Algèbre 1

Cours et Travaux Dirigés

Marc Pauly

Cours d'algèbre 1

Marc Pauly

Sommaire du cours d'Algèbre 1

Chapitre 1. Logique et ensembles

Chapitre 2. Groupes. Anneaux. Corps.

Chapitre 3. Espaces vectoriels

1. Définition d'espace vectoriel
2. Propriétés élémentaires
3. Sous-espaces vectoriels
   3.1. Somme de sous-espaces vectoriels. Décomposition en somme directe
4. Applications linéaires
5. Noyau et image d'une application linéaire
6. Projecteurs
7. Familles libres/génératrices. Bases
8. Dimension d'un espace vectoriel
9. Vocabulaire du chapitre
10. Exercices

Annexes

1. Preuve du théorème 3.13.
2. Preuve du théorème 3.14.
3. Le lemme de Zorn

Chapitre 1. Logique et ensembles

1 Introduction à la logique

1.1 Négation, disjonction et le principe du tiers exclu

Les mathématiques sont une science fondée sur le raisonnement.

Le raisonnement utilise des phrases mathématiques qui peuvent être vraies ou fausses.

Si P est une phrase mathématique, on peut toujours former **la négation** de P. On la note (non P).

Si P est vraie, sa négation est fausse. Si P est fausse, sa négation est vraie.

Donc la négation de la négation de P (on dit aussi **la double négation de** P) a toujours la même valeur de vérité que P. On écrit cela

$$P = \text{non non } P$$

Par exemple, si on dit : «La relation $1+1 \neq 2$ est fausse», on dit la double négation d'une phrase beaucoup plus simple : «La relation $1+1=2$ est vraie». Mathématiquement, on dit deux fois la même chose.

Lorsqu'on a deux phrases P, Q, on peut former **leur disjonction**. On la note (P ou Q). Si au moins une des phrases P, Q est vraie, alors (P ou Q) est vraie. Si P, Q sont toutes les deux fausses, alors (P ou Q) est fausse.

Autrement dit, la phrase (P ou Q) est vraie exactement si P est vraie ou Q est vraie. On voit qu'on définit la disjonction à l'aide du mot «ou» de la langue française. Il est donc très important d'avoir bien compris l'idée que ce mot traduit.

Nous avons déjà vu qu'une phrase mathématique peut être vraie ou fausse. Mais est-ce qu'elle peut être ni vraie ni fausse (une troisième possibilité) ? Pour faire des mathématiques, cela ne serait pas très pratique. On impose donc **le principe du tiers exclu** qui élimine toute autre possibilité que le «vrai» et le «faux».

> **Principe du tiers exclu.** *Toute phrase mathématique P est vraie ou fausse.*

Une autre manière d'énoncer le principe du tiers exclu utilise la disjonction et la négation.

> **Principe du tiers exclu.** *Quelle que soit la phrase mathématique P, la phrase (P ou non P) est vraie.*

1.2 Conjonction, implication et équivalence

De la même manière que nous avons formé la disjonction de deux phrases P, Q on peut aussi former **leur conjonction**. On la note (P et Q).

Si P, Q sont toutes deux vraies, alors (P et Q) est vraie. Si au moins une des deux phrases P, Q est fausse, alors (P et Q) est fausse.

La conjonction (P et Q) est donc vraie exactement si P est vraie et Q est vraie. Il est également très important d'avoir compris le sens du mot français «et».

Tout le monde sait que

$$\begin{aligned} \text{non } (P \text{ ou } Q) &= (\text{non } P) \text{ et } (\text{non } Q) \\ \text{non } (P \text{ et } Q) &= (\text{non } P) \text{ ou } (\text{non } Q) \end{aligned}$$

Remarque : Le français exprime «(non P) et (non Q)» par la formule symétrique «ni P ni Q», alors que l'anglais la traduit de manière non symétrique : «*neither P nor Q*».

On peut utiliser ces régles pour les appliquer à la négation du principe du tiers exclu. Comme la phrase (P ou (non P)) est toujours vraie, sa négation est toujours fausse. Mais sa négation est ((non P) et (non non P)), c'est-à-dire ((non P) et P).

Le principe du tiers exclu a une conséquence intéressante : **la phrase (non P) et P) est toujours fausse.** Cela veut dire qu'il est impossible que les deux phrases P, (non P) soient vraies en même temps. C'est une bonne nouvelle pour les mathématiques, car **on élimine ainsi la possibilité d'une contradiction**. Une contradiction est une phrase P qui est à la fois vraie et fausse.

C'est cette absence de contradictions qu'on utilise dans **les démonstrations par l'absurde** :
Si on montre qu'une phrase P implique Q, et que P implique aussi (non Q), alors P ne peut pas être vraie. En effet, si P était vraie, alors Q et (non Q) seraient toutes les deux vraies, ce qui est impossible, comme on vient de le voir. Donc P n'est pas vraie, ce qui signifie grâce au principe du tiers exclu que P est fausse et que (non P) est vraie.

On en déduit ceci : si on doit montrer qu'une phrase P est vraie, on peut essayer de montrer que sa négation (non P) mène à une contradiction. Le raisonnement du paragraphe précédent montre alors que (non non P) est vraie, ce qui achève le travail.

L'implication $\Longrightarrow$

Maintenant, nous allons nous intéresser à la phrase (si P, alors Q), phrase qu'on appelle **une implication**. On la note ($P \Rightarrow Q$). Nous allons voir qu'on peut l'exprimer à l'aide des opérateurs logiques que nous avons vus ci-dessus.

Quelle est la négation de (si P, alors Q) ? En d'autres termes, quand peut-on dire que la phrase (si P, alors Q) est fausse ? Nous posons ici la question de la négation de la causalité. La causalité est la mise en relation entre phrases, la cause P et l'effet Q. Chaque fois qu'on a la cause, on a aussi l'effet. Pour faire la négation de la causalité, il faut donc qu'il y ait la cause, mais qu'il n'y ait pas l'effet.

Exemple. «Si c'est mercredi, alors il fait nuageux à Pékin». C'est une causalité. La cause «c'est mercredi» appelle l'effet «il fait nuageux à Pékin». Si on veut prouver que la phrase est fausse, on peut le faