrice $A = \begin{pmatrix} 2 & 1 & -3 \end{pmatrix}$.

3.7 Sommes et Sommes Directes

Soit V un $\mathbb{K}$-espace vectoriel. Soient U et W deux sous-espaces de V. On définit un nouveau sous-ensemble de V.

Définition 3.7.1. La `somme` de U et W est le sous-ensemble de V défini par

$$U + W := \{u + w | \ u \in U, w \in W\}.$$

Théorème 3.7.2. *La somme $U + W$ de deux sous-espaces U et W de V est un sous-espace vectoriel.*

Preuve. Exercice. □

Définition 3.7.3. On dit que la somme $U + W$ est une `somme directe` si pour tout $t \in U + W$, il existe un unique couple $(u, w) \in U \times W$ tel que $t = u + w$. En d'autre termes, la somme est directe si la décomposition de tout élément de $U + W$ en somme d'un élément de U et d'un élément de W est unique. Dans ce cas, on écrit $U \oplus W$.

Cette définition s'étend sans aucune difficulté au cas d'un nombre fini de sous-espaces. On peut même définir la notion de somme directe d'une famille infinie, dénombrable ou non, de sous-espaces, mais on se limite au cas fini pour l'instant.

Théorème 3.7.4. *L'espace vectoriel V est la somme directe des sous-espaces U et W si et seulement si :*

(i) $V = U + W$ *et*

(ii) $U \cap W = \{\mathbf{0}\}$.

Preuve. Supposons que $V = U \oplus W$. Il est clair que $V = U + W$. Si $t \in U \cap W$ avec $t \neq \mathbf{0}$, alors pour $u \in U$ et $w \in W$, on a $s = u + w = (u + t) + (w - t)$ deux représentations différentes de $s \in U + W$ en tant que somme d'un élément de U et d'un élément de W et la somme ne serait pas directe. Donc $t = \mathbf{0}$ et ainsi, $U \cap W = \{\mathbf{0}\}$. Inversement, supposons que $V = U + W$ et $U \cap W = \{\mathbf{0}\}$. Soit $t = u_1 + w_1 = u_2 + w_2 \in U + W$. Donc, $u_1 - u_2 = w_2 - w_1$. Ainsi, $u_1 - u_2 \in U \cap V = \{\mathbf{0}\}$, ce qui implique que $u_1 = u_2$. DE la même manière, $w_1 = w_2$. Donc, la représentation de t est unique, et ainsi la somme est directe. □

Exercice 9 (Travaux dirigés).

1. Donnez un exemple montrant que la réunion de deux sous-espaces vectoriels n'est pas forcément un espace vectoriel.
2. Soit $V = \mathbb{K}^{\mathbb{N}}$ l'ensemble de toutes les suites $(a_1, a_2, a_3, \cdots)$ déléments de $\mathbb{K}$ muni de l'addition par composante et de la multiplication par un scalaire par composante. Vérifiez que V est un $\mathbb{K}$-espace vectoriel. Notons $\mathbb{K}^{(\mathbb{N})}$ le sous-ensemble des suites à support fini, i.e., les suites dont tous les termes sont nuls sauf un nombre fini d'entre eux. Montrez que $\mathbb{K}^{(\mathbb{N})}$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$.
3. Est-ce que le sous-ensemble de $\mathbb{R}^2$ suivant est un espace vectoriel sur $\mathbb{R}$?

   $$E = \{(x, y) \in \mathbb{R}^2 | \ x \geq 0\}.$$

   Expliquez.
4. Décidez, dans chacun des cas suivant, si $V = \mathbb{R}^2$ muni des lois d'additions et de multiplications par un scalaire données sont des espaces vectoriels sur $\mathbb{R}$ ou non (justifiez en cas de réponse négative) :

i). $(a,b)+(c,d)=(a+b,c+d)$ et $k(a,b)=(ka,b)$.

ii). $(a,b)+(c,d)=(a+b)$ et $k(a,b)=(ka,kb)$.

iii). $(a,b)+(c,d)=(a+b,c+d)$ et $k(a,b)=(k^2a,k^2b)$.

5. Considérons le système d'equations linéaires en les inconnus $x_1,\cdots,x_n$ et à coefficients dans $\mathbb{R}$ suivant :

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n&=0\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n&=0\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots&\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n&=0 \end{aligned}$$

Un tel système est dit *homogène* (toutes les monômes ont le même degré, ici 1). Montrez que l'ensemble de toutes les solutions de ce système forme un sous-espace vectoriel de $\mathbb{R}^n$. Si le systéme linéaire n'est pas homogène, est-ce que l'ensemble des solutions forme toujours un espace vectoriel ? Si oui, démontrez, si non donnez un contre-exemple.

6. Soit $V=\mathcal{F}(E,\mathbb{K})$ comme dans Exemples 3.1.10 avec $\mathbb{K}=\mathbb{R}$. Montrez que le sous ensemble W de $\mathcal{F}(E,\mathbb{K})$ des fonctions bornées dans V est un sous-espace vectoriel. On rappelle qu'une fonction f á valeur réelle est bornée s'il existe un nombre réel $M\in\mathbb{R}$ tel que $|fx|\leq M$ pour tout $x\in E$.

7. Donnez un système générateur de $\mathbb{C}^2$ en tant que $\mathbb{C}$-espace vectoriel, puis en tant que $\mathbb{R}$-espace vectoriel.

8. Soit $V=\mathbb{R}^4$ en tant que $\mathbb{R}$-espace vectoriel. Déterminez si $v=(3,9,-4,-2)$ appartient au sous-espace de V engendré par $u_1=(1,-2,0,3)$, $u_2=(2,3,0,-1)$ et $u_3=(2,-1,2,1)$.

9. Décrivez les espaces colonnes des matrices suivantes :

a). $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

b). $A=\begin{pmatrix}2&3\\1&\frac{3}{2}\end{pmatrix}$.

c). $A=\begin{pmatrix}1&2&3\\0&0&4\end{pmatrix}$.

10. a). Décrivez un sous-espace de $\mathrm{M}_2(\mathbb{R})$ contenant $A=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ mais pas $B=\begin{pmatrix}0&0\\0&-1\end{pmatrix}$.

b). Si un sous-espace de $\mathrm{M}_2(\mathbb{R})$ contient A et B, est-ce que ce sous-espace doit contenir I_2 ?

c). Décrivez un sous-espace de $\mathrm{M}_2(\mathbb{R})$ ne contenant aucune matrice diagonale non-nulle. Une matrice carée est dite `diagonale` si tous ses coefficients qui ne sont pas sur la diagonale sont nuls.

11. Vrai ou faux, justifiez votre réponse :

a). L'ensemble des matrices symétriques de $\mathrm{M}_n(\mathbb{K})$ forme un sous-espace vectoriel.

b). L'ensemble des matrices antisymétriques de $\mathrm{M}_n(\mathbb{K})$ forme un sous-espace vectoriel.

c). L'ensemble des matrices de $\mathrm{M}_n(\mathbb{K})$ qui ne sont pas symétriques forme un sous-espace vectoriel.

12. Vrai ou faux, justifiez votre réponse :
    a). Les éléments b qui ne sont pas dans $C(A)$ (pour une matrice A) forme un sous-espace.
    b). Si $C(A) = \mathbf{0}$, alors A est la matrice nulle.
    c). Soit $A \in \mathrm{M}_{m\times n}(\mathbb{R})$, alors $C(2A) = C(A)$.
    d). Soit $A \in \mathrm{M}_n(\mathbb{K})$, alors $C(A - I_n) = C(A)$

3.8 Base et Dimension

Dans cette section, on fixe un corps $\mathbb{K}$. On va aborder les notions fondamentales de base et de dimension d'un espace vectoriel.

3.8.1 Base

Avant de traiter le cas général, revenons d'abord au cas du $\mathbb{R}$-espace vectoriel $\mathbb{C}$. On sait que tout nombre complexe z est une combinaison linéaire à coefficients réels de 1 et de i, i.e. $z = a + ib$ où $a, b \in \mathbb{R}$, ou encore que $L(1, i) = \mathbb{C}$ (i.e. $\{1, i\}$ engendre $\mathbb{C}$) en tant que $\mathbb{R}$-espace vectoriel. En plus, cette écriture est UNIQUE, ce qui revient à dire que si $z = a + ib = a' + ib'$ alors $a = a'$ et $b = b'$ (ce qui équivaut à dire que si $z = a + ib = 0$ alors $a = b = 0$). On dit que $\{1, i\}$ est une base de $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel. De la même manière, on voit que tout élément, disons (a, b), du $\mathbb{R}$-espace vectoriel $\mathbb{R}^2$ s'écrit de maniére unique comme $(a, b) = ae_1 + be_2$ où $e_1 = (1, 0)$ et $e_2 = (0, 1)$. Dans chacun des deux cas ci-dessus, les vecteurs 1 et i pour $\mathbb{C}$ et les vecteurs e_1 et e_2 pour $\mathbb{R}^2$, ont les ont deux propriétés fondamentales qui incarnent la notion de base : ils suffisent pour décrire tout él'ement de l'espace ent tant que leurs combinaisons linéaires, et chaque écriture est unique. On peut faire le même exercice pour $\mathbb{C}^n$, $\mathbb{R}^n$ et d'autres espaces vectoriels. Dans ce paragraphe, nous allons formaliser ces notions.

Définition 3.8.1 (Indépendance linéaire)**.** Soit V un $\mathbb{K}$-espace vectoriel et $E \subseteq V$ un sous-ensemble (fini ou infini). On dit que les vecteurs de E sont `linéairement indépendants` (ou, par abus, que E est linéairement indépendant), ou que E forme une `famille libre` de vecteurs, si :

$$\forall n \in \mathbb{N} \setminus \{0\}, \forall a_1, a_2, \cdots, a_n \in \mathbb{K} \text{ et } \forall v_1, v_2, \cdots, v_n \in E : \left(\sum_{i=1}^{n} a_i v_i = \mathbf{0} \Rightarrow a_1 = a_2 = \cdots = a_n = 0 \right).$$

Sinon, on dit que les vecteurs de E sont `linéairement dépendants` (ou, par abus, que E est linéairement dépendant), ou encore que E forme une famille `liée`.

Ainsi, $v_1, v_2, \cdots, v_m \in V$ sont linéairement indépendants si l'égalité

$$a_1 v_1 + a_2 v_2 + \cdots + a_m v_m = 0, \;\; a_1, a_2, \cdots a_m \in \mathbb{K},$$

implique

$$a_1 = a_2 = \cdots = a_m = 0.$$

Remarquons que si l'un des $v_i \in E$ est le vecteur null, alors les vecteurs de E sont forcément linéairement dépendants.

Exemples 3.8.2. Considérons le $\mathbb{R}$-espace vectoriel $\mathbb{R}^3$. Soient les vecteurs $u = (1, -1, 0)$, $v = (1, 3, -1)$ et $w = (5, 3, -2)$. Comme $3u + 2v - w = 0$, ces vecteurs sont linéairement dépendants.

Exemples 3.8.3. Soit le $\mathbb{R}$-espace vectoriel $V = \mathbb{R}[X]$. Soient $f(X) = 1 + X^2$ et $g(X) = 3 + 2X^3 + X^5$. Si $a_1, a_2 \in \mathbb{R}$ tels que $a_1 f(X) + a_2 g(X) = 0$, alors $a_1 + 3a_2 + a_1 X^2 + 2a_2 X^3 + a_2 X^5 = 0$. Donc $a_1 = a_2 = 0$ et ainsi $f(X)$ et $g(X)$ sont linéairement indépendants.

Proposition 3.8.4. *Soit $m \geq 2$. Les vecteurs $v_1, v_2, \cdots, v_m$ sont linéairement dépendants si et seulement si l'un d'entre eux est la combinaison linéaire des autres.*

Démonstration. Exercice. □

Définition 3.8.5 (Base)**.** On appelle un sous-ensemble $\mathcal{B}$ d'un espace vectoriel V `une base` de V si $\mathcal{B}$ engendre V et si $\mathcal{B}$ forme une famille libre de vecteurs.

Proposition 3.8.6. *Une famille $\mathcal{B}$ de vecteurs d'un espace vectoriel V est une base si et seulement si tout vecteur $v \in V$ s'écrit de manière unique comme combinaison linéaire d'élements de $\mathcal{B}$:*

$$v = a_1 v_1 + \cdots + a_n v_n.$$

Démonstration. Exercice. □

Exemples 3.8.7. Considérons le $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$. Soit $e_1, e_2, \cdots, e_n$ les vecteurs définis comme dans l'exemple 3.3.7. On vérifie facilement que $\{e_1, \cdots, e_n\}$ est une base de V que l'on appelle `base canonique`.

Exemples 3.8.8. Soit le $\mathbb{K}$-espace vectoriel $V = \mathbb{K}[X]$. L'ensemble $\mathcal{B} = \{X^i |\ i = 0, 1, 2, \cdots\}$ forme une base de V.

Le théorème suivant caracterise les bases finis, auxquelles on va se réduire la plupart du temps.

Théorème 3.8.9. *Soit V un $\mathbb{K}$-espace vectoriel et $\mathcal{B} = \{v_1, v_2, \cdots, v_n\} \subseteq V$ un sous-ensemble fini. Les assertions suivantes sont équivalentes :*

(i) *$\mathcal{B}$ est une base de V.*

(ii) *$\mathcal{B}$ est un ensemble minimal de générateurs de V, i.e. : E engendre V mais pout tout $v \in \mathcal{B}$, $\mathcal{B} \setminus \{v\}$ n'engendre pas V.*

(iii) *Tout $v \in V$ s' écrit comme $v = \sum_{i=1}^{n} a_i v_i$ de manière unique, i.e. avec des uniques $a_1, a_2, \cdots, a_n$.*

(iv) *$\mathcal{B}$ est un ensemble maximal linéairement indépendant, i.e. : les vecteurs de $\mathcal{B}$ sont linéairement indépendant mais pour tout $v \notin \mathcal{B}$, les vecteurs de l'ensemble $\mathcal{B} \cup \{v\}$ sont linéairement dépendants.*

Démonstration. A faire (en classe). □

Corollaire 3.8.10. *Soit V un $\mathbb{K}$-espace vectoriel et $E \subseteq V$ un sous-ensemble fini qui engendre V. Alors, V possède une base contenue dans E.*

Démonstration. On enlève successivement des éléments de E et on utilise le théorème 3.8.9. □

3.8.2 Dimension

La "dimension" est un invariant fondamental des espaces vectoriels qui permet en quelque sorte de mesurer leurs "tailles". C'est un peu plus pertinent que la cardinalité (qui mesure la "taille" d'un ensemble) car la dimension prends en compte la structure d'espace vectoriel.

Lemme 3.8.11. *Soient V un $\mathbb{K}$-espace vectoriel de type fini et $\mathcal{B} = \{w_1, w_2, \cdots, w_n\}$ une base de V. Soit $\omega = \sum_{i=1}^{n} a_i w_i \in V$ ($a_i \in \mathbb{K}$). Si $a_j \neq 0$, alors $\mathcal{B}' = \{w_1, w_2, \cdots, w_{j-1}, \omega, w_{j+1}, \cdots, w_n\}$ est une base de V. On peut donc changer w_j en ω (avec $a_j \neq 0$) et on obtient encore une base.*

3.8.3 Déterminants

Exercice 10 (Travaux dirigés). 1. Considérons $\mathbb{R}^4$ en tant que $\mathbb{R}$-espace vectoriel. Montrez que les vecteurs suivants sont indépendants : $(6,2,3,4)$, $(0,5,-3,1)$ et $(0,0,7,-2)$.

2. Démontrez la Proposition 3.8.4.
3. Montrez que deux vecteurs sont linéairement dépendants si et seulement si l'un d'entre eux est un multiple de l'autre.
4. Vérifiez l'exemple 3.8.7.
5. Donnez une base du $\mathbb{R}$-espace vectoriel $V = \{(a,a,b) | a,b \in \mathbb{R}\}$.
6. Soit le $\mathbb{Q}$-espace vectoriel $V = \mathbb{Q}^3$ et $W \subseteq V$ le sous-espace engendré par $E = \{(1,2,3),(2,3,4),(3,5,7)\}$. Montrez que E n'est pas une base de V mais que $\{(1,2,3),(2,3,4)\}$ en est une.
7. Montrez que l'ensemble suivant est un $\mathbb{R}$-espace vectoriel :

$$V = \{f : \mathbb{N} \to \mathbb{R} |\ \exists S \subseteq \mathbb{N} \text{ fini }, \text{ pour tout } n \in \mathbb{N} \setminus S, f(n) = 0\}.$$

   Trouvez une base de V.
8. Démontrez la proposition 3.8.6.

3.9 Applications Linéaires

Exercice 11 (Travaux dirigés).

4 Introduction à la théorie des Groupes

On sait que l'ensemble $\mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$ est muni de deux opérations usuelles à savoir : L'addition et la multiplication. Un espace vectoriel est aussi muni d'une opération de telle sorte : L'addition de deux vecteurs. Cela donne un nouveau moyen de mieux comprendre ces ensembles et mieux encore : de les classifier. Ainsi, avec ces opérations, on a ce qu'on appellera des `structures algébriques` sur ces ensembles. Ainsi notre but est de formaliser ces idées de manière abstraite.

Définition 4.0.1. Soit E un ensemble. Une `opération binaire` (ou `loi de composition interne`) $\star$ sur E est définie par l'application :

$$\begin{aligned} E \times E &\to E \\ (x,y) &\mapsto x \star y. \end{aligned}$$

Autrement dit, pour tout x et y éléments de E, $x \star y$ est un élément de E et il est défini de manière unique. Un ensemble E muni d'une opération $\star$ sera noté par $(E, \star)$. S'il n'y a pas de confusion, l'opération $x \star y$ sera notée tout simplement par xy.
Si T est une partie de E, on dit que l'opération est `fermée` sur T, si la restriction de l'application sur $T \times T$ a pour image dans T. Autrement dit, pour tout x et y dans T, on a $x \star y \in T$. On dit aussi que la loi de composition sur T est interne.
Un opération binaire sur un ensemble E définit de ce qu'on appellera `une structure algébrique` sur E. Autrement dit, on dit que $(E, \star)$ est une structure algébrique.

Exemples 4.0.2.
1. L'addition, la soustraction et la multiplication sont des opérations binaires sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$;
2. La soustraction n'est une loi de composition interne sur $\mathbb{N}$;
3. L'addition et la multiplication des matrices carrées sont des opérations binaires ;
4. L'addition et la soustraction de vecteurs sont des opérations binaires sur les espaces vectoriels ;
5. Le produit vectoriel de deux vecteurs sur $\mathbb{R}^3$ est une opération binaire sur $\mathbb{R}^3$;
6. La loi de composition d'applications est une opération binaire sur l'ensemble $\mathbb{R}^{\mathbb{R}}$ des applications numériques ;
7. L'addition est une loi de composition interne sur l'ensemble des nombres paires ;
8. L'addition n'est pas une loi de composition interne sur l'ensemble des nombres impaires.

En primaire, on a appris les tables d'additions et de multiplications sur l'ensemble des entiers naturels. Ci dessous est une tentative de formaliser cet idée sur un ensemble fini :

Définition 4.0.3. Soit $(E, \star)$ un ensemble fini muni de l'opération binaire $\star$. Le tableau qui présente, pour tout élément x et y de E, les résultats qu'on obtient par la loi $\star$ est appelé `table de Cayley` de $(E, \star)$.

Exemples 4.0.4. Soit $(\{-1, 0, 1\}, \times)$ un ensemble où $\times$ est la multiplication usuelle sur $\mathbb{Z}$. Son table de Cayley est le suivant :

$\times$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

Voici quelques caractéristiques usuelles d'une opération binaire sur un ensemble :

Définition 4.0.5. Soit $(E, \star)$ un ensemble. On dit que :

i). La loi $\star$ est `associative` si pour tout x, y et z dans E, on a $x \star (y \star z) = (x \star y) \star z$;

ii). La loi $\star$ est `commutative` si pour tout a et b dans E, on a $a \star b = b \star a$;

iii). E admet `un élément neutre` ou `un identité` e si pour tout $x \in E$, on a $e \star x = x \star e = x$;

iv). Supposons que E admet un élément neutre e. Un élément t de E admet `un inverse` s'il existe un élément u de E tel que $t \star u = u \star t = e$.

Proposition 4.0.6. *Soit $(E, \star)$ une structure algébrique admettant un élément neutre. Alors :*

i). L'élément neutre est unique ;

ii). Si de plus, l'opération est associative, l'inverse d'un élément inversible est unique.

L'inverse d'un élément inversible x de E sera noté par x^{-1}.

Démonstration.
i). Supposons qu'on a deux éléments neutres e_1 et e_2. Par définition, on a $e_1 \star e_2 = e_1 = e_2 \star e_1 = e_2$. D'où $e_1 = e_2$, i.e, l'élément neutre est unique.

ii). Soit x un élément inversible de E. Désignons par e l'élément neutre. Supposons qu'ils existent deux inverses de y_1 et y_2 de x. Par définition, on a : $x \star y_1 = e = x \star y_2$. Donc, en multipliant cet égalité par y_1 à gauche, on a, par associativité de l'opération binaire, $(y_1 \star x) \star y_1 = (y_1 \star x) \star y_2$. D'où, $y_1 = y_2$.

□

4.1 Introduction et Définitions

Définition 4.1.1. Une structure algébrique $(E, \star)$ est dite `un monoïde` si elle admet un élément neutre et la loi de composition interne $\star$ est associative. Si de plus, tout élément de E admet un inverse, alors la structure $(E, \star)$ est appelé `un groupe`. Une structure de groupe est dite `abélienne` si la loi de composition est aussi commutative. On dit dans ce cas que le groupe est `abélien`.

Remarque 4.1.2. Si $(E, \star)$ est un monoïde, l'ensemble E est non vide.

Proposition 4.1.3. *Soient $(M_1, \star_1)$ et $(M_2, \star_2)$ deux monoïdes d'éléments neutres respectifs e_1 et e_2. Considérons l'opération binaire $\star$ sur l'ensemble produit $G{:=}M_1 \times M_2$ définie par :*

$$\begin{aligned} G \times G &\to G \\ ((a,x),(b,y)) &\mapsto (a,x) \star (b,y){:=}(a \star_1 b, x \star_2 y). \end{aligned}$$

La structure $(G, \star)$ est un monoïde d'élément neutre (e_1, e_2). C'est ainsi qu'on définit une structure algébrique sur un produit cartésien de deux ensembles.

Démonstration. A faire en classe. □

Exemples 4.1.4.

1. $(\mathbb{R}, \times)$ est un monoïde ;
2. $(\mathbb{N}, +)$ n'est pas un groupe mais c'est un monoïde ;
3. $(\mathbb{Z} \setminus \{0\}, \times)$ est un monoïde, mais pas un groupe ;
4. Soit $n \geq 3$. Les structures $(\mathbb{Z}/n\mathbb{Z} \setminus \{\dot{0}\}, \times)$ et $(\mathrm{M}_n(\mathbb{R}) \setminus \{0\}, \times)$ ne sont pas de groupes en général mais des monoïdes ;
5. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens ;
6. $(\mathbb{R}^2, +)$ est un groupe abélien ;
7. Soit n un entier naturel non nul. Les structures $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathrm{M}_n(\mathbb{R}), +)$ sont des groupes abéliens ;
8. Soient n et m deux entiers naturels non nuls. La structure $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ est un groupe abélien ;
9. Si V est un espace vectoriel, la structure $(V, +)$ est un groupe abélien ;
10. L'ensemble des rotations de centre $(0,0)$ sur $\mathbb{R}^2$ définit un groupe abélien avec la loi composition des transformations ;
11. L'ensemble des applications numériques bijectives définit un groupe non abélien avec la loi de composition des applications ;
12. L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices carrées inversibles d'ordre $n \geq 2$ à coefficients dans $\mathbb{R}$ définit un groupe non abélien avec la loi multiplication des matrices ;
13. Soit E un ensemble fini. L'ensemble $\mathrm{P}(E)$ des applications bijectives de E dans E définit un groupe avec la loi de composition des applications. On appelera cet groupe, `le groupe de permutation` de l'ensemble E. Si E est de cardinal n, on notera cet groupe par S_n.

Dans toute la suite, on ne s'intéressera qu'à des structures de groupes. C'est l'objectif principal de notre cours d'algèbre 1 même si l'étude des monoïdes est une branche très riche de l'algèbre abstraite.

Définition 4.1.5. Soient $(G, \star)$ un groupe et H une partie de G. On dit que H est un `sous-groupe` de G si $(H, \star)$ est un groupe. Si H est un sous-groupe de G, on le notera par $H < G$.

Proposition 4.1.6. *Soit $(G, \star)$ un groupe. Une partie H de G est un sous-groupe de G si et seulement si les propositions suivantes sont vérifiées :*

i). Pour tout x et y dans H, on a $x \star y \in H$;

ii). L'élément neutre de G est dans H;

iii). Si x est un élément de H, l'inverse x^{-1} de x dans G appartient à H.

Autrement dit, une partie non-vide H de $(G, \star)$ est un sous-groupe de G si et seulement si pour tout x et y dans H, on a $x \star y^{-1}$ appartient à H.

Démonstration. Exercice. □

Exemples 4.1.7. Soit n un entier naturel non nul.

1. Si $(G, \star)$ est un groupe d'identité e, les parties G et $\{e\}$ sont des sous-groupes de G. On les appelle `les sous-groupes triviaux` de G. Un sous groupe non trivial de G sera appelé un `sous-groupe propre` de G;
2. $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$;
3. Le sous-ensemble $n\mathbb{Z}$ des multiples de n dans $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$;
4. Le sous-ensemble des matrices d'ordre n à coefficient dans $\mathbb{R}$ dont le déterminant est égal à 1 est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. Ce sous-groupe sera noté par $\mathrm{SL}_n(\mathbb{R})$ et sera appelé `le groupe linéaire spécial.`
5. Soit $E = \{1, 2, \ldots, n\}$. Le groupe S_n est un sous groupe de S_{n+1}. Si $k \in \{1, 2, \ldots, n\}$, le sous ensemble des éléments qui fixe k dans $\mathrm{P}(E)$ est un sous-groupe de S_n;
6. Si $n \leq 3$, les sous groupes triviaux sont les seuls sous groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$;
7. Le sous ensemble $\{0, 2\}$ est le seul sou groupe propre de $(\mathbb{Z}/4\mathbb{Z}, +)$;
8. Les sous ensembles $\{(0,0), (0,1)\}$ et $\{(0,0), (1,0)\}$ sont les seuls sous groupes propres de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

Proposition 4.1.8. *Soient H et K deux sous groupes d'un groupe G. Alors, le sous-ensemble $H \cap K$ est un sous groupe de G. Mais, en général, le sous ensemble $H \cup K$ de G n'est pas un sous groupe de G.*

Démonstration. Exercice. □

Soient $(G, \star)$ un groupe et g un élément de G. Considérons le sous-ensemble $< g >$ de G défini par :

$$< g > := \left\{ g^k : \ k \in \mathbb{Z} \right\}$$

où g^k:=$g \star g \star \cdots \star g$, k fois si $k \geq 1$, $\quad g^0$:=e, l'identité de G et on a g^k:=$(g^{-1})^{-k}$ si k est strictement négatif.

Proposition 4.1.9. *Le sous ensemble $< g >$ est un sous groupe de G. Plus précisément, si $H < G$ contenant l'élément g, alors $< g >$ est un sous groupe de H. On dit dans ce cas que $< g >$ est `le sous groupe cyclique engendré par` g.*

Démonstration. Vérifions les critères de sous-groupes mentionnées dans la Proposition 2.12 :

i). Soient x et y deux éléments de $< g >$. Par définition, ils existent n et m deux entiers tels que $x = g^n$ et $y = g^m$. Ainsi, $xy = g^{n+m}$. D'où $xy \in < g >$.

ii). Par définition, $g^0 = e$. Donc, l'élément neutre est dans $< g >$.

iii). Soit $x \in < g >$. Par définition il existe un entier i tel que $g^i = x$. De plus, $x \star g^{-i} = g^0 = e$. Donc, g^{-i} est l'inverse de x. Par définition, $g^{-i} \in < g >$.

□

Exemples 4.1.10. 1. Soit n un entier naturel non nul. Le sous groupe $n\mathbb{Z}$ est un sous groupe cyclique de $\mathbb{Z}$ engendré par n;

2. Le sous ensemble $\{0, 5, 10, 15\}$ est un sous groupe cyclique de $(\mathbb{Z}/20\mathbb{Z}, +)$ engendré par 5.

Définition 4.1.11. On dit qu'un groupe G est `cyclique` s'il est engendré par un de ces éléments.

Proposition 4.1.12. *Soit n un entier non nul. Les groupes $(Z, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont cycliques.*

Démonstration. Ces groupes sont engendrés respectivement par 1 et $\dot{1}$. □

Définition 4.1.13. Soient G un groupe et g un élément de G. Le nombre d'éléments de G qu'on notera par $|G|$ est appelé `ordre` du groupe G. On appellera l'ordre du groupe $< g >$, `l'ordre de l'élément` g qu'on notera par $|g|$. Ainsi, si le groupe G est fini, l'ordre de G n'est autre que le cardinal de G. Sinon, l'ordre de G est infini.

Exercice 12 (Travaux dirigés). 1. Pour chacune des opérations binaires sur $\mathbb{Z}$ suivantes laquelle est associative ? laquelle est commutative ? laquelle admet un identité ?

i). $(x, y) \mapsto x - y$;

ii). $(x, y) \mapsto x^y$;

iii). $x \star y := xy - x - y + 2$.

2. Considérons le rectangle R défini par $\left\{(x, y) \in \mathbb{R}^2 : |x| \leq n; |y| \leq m\right\}$ où n et m sont des entiers naturels non nuls distincts. Montrer que les quatre symétries de R suivantes forment un groupe avec la loi de composition des applications :

a). L'identité e : $(x, y) \mapsto (x, y)$;

b). La réflexion r_1 : $(x, y) \mapsto (x, -y)$;

c). La réflexion r_2 : $(x, y) \mapsto (-x, y)$;

d). La rotation d'angle π et de centre $(0, 0)$ r_3 : $(x, y) \mapsto (-x, -y)$.

Ecrire le table de Cayley de ce groupe. Le groupe est-il abélien ?

3. Pour chacune des structures suivantes, déterminer si c'est un groupe ou pas :

i). $(\mathbb{Z}, -)$ où l'opération binaire $-$ désigne la soustraction usuelle sur les nombres ;

ii). $(\mathbb{R}, \star)$ où l'opération binaire $\star$ est définie par : $x \star y := x + y - 1$;

iii). $\left(\mathbb{Z}/n\mathbb{Z} \setminus \left\{\dot{0}\right\}, \times\right)$ où n est un nombre entier naturel non nul ;

iv). $(\{z \in \mathbb{C} : |z| = 1\}, \times)$ où $\times$ désigne la multiplication de nombres complexes.

4. Compléter les tables de Cayley des groupes suivants :

$\star$	e	a	b
e		a	
a			
b			

;

$\star$	a	b	c	d
a			d	
b	a			
c			b	
d				

5. Montrer que les sous-ensembles suivants ne sont pas de sous-groupes de $(\mathbb{Z}, +)$: L'ensemble des nombres entiers impairs ; L'ensemble des entiers positifs ; L'ensemble $\{-2, -1, 0, 1, 2\}$; L'ensemble vide.
6. Déterminer les ordres des groupes suivants : $(\mathbb{Z}/n\mathbb{Z}, +)$; $(\mathbb{Z}, +)$; S_n; $\mathrm{GL}_2(\mathbb{R})$.
7. Déterminer les ordres des éléments suivants :
   i). $2 \in (\mathbb{Z}/10\mathbb{Z}, +)$;
   ii). $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$;
   iii). L'identité dans un groupe ;
   iv). $\pi \in (\mathbb{R}, +)$;
8. Démontrer la Proposition 2.12.
9. Démontrer la Proposition 2.14.
10. Soient $(G, \star)$ un groupe fini d'identité e et $g \in G$. Montrer qu'ils existent deux entiers naturels non nuls distincts i et j tels que $a^i = a^j$. En déduire qu'il existe un entier naturel non nul n tel que $a^n = e$.
11. Soit $(G, \star)$ un groupe d'ordre pair. Montrer qu'il existe un élément a de G tel que $a^2 = e$.
12. Déterminer tout les sous-groupes des groupes suivants : $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathbb{Z}/12\mathbb{Z}, +)$.
13. Montrer que les sous-groupes de $(Z, +)$ sont de la forme $n\mathbb{Z}$ où n est un entier naturel.
14. Soient G un groupe fini et g un élément de G. Montrer que $|g|$ divise $|G|$.

4.2 Homomorphismes de Groupes

Définition 4.2.1. Un tableau carré à n lignes remplies par n éléments distincts dont chaque ligne et chaque colonne ne contient qu'un seul de ces éléments est appelé `carré latin`.

Exemples 4.2.2.
1. Un sudoku est un carré latin ;
2. Le table de Cayley du groupe $(\mathbb{Z}/6\mathbb{Z}, +)$ est un carré latin ;
3. Le table de Cayley du monoïde $(\mathbb{Z}/6\mathbb{Z}, \times)$ n'est pas un carré latin.

Proposition 4.2.3. *Le table de Cayley d'un groupe fini est un carré latin.*

Démonstration. A faire en classe. □

Maintenant examinons les tables de Cayley des groupes : $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\{1, -1\}, \times)$. Le table de Cayley de $(\mathbb{Z}/2\mathbb{Z}, +)$ est :

+	0	1
0	0	1
1	1	0

tandis que celui de $(\{1,-1\},\times)$ est le suivant :

$\times$	1	-1
1	1	-1
-1	-1	1

.

A première vue, ces groupes sont différents. Les ensembles ne sont pas les mêmes, ni les structures. Mais les tables de Cayley correspondants sont similaires à celui du groupe $(\{a,b\},\star)$ dont le table de Cayley est le suivant :

$\star$	a	b
a	a	b
b	b	a

.

Dans ce cas, on dit que les groupes $(\mathbb{Z}/2\mathbb{Z},+)$ et $(\{1,-1\},\times)$ sont `isomorphes`. Ainsi, l'idée est de comparer deux structures. Mais, pour cela, l'existence d'une application entre les deux ensembles qui définissent les groupes ne suffira pas. Il nous faut aussi un minimum de "compatibilité" entre les deux structures.
La généralisation de manière formelle de ces idées est l'objet de cette section.

4.2.1 Introduction et Définitions

Définition 4.2.4. Soient $(G_1,\star_1)$ et $(G_2,\star_2)$ deux groupes. Une application f de G_1 dans G_2 qui est compatible aux structures de deux groupes est appelée `homomorphisme de groupes`. Plus précisément, l'application f de G_1 dans G_2 est un homomorphisme si pour tout x et y éléments de G_1, on a :

$$f(x\star_1 y)=f(x)\star_2 f(y).$$

Si de plus, l'application f est bijective, on dit que f est `un isomorphisme` et on note par $G_1\simeq G_2$.

Exemples 4.2.5.
1. Soit $(G,\star)$ un groupe. L'identité Id_G est un isomorphisme ;
2. L'injection canonique $(\mathbb{Z},+)\hookrightarrow(\mathbb{R},+)$ est un homomorphisme ;
3. L'application $(\mathbb{Z}/2\mathbb{Z},+)\ni x\mapsto(-1)^x\in(\{1,-1\},\times)$ est un isomorphisme ;
4. La surjection canonique $(\mathbb{Z},+)\to(\mathbb{Z}/n\mathbb{Z},+)$ est un homomorphisme ;
5. L'application $(\mathrm{GL}_n(\mathbb{R}),\times)\ni A\mapsto\det(A)\in(\mathbb{R}\setminus\{0\},\times)$ est un homomorphisme ;
6. Une application linéaire entre deux espaces vectoriels est un homomorphisme ;
7. L'application exponentielle induit un isomorphisme de $(\mathbb{R},+)$ dans $(\mathbb{R}_+\setminus\{0\},\times)$.

Proposition 4.2.6. *Soient $(G_1,\star_1)$ et $(G_2,\star_2)$ deux groupes. Si f est un homomorphisme de G_1 dans G_2, alors :*

i). $f(e_1)=e_2$, où e_1 et e_2 sont respectivement les identités de G_1 et G_2;

ii). Si $\overline{x}$ est l'inverse d'un élément x de G_1, alors $f(\overline{x})$ est l'inverse de $f(x)$ dans G_2.

Démonstration. i). Par définition, on a $f(e_1)=f(e_1\star_1 e_1)=f(e_1)\star_2 f(e_1)$. L'élément $f(e_1)$ de G_2 est inversible. Donc, en multipliant cet inverse à gauche, on a : $e_2=f(e_1)$;

ii). On a $e_1=x\star_1\overline{x}$. Donc, $e_2=f(e_1)=f(x\star_1\overline{x})=f(x)\star_2 f(\overline{x})$. D'où le résultat.

□

Proposition 4.2.7. *Soient $(G_1, \star_1), (G_2, \star_2)$ et $(G_3, \star_3)$ des groupes. Soient $f : G_1 \to G_2$ et $g : G_2 \to G_3$ deux homomorphismes. Alors :*

i). $g \circ f : G_1 \to G_3$ est un homomorphisme ;

ii). Si de plus f est bijective, l'inverse de f est aussi un isomorphisme.

Démonstration. A faire en classe. □

Corollaire 4.2.8. *La relation d'isomorphisme entre groupes est une relation d'équivalence.*

Démonstration. A faire en classe. □

Définition 4.2.9. Soit $f : (G_1, \star_1) \to (G_2, \star_2)$ un homomorphisme de groupes. Le sous ensemble $\mathrm{Im}(f)$ de G_2 défini par :

$$\mathrm{Im}(f) := \{f(x) : \ x \in G_1\}$$

est appelé `l'image de` f tandis que le sous ensemble $\mathrm{Ker}(f)$ de G_1 défini par :

$$\mathrm{Ker}(f) := \{x \in G_1 : \ f(x) = e_2\}$$

est appelé `le noyau de` f où e_2 est l'identité de G_2.

Proposition 4.2.10. *Soient $f : (G_1, \star_1) \to (G_2, \star_2)$ un homomorphisme de groupes, H_1 un sous groupe de G_1 et H_2 un sous groupe de G_2. Alors :*

i). $\mathrm{Im}(f)$ est un sous groupe de G_2;

ii). $\mathrm{Ker}(f)$ est un sous groupe de G_1;

iii). L'image réciproque $f^{-1}(H_2)$ est un sous groupe de G_1;

iv). Mais, l'image directe $f(H_1)$ n'est pas un sous groupe en général ;

v). Si de plus f est injective, on a $\mathrm{Ker}(f) = \{e_1\}$ où e_1 est l'identité de G_1. L'application f définit ainsi un isomorphisme de G_1 dans $\mathrm{Im}(f)$.

Démonstration. Exercice. □

4.2.2 Groupes Quotients

Soient $(G, \star)$ un groupe et H un sous groupe de G. Pour tout élément x de G, on définit les ensembles $x \star H$ et $H \star x$ comme suit :

$$x \star H := \{x \star h : \ h \in H\}\,; \quad H \star x := \{h \star x : \ h \in H\}\,.$$

S'il n'y a pas de confusions, on écrit gH et Hg.
La relation binaire $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) définit pour tout a et b par :

$$a\mathcal{R}_g b \ (\text{resp. } a\mathcal{R}_d b) \Leftrightarrow aH = bH \ (\text{resp. } Ha = Hb)$$

est une relation d'équivalence sur G. Autrement dit,

$$a\mathcal{R}_g b \ (\text{resp. } a\mathcal{R}_d b) \Leftrightarrow b^{-1}a \in H \ (\text{resp. } ab^{-1} \in H).$$

Ainsi, on a :

Lemme 4.2.11. *Soient $(G, \star)$ et H un sous groupe de G. Alors :*

i). Pour tout x et y dans G, on a : Soit $xH = yH$ (resp. $Hx = Hy$), soit $xH \cap yH = \emptyset$ (resp. $Hx \cap Hy = \emptyset$);

ii). Pour tout $x \in G$, l'application $H \ni h \mapsto xh \in xH$ (resp. $H \ni h \mapsto hx \in Hx$) est bijective.

Démonstration. i). Il suffit de montrer que les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont des relations d'équivalences ;

ii). Considérons la relation $\mathcal{R}_g$. On applique le même raisonnement pour la relation $\mathcal{R}_d$.
Injectivité : Soient h_1 et h_2 deux éléments de H tels que $xh_1 = xh_2$. Comme G est un groupe, l'élément x est inversible. En multipliant cet égalité à gauche par x^{-1}, on a $h_1 = h_2$. Donc, l'application est injective ;
Surjective : Soit $y \in xH$. Par définition, il existe $h \in H$ tel que $y = xh$. Donc, l'application est surjective.

□

Théorème 4.2.12 (Théorème de Lagrange)**.** *Soient G un groupe fini et H un sous groupe de G. On a :*

$$|G| = [G : H]\,|H|$$

où $[G : H] := |G/\mathcal{R}_g| = |G/\mathcal{R}_d|$. L'entier $[G : H]$ est appelé `l'indice` de H dans G. En particulier, $|H|$ divise $|G|$.

Démonstration. Comme G est un ensemble fini, donc les ensembles $G/\mathcal{R}_g$ et $G/\mathcal{R}_d$ sont finis. Or, les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont des relations d'équivalences. Donc, les ensembles $G/\mathcal{R}_g$ et $G/\mathcal{R}_d$ forment respectivement une partition de l'ensemble G. De plus, d'après le lemme précédent, pour tout x et y dans G, on a :

$$|H| = |xH| = |yH| \text{ (resp. } |H| = |Hx| = |Hy|).$$

D'où : $|G| = [G : H]\,|H|$ où $[G : H] := |G/\mathcal{R}_g| = |G/\mathcal{R}_d|$. □

L'exemple suivant est fondamental :
Considérons le groupe S_3 et l'application bijective f élément de S_3 définie par : $\sigma(1) = 2, \sigma(2) = 1$ et $\sigma(3) = 3$. Le sous ensemble $H = \{\mathrm{Id}_{\{1,2,3\}}, \sigma\}$ est un sous groupe de S_3. Considérons l'élément $\tau \in S_3$ défini par : $\tau(1) = 3, \tau(2) = 2$ et $\tau(3) = 1$. Ainsi, on peut vérifier qu'on a : $\tau H \neq H\tau$. Supposons de plus qu'il existerait un homomorphisme de groupes $f : S_3 \to G$ telle que $H = \mathrm{Ker}(f)$. Par définition, on a $f(\sigma) = e_G$, l'identité de G. De plus, on a :

$$\begin{aligned} f(\tau\sigma\tau^{-1}) &= f(\tau)f(\sigma)f(\tau^{-1}) \\ &= f(\tau)e_G(f(\tau))^{-1} \\ &= f(\tau)(f(\tau))^{-1} = e_G \end{aligned}$$

, i.e, $\tau\sigma\tau^{-1} \in H$. Autrement dit, on a $\tau H\tau^{-1} = H$. Ce qui contredit le fait que $\tau H \neq H\tau$. D'où : H ne peut pas être le noyau d'un homomorphisme de S_3 vers n'importe quel groupe. En effet,

Proposition 4.2.13. *Soit $f : G_1 \to G_2$ un homomorphisme de groupes. Pour tout $x \in G_1$, on a :*

$$x\mathrm{Ker}(f) = \mathrm{Ker}(f)x.$$

Autrement dit, pour tout $x \in G$ et $h \in \mathrm{Ker}(f)$, on a : $xhx^{-1} \in \mathrm{Ker}(f)$ ou bien pour tout $x \in G$, on a $x\mathrm{Ker}(f)x^{-1} = \mathrm{Ker}(f)$.

De manière générale ;

Proposition 4.2.14. *Soient G un groupe et H un sous groupe de G. Les deux propositions suivantes sont équivalentes :*

i). $G/\mathcal{R}_g = G/\mathcal{R}_d$;

ii). Pour tout $x \in G$, on a $xH = Hx$ (ou bien $xHx^{-1} = H$).

Si l'une de deux propositions est vérifiée, les deux ensembles quotients induits par les deux relations d'équivalences coïncident et on le notera par G/H.

Démonstration. Supposons qu'on a $G/\mathcal{R}_g = G/\mathcal{R}_d$. Soit $x \in G$. Par hypothèse, il existe $y \in G$ tel que $xH = Hy$. Comme H est un sous groupe, l'identité e de G est dans H. Donc, $x = xe \in Hy$, i.e, il existe $h \in H$ tel que $x = hy$. En multipliant ce dernier égalité à droite par y^{-1}, on a $xy^{-1} = h \in H$. Par définition de la relation $\mathcal{R}_d$, cela veut dire que : $Hx = Hy$. D'où, $xH = Hx$ ou bien $xHx^{-1} = H$. La réciproque est relativement facile. □

Ainsi, on définit :

Définition 4.2.15. Soit G un groupe. Un sous groupe H de G est appelé `un sous groupe normal` de G si l'une des propositions précédentes est vérifiée.

Théorème 4.2.16. *Soient G un groupe et H un sous groupe normal de G. Alors, l'opération binaire sur G induit une relation binaire $\star$ sur l'ensemble quotient G/H définie pour tout x et y dans G par :*

$$(xH) \star (yH) := xyH.$$

De plus, $(G/H, \star)$ définit une structure de groupe. En particulier, la surjection $G \to G/H$ est un homomorphisme surjective de groupes dont le noyau est H.

Démonstration. A faire en classe. Noter bien que l'élément neutre de G/H est H, la classe de l'élément neutre. □

Remarque 4.2.17. Il est important de noter que tout sous groupe d'un groupe abélien est normal.

Théorème 4.2.18 (Premier théorème d'isomorphisme)**.** *Soit $f : (G_1, \star_1) \to (G_2, \star_2)$ un homomorphisme de groupes. On a :*

$$G_1/\mathrm{Ker}(f) \simeq \mathrm{Im}(f).$$

Démonstration. On montre que l'application f définie par :

$$\begin{aligned} f : & G_1/\mathrm{Ker}(f) \to \mathrm{Im}(f) \\ & x\mathrm{Ker}(f) \mapsto f(x) \end{aligned}$$

définit un isomorphisme de groupes. □

Exemples 4.2.19. 1. Par l'homomorphisme surjective $\mathrm{GL}_n(\mathbb{R}) \ni A \mapsto \det(A) \in \mathbb{R} \setminus \{0\}$, on en déduit $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R} \setminus \{0\}$;

2. Considérons l'homomorphisme de groupes $f : (\mathbb{R}, +) \ni \theta \mapsto e^{2i\pi\theta} \in (\mathbb{C} \setminus \{0\}, \times)$. On montre qu'on a : $\mathrm{Im}(f) = S^1 := \{z \in \mathbb{C} : \ |z| = 1\}$ et $\mathrm{Ker}(f) = \mathbb{Z}$. Ainsi, on a :

$$(\mathbb{R}/\mathbb{Z}, +) \simeq (S^1, \times)$$

où S^1 est le cercle de rayon 1 dans $\mathbb{R}^2$.

Théorème 4.2.20 (Troisième théorème d'isomorphisme)**.** *Soient $(G, \star)$ un groupe, H et N deux sous groupes normaux de G tels que $H \subset N$. Alors, H est un sous groupe normal de N. De plus, le groupe N/H est un sous groupe normal de G/H et on a :*

$$(G/H)/(N/H) \simeq G/N.$$

Démonstration. On montre que l'application f définie par :

$$\begin{aligned} f : & G/H \to G/N \\ & xH \mapsto xN \end{aligned}$$

est un homomorphisme surjective de groupes. N'oubliez pas de démontrer que l'application est bien définie d'abord.
Ainsi, on a : $\mathrm{Im}(f) = G/N$ et $\mathrm{Ker}(f) = \{xH : \ xN = N\} = \{xH : \ x \in N\} = N/H$. D'après le premier théorème d'isomorphisme, on a le résultat.

□

Exemples 4.2.21. Soit n un entier naturel non nul. Considérons le groupe $G = (\mathbb{Z}, +)$. Soit d un diviseur positif de n. Ainsi, $n\mathbb{Z}$ et $d\mathbb{Z}$ sont de sous groupes normaux de G tels que $n\mathbb{Z} \subset d\mathbb{Z}$. D'où, d'après le troisième théorème d'isomorphisme, on en déduit :

$$(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}.$$

Le théorème suivant classifie les groupes cycliques à isomorphismes près :

Théorème 4.2.22. *Soit G un groupe cyclique. On a $G \simeq \mathbb{Z}$ ou $G \simeq \mathbb{Z}/n\mathbb{Z}$ où n est un entier naturel.*

Démonstration. Soit g un élément de G tel que $G =< g >$. Considérons l'homomorphisme de groupe f définie par :

$$\begin{aligned} f : & \mathbb{Z} \to G \\ & k \mapsto g^k. \end{aligned}$$

L'homomorphisme f est par définition surjective. Donc, d'après le premier théorème d'isomorphisme, on a $\mathbb{Z}/\mathrm{Ker}f \simeq G$. Or, on sait que les sous groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où n est entier naturel. D'où le résultat. □

Exercice 13 (Travaux dirigés). 1. Pour chacune des applications suivantes, déterminer si c'est un homomorphisme de groupes ou pas :

i). $(\mathbb{R} \setminus \{0\}, \times) \ni a \mapsto \log|a| \in (\mathbb{R}, +)$;

ii). $(\mathbb{C}, +) \ni x \mapsto |x| \in (\mathbb{R}, +)$;

iii). $(\mathbb{Z}, +) \ni t \mapsto 5t \in (\mathbb{Z}, +)$;

iv). $(\mathbb{R}^2, +) \ni (x, y) \mapsto xy \in (\mathbb{R}, +)$;

v). $(\mathbb{R}^2, +) \ni (u, v) \mapsto u - v \in (\mathbb{R}, +)$.

2. Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. Montrer que $G_1 \times G_2 \simeq G_2 \times G_1$.
3. Considérons les groupes $G_1 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ et $G_2 = (\mathbb{Z}/4\mathbb{Z}, +)$. Montrer que

$$G_1 \ncong G_2.$$

4. Démontrer la Proposition 2.29.
5. Considérons l'homomorphisme de groupes $f : (\mathbb{Z}/12\mathbb{Z}, +) \ni n \mapsto i^n \in (\mathbb{C}^\star, \times)$ où i est un élément de $\mathbb{C}$ tel que $i^2 = -1$. Déterminez $\mathrm{Im}(f)$ et $\mathrm{Ker}(f)$ ainsi que $(\mathbb{Z}/12\mathbb{Z})/\mathrm{Ker}(f)$. Puis écrire les tables de Cayley des groupes $(\mathbb{Z}/12\mathbb{Z})/\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$. Vérifier qu'ils sont bien similaires.
6. Pour chacune des homomorphismes suivantes, déterminer son image et son noyau. Puis écrire le résultat qu'on obtient du premier théorème d'isomorphisme :

i). $(\mathbb{Z}, +) \ni m \mapsto 2m \in (\mathbb{Z}, +)$;

ii). $(\mathbb{R}, +) \ni x \mapsto e^{ix} \in (\mathbb{C}^\star, \times)$;

iii). $\det : (\mathrm{GL}_2(\mathbb{R}) \to (\mathbb{C}^\star, \times))$;

iv). $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$;

7. Soit G un groupe abélien fini tel que pour tout élément x de G, on a $x = e$ ou $x^2 = e$ où e est l'identité de G. Montrer que $|G| = 2^n$ où n est un entier naturel.
8. Soient G un groupe et H un sous groupe d'indice 2 de G. Montrer que H est un sous groupe normal de G.

4.3 Exemples de Groupes

4.3.1 Le groupe de permutations S_n

Dans toute la suite, considérons le groupe de permutations S_n comme étant le groupe des applications bijectives de l'ensemble $\{1, 2, 3, \ldots, n\}$ dans lui même. Il est clair que l'ordre du groupe S_n est $n!$. Et bien évidemment, la loi binaire sur S_n est la loi de composition d'applications. S'il n'y a pas de confusion, on notera les deux compositions possibles de deux éléments σ et τ de S_n par $\sigma\tau$ et $\tau\sigma$.

Dans la littérature, ils existent deux notations pour les éléments de S_n : La notation en matrices et la notation en cycles.

La notation en matrices : Soit $\sigma \in S_n$ défini pour tout $i \in \{1, 2, 3, \ldots, n\}$ par $\sigma(i) = a_i \in \{1, 2, 3, \ldots, n\}$. Ainsi, l'élément σ sera noté par : $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$.

La notation en cycles : Un élément σ de S_n est appelé un k-`cycle` s'il existe k éléments $a_1, a_2, \ldots, a_k$ de $\{1, 2, 3, \ldots, n\}$ tels que :

— $\sigma(i) = i$ si $i \notin \{a_1, a_2, \ldots, a_k\}$;

— $\sigma(a_i) = a_{i+1}$ si $1 \leq i \leq k - 1$;

— $\sigma(a_k) = a_1$.

Dans ce cas, on notera σ par :

$$(a_1\ a_2 \cdots a_k).$$

Deux cycles $(a_1\ a_2 \cdots a_k)$ et $(b_1\ b_2 \cdots b_l)$ sont dits `disjoints` si $\{a_1, a_2, \cdots, a_k\} \cap \{b_1, b_2, \cdots, a_l\} = \emptyset$.

Proposition 4.3.1. *Soient σ et τ deux cycles disjoints. On a : $\sigma\tau = \tau\sigma$.*

Démonstration. A faire en classe. □

Définition 4.3.2. Un 2-cycle est appelé `une transposition`.

Proposition 4.3.3. *Soit $\sigma = (a_1\ a_2 \cdots a_k)$ un cycle de S_n où $k \geq 2$. Alors, σ peut être une composition des transpositions. Plus précisément, on a :*

$$(a_1\ a_2 \cdots a_k) = (a_1\ a_2)(a_2\ a_3) \cdots (a_{k-1}\ a_k).$$

Démonstration. On montre qu'on a : $(a_1\ a_2 \cdots a_k) = (a_1\ a_2)(a_2\ a_3 \ldots a_k)$. Puis, on raisonne par récurrence. □

Remarque 4.3.4. Noter bien que la décomposition d'un cycle en produit de transpositions n'est pas unique. Par exemple, dans S_3, on a :

$$(1\ 2)(2\ 3)(3\ 1) = (2\ 3).$$

Proposition 4.3.5. *Toute permutation de S_n est un produit (ou une composition) de cycles deux à deux disjoints. Par conséquent, elle est aussi un produit de transpositions.*

Démonstration. A faire en classe. □

Remarque 4.3.6. Bien qu'une permutation soit un produit de transpositions, noter bien que ces transpositions qui la décomposent ne sont pas deux à deux disjoints. Sinon, toute permutation serait d'ordre 1 ou 2 qui n'est pas vrai si $n \geq 3$.

Mais, en général, ce qui est sur est le suivant :

Théorème 4.3.7. *Le nombre de transpositions qui décomposent une permutation donnée : soit il est pair, soit il est impair.*

Définition 4.3.8. Une permutation de S_n est dite `pair` si elle est décomposée par un nombre pair de transpositions. Dans le cas contraire, on dit qu'elle est `impaire`.

On peut déterminer facilement la parité d'une permutation comme l'indique la remarque suivante :

Remarque 4.3.9. D'après la Proposition 2.3.3, un k-cycle est une composition de $k-1$ transposition. Donc, si une permutation donnée est une composition de t cycles de longueur $k_1, k_2, \ldots, k_t$ respectivement, sa parité est la même que celle du nombre $k_1 + k_2 + \cdots + k_t + t$.

L'application

$$\begin{aligned}\epsilon :& S_n \to (\{1,-1\},\times)\\ &\sigma \mapsto \begin{cases}1 & \text{si } \sigma \text{ est paire;}\\ -1 & \text{sinon}\end{cases}\end{aligned}$$

est un homomorphisme surjective de groupes. Ainsi, d'après le premier théorème d'isomorphisme, on a $S_n/\mathrm{Ker}\epsilon = \{1,-1\}$. Par conséquent, l'ensemble de permutations paires forment un sous groupe normal d'indice 2 dans S_n. On notera cet sous-groupe par A_n et sera appelé `le groupe alterné de degré` n. De plus, d'après la Proposition 2.3.3., un k-cycle est dans A_n si et seulement si k est impair.
On termine cet exemple avec un théorème important qui justifie l'importance de S_n dans la théorie des groupes :

Théorème 4.3.10 (Théorème de Cayley)**.** *Soit $(G,\star)$ un groupe fini d'ordre n. Alors, G est isomorphe à un sous-groupe de S_n.*

Démonstration. Soit $g \in G$. Considérons l'application $f_g : G \in x \mapsto g \star x \in G$. Pour tout $g \in G$, l'application f_g est clairement bijective. Autrement dit, f_g est un élément de $P(G)$, le groupe des applications bijectives de G dans G. Maintenant considérons le sous-ensemble H de $P(E)$ défini par :

$$H := \left\{\sigma \in P(E) :\ \exists g \in G \text{ tel que } \sigma = f_g\right\}.$$

Le sous-ensemble H est un sous groupe de $P(E)$. En effet :

- Si on désigne par e l'identité de G, l'application f_e est clairement l'identité de $P(E)$. Donc, $\mathrm{Id}_G \in H$;
- Soient f_{g_1} et f_{g_2} deux éléments de H. Pour tout $x \in G$, on a :

  $$(f_{g_1} \circ f_{g_2})(x) = f_{g_1}(f_{g_2}(x)) = f_{g_1}(g_2 \star x) = (g_1 \star g_2) \star x = f_{g_1 g_2}(x).$$

  Donc, la composition des applications est stable dans H.
- Soit $g \in G$. On a $f_g^{-1} = f_{g^{-1}}$. Ce qui veut dire que $f_g^{-1} \in H$.

Finalement, considérons l'application $f : G \ni g \mapsto f_g \in H$. Clairement, cette application est bijective. De plus, on a : $f(g_1 \star g_2) = f_{g_1 g_2} = f_{g_1} \circ f_{g_2}$. Donc, f est un isomorphisme de groupes. Autrement dit, $G \simeq H$. Or, H est un sous-groupe de $P(E)$ qui est isomorphe à S_n. D'où le résultat. □

4.3.2 Le groupe diédral D_n

Dans cette sous-section, dans le plan euclidien, on désignera par R_n un polygone régulier de n côtés. Notons son centre par C. On sait qu'ils existent exactement $2n$ symétries qui laissent le polygone R_n invariant, à savoir :

- Les n rotations de centre C respectivement d'angle $\frac{2k\pi}{n}$ où $k = 1, 2, 3, \ldots, n$;
- Les n réflexions axiales déterminées respectivement par les n axes de symétries de R_n.

Proposition 4.3.11. *Les $2n$ symétries de R_n définies ci-dessus forment un groupe d'ordre $2n$ avec la loi de composition de transformations sur le plan euclidien. On notera cet groupe par D_n et sera appelé* `le groupe diédral` *d'ordre $2n$. De plus, si r et τ sont respectivement la rotation d'angle $\frac{2\pi}{n}$ et une symétrie axiale, on a :*

$$D_n = \left\{ r^k : \ k = 1, 2, \ldots, n \right\} \cup \left\{ r^k \tau : \ k = 1, 2, \ldots, n \right\}$$

et $(r^k\tau) \circ (r^l\tau) = r^{k-l}$.

Démonstration. A faire en classe. □

Remarque 4.3.12. Le théorème de Cayley nous garantit que D_n est isomorphe à un sous-groupe de S_{2n}. Par contre, naturellement, un élément de D_n permute les n sommets du polygone R_n. Ainsi, tout élément de D_n peut être considérer comme une permutation de l'ensemble de n sommets de R_n. Ainsi, D_n est un sous-groupe de S_n.

4.3.3 Le groupe linéaire $\mathrm{GL}_n(\mathbb{R})$

Rappelons que $\mathrm{GL}_n(\mathbb{R})$ désigne le groupe des matrices inversibles d'ordre n à coefficients dans $\mathbb{R}$. Le groupe est un groupe non abélien infini. L'application

$$\begin{aligned} \det : \mathrm{GL}_n(\mathbb{R}) &\to \mathbb{R}^\star \\ A &\mapsto \det A \end{aligned}$$

est un homomorphisme surjective. Son noyau est l'ensemble des matrices inversibles noté par $\mathrm{SL}_n(\mathbb{R})$ dont le déterminant est 1. En utilisant cet homomorphisme, on montre qu'on a

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^\star.$$

Ainsi, comprendre le groupe $\mathrm{GL}_n(\mathbb{R})$ revient à comprendre son sous-groupe normal $\mathrm{SL}_n(\mathbb{R})$.

Proposition 4.3.13. *Le groupe de permutations S_n est isomorphe à un sous-groupe de* $\mathrm{SL}_n(\mathbb{R})$.

Démonstration. On montre que S_n est isomorphe au groupe de matrices de permutations P_n. Puisque pour tout $P \in P_n$, $\det P = 1$, le groupe de matrices de permutations est un sous-groupe de $\mathrm{SL}_n(\mathbb{R})$. □

Notons par $\mathrm{GL}_n(\mathbb{Z})$ l'ensemble des matrices inversibles d'ordre n à coefficient dans $\mathbb{Z}$. Alors :

Proposition 4.3.14. $\mathrm{GL}_n(\mathbb{Z})$ *est un groupe des matrices dont le déterminant est* ± 1. *Le noyau de la restriction de l'homomorphisme* det *sera noté par* $\mathrm{SL}_n(\mathbb{Z})$.

Démonstration. On montre que le sous-ensemble $\mathrm{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{Gl}_n(\mathbb{R})$. Le plus dur est de montrer que si une matrice carrée à coefficients dans $\mathbb{Z}$ est inversible, son inverse est aussi à coefficients dans $\mathbb{Z}$. Mais, c'est faisable.
Soit $A \in \mathrm{GL}_n(Z)$. Donc, par définition, la matrice inverse A^{-1} est à coefficients dans $\mathbb{Z}$. Ainsi, $\det A$ et $\det A^{-1}$ sont des entiers. Or, $AA^{-1} = I_n$. Donc, $\det A^{-1} = \frac{1}{\det A}$. Comme $\det A$ et $\det A^{-1}$ sont des entiers, ceci n'est possible que si $\det A = \pm 1$. □

Soit E un espace vectoriel sur $\mathbb{R}$. Rappelons qu'une application f de E vers un $\mathbb{R}$- espace vectoriel F est `une application linéaire` si pour tout (x, y) dans E^2 et (λ, μ) dans $\mathbb{R}^2$, on a :

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y).$$

En particulier, f est un homomorphisme de groupes puisque $(E, +)$ et $(F, +)$ sont des groupes abéliens.
Dans le cas où $F = E$, on dit que f est `un endomorphisme`. Si de plus, E est de dimension n, en utilisant l'identification des éléments de E via l'isomorphisme $E \simeq R^n$, il existe une matrice A d'ordre n telle que pour tout $x \in E$, on a :

$$f(x) = Ax.$$

Si $(b_1, b_2, \ldots, b_n)$ désigne une base de E, la matrice de f est complètement déterminé de manière unique dans cette base, et l'on a :

$$A = (f(b_1)\ f(b_2)\ \cdots\ f(b_n))$$

où $f(b_i)$ est le vecteur de la i-ième colonne de A. Désignons respectivement par $\mathrm{Ker}f$ et $\mathrm{Im}f$ le noyau et l'image de l'endomorphisme f. On a les propriétés suivants :

— $\mathrm{Ker}f$ et $\mathrm{Im}f$ sont des sous-espaces vectoriels de E;

— $\mathrm{Ker}f = N(A)$ et $\mathrm{Im}f = C(A)$.

Ainsi, si on désigne par $\mathcal{L}(E)$ l'ensemble des endomorphismes de E, on a l'isomorphisme suivante :

$$(\mathcal{L}(E), +) \simeq (M_n(\mathbb{R}), +).$$

De plus, si on note par $\mathrm{GL}(E)$ l'ensemble des endomorphismes bijectives de E, on a :

$$(\mathrm{GL}(E), \circ) \simeq (\mathrm{GL}_n(\mathbb{R}), \times).$$

Maintenant considérons le cas où l'on a $n = 2$. Désignons par $\mathrm{O}_2(\mathbb{R})$ le sous-ensemble de $\mathrm{GL}_2(\mathbb{R})$ défini par :

$$\mathrm{O}_2(\mathbb{R}) := \left\{ A \in \mathrm{GL}_n(\mathbb{R}) :\ A^T A = A A^T = I_2 \right\}.$$

C'est l'ensemble des matrices orthogonaux d'ordre 2. On a :

Proposition 4.3.15. $\mathrm{O}_2(\mathbb{R})$ *est un sous-groupe de* $\mathrm{GL}_2(\mathbb{R})$. *De plus, pour tout* $A \in \mathrm{O}_2(\mathbb{R})$, *on a*

$$\det A = \pm 1$$

et soit A *est une matrice de rotation, soit elle est une matrice de réflexion. Plus précisément,*

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \quad \textit{ou } A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

pour un certain angle θ. *Le groupe des rotations sera noté par* $\mathrm{SO}_2(\mathbb{R})$.

Démonstration. A faire en classe. □

Corollaire 4.3.16. *Le groupe diédral* D_n *est isomorphe à un sous-groupe de* $\mathrm{O}_2(\mathbb{R})$.

Démonstration. A faire en classe. la Proposition 2.3.15. permet d'expliciter le groupe diédral D_n sous forme matricielle. □

Pour finir, énonçons le résultat important suivant :

Théorème 4.3.17. *Le groupe* $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par :*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Exercice 14 (Travaux dirigés).

1. Pour chacune des permutations suivantes, écrire-la comme composée des cycles :
   i). $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;
   ii). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix}$;
   iii). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 3 & 2 & 5 \end{pmatrix}$.
2. Pour chacune des permutations suivantes, écrire-la en matrice-notation :
   i). $(1\,2\,3)(4\,6\,8)$;
   ii). $(1\,6)(4\,2)(5\,3)$;
   iii). $(1\,5\,3)$;
   iv). $(1\,9\,3)(2\,6)(7\,8)$;
   v). $)(2\,4)(3\,5\,7)$.
3. Pour chacune des cas suivants, calculer $\sigma\tau$ et $\tau\sigma$:
   i). Dans S_4, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \tau = (1\,2)(3\,4)$;
   ii). Dans S_5, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$;
   iii). Dans S_6, $\sigma = (1\,2)(5\,6), \tau = (1\,3\,4\,6\,2)$.
   Ecrire les résultats en utilisant les deux notations.
4. Pour chacune des permutations suivantes, déterminer si elle est paire ou impaire :
   i). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$;
   ii). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$;
   iii). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$;
   iv). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 6 & 9 & 8 & 5 & 4 & 7 \end{pmatrix}$.

5. i). Respectivement dans S_3 et S_4, combien de transpositions a t-on ? Quand est-il des 3-cycles ? des 4-cycles (dans S_4) ?
   ii). Soit H l'ensemble des éléments qui ne sont pas des transpositions, ni des 3-cycles, ni des 4-cycles dans S_4. Le sous-ensemble H est-il un sous groupe ? Si oui, déterminer son ordre et trouver un groupe usuel (qu'on connait très bien) qui est isomorphe à H.
6. Dans chacun des groupes suivants, déterminer le nombre d'éléments d'ordre 2 et le nombre d'éléments d'ordre 3 : S_3, A_4, D_5 et D_6.
7. Pour tout $k \in \{1,2,3,4,5,6\}$, déterminer le nombre d'éléments d'ordre k dans A_5.
8. Pour chacun des cas suivants, déterminer si le sous-ensemble est un sous-groupe de S_4 ou pas. Dans le cas où le sous-ensemble est un groupe, déterminer si c'est un groupe normal :
   i). $\{\mathrm{id}, (1\,3\,4), (1\,4\,3)\}$;
   ii). $\{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$;
   iii). $\{\mathrm{id}, , (1\,2\,3\,4), (1\,4\,3\,2), (1\,3)(2\,4)\}$;
   iv). $\{\mathrm{id}, , (1\,2\,3), (1\,3\,2), (2\,3\,4), (2\,4\,3)\}$.
9. Considérons l'application $f : (\mathbb{Z} \times \mathbb{Z}) \ni (m,n) \mapsto \sigma^n \tau^m \in S_4$ où $\sigma = (1\ 2)(3\ 4)$ et $\tau = (1\ 3)(2\ 4)$. Montrer que f est un homomorphisme de groupes. Expliciter le résultat du premier théorème d'isomorphisme.
10. Notons respectivement par ρ et τ une rotation et une réflexion dans le groupe diédral D_n. Montrer que $\tau^{-1} = \rho\tau\rho$.
11. Considérons un homomorphisme $f : S_n \to \mathbb{Z}/3\mathbb{Z}$ où $n \geq 3$. Montrer que f est trivial,i.e, pour tout $\sigma \in S_3$, on a $f(\sigma) = 0$.
12. i). Montrer que $S_3 \simeq D_3$.
    ii). Expliciter tout les éléments de D_3 en forme de matrices, en utilisant le fait qu'il est isomorphe à un sous groupe de $\mathrm{O}_2(\mathbb{R})$.
13. i). Soit $(G, \star)$ un groupe d'ordre un nombre premier p. Montrer que $G \simeq \mathbb{Z}/p\mathbb{Z}$, i.e, à isomorphisme près, il n'existe qu'un seul groupe d'ordre p où p un nombre premier.
    ii). Pour tout $n \in \{1,2,3,4,5,6,7\}$, trouver les classes d'isomorphismes des groupes d'ordre n.

5 Introduction à la théorie des Anneaux

5.1 Introduction et Définitions

Dans le chapitre précédent, on a considéré des ensembles avec une structure définissant des groupes. Mais, on remarque que dans la plus part de ces ensembles, il y a deux structures différentes. Comme l'on a dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R})$ et $\mathbb{R}[x]$, l'ensemble des polynômes à une variable. Ils ont en commun les faits suivants :

— L'addition (+) définit une structure de groupe abélien ;
— La multiplication $(\times)$ définit un monoïde ;
— Distributivité : Pour tout a, b et c, on a : $(a+b) \times c = a \times c + b \times c$ et $c \times (a+b) = c \times a + c \times b$.

La formalisation de cette nouvelle structure est le but de ce chapitre. Par abus de notation, s'il n'y a pas de confusion, la loi binaire qui définit une structure de groupe abélien sur un ensemble quelconque sera notée par $+$. Tandis que, si la loi binaire définisse un monoïde, elle sera notée par $\times$. L'élément neutre par rapport à l'addition sera noté par 0 et l'identité par rapport à la multiplication sera noté par 1.

Définition 5.1.1. Soit $(A, +, \times)$ une structure algébrique telle que $(A, +)$ est un groupe abélien et $(A, \times)$ est un monoïde. On dit que $(A, +, \times)$ est `un anneau` si on a la distributivité de deux loi binaires. Si $(A, \times)$ est un monoïde commutatif, on dit que $(A, +, \times)$ est `un anneau commutatif`. Un élément de A est dit `inversible` s'il est inversible par rapport à la loi multiplication. L'ensemble des éléments inversibles d'un anneau A est noté par $A^\times$. Si de plus, on a $A^\times = A \setminus \{0\}$, on dit que $(A, +, \times)$ est `un corps`.

Exemples 5.1.2.
1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R})$ et $\mathbb{R}[x]$ sont des anneaux ;
2. $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ et $\mathbb{R}[x]$ sont des anneaux commutatifs ;
3. $\mathbb{Z}$ et $M_n(\mathbb{R})$ ne sont pas des corps ;
4. $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps ;
5. $M_n(\mathbb{R})$ n'est pas un anneau commutatif ;
6. $\mathbb{Z}[i] := \{a + ib \in \mathbb{C} : \ a, b \in \mathbb{Z}\}$ où $i = \sqrt{-1}$ est un anneau commutatif. On a

$$(\mathbb{Z}[i])^\times = \{-1, 1, i, -i\}.$$

Proposition 5.1.3. *Soient A_1 et A_2 deux anneaux. Alors, le produit scalaire $A = A_1 \times A_2$ définit une structure d'anneau avec les opérations induites naturellement de celles de A_1 et A_2.*

Démonstration. A faire en classe. □

5.2 Idéaux et Anneaux quotients

Considérons l'anneau des entiers $(Z, +, \times)$. On sait que les sous groupes de $(Z, +)$ sont de la forme $n\mathbb{Z}$ où n est un entier naturel. Comme $(Z, +)$ est un groupe abélien, l'ensemble quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien. De plus, la multiplication dans $\mathbb{Z}$ induit une structure monoïde sur $\mathbb{Z}/n\mathbb{Z}$ d'identité $\dot{1}$. De plus, pour tout $\dot{a}, \dot{b}$ et $\dot{c}$ dans $\mathbb{Z}/n\mathbb{Z}$, on a :

$$\dot{c}(\dot{a} + \dot{b}) = \dot{c}\dot{a} + \dot{c}\dot{b} = (\dot{a} + \dot{b})\dot{c}.$$

Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau et l'on a :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\dot{a} : \ \text{pgcd}(a, n) = 1\}.$$

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.
La généralisation de cet exemple est l'objet de cette section.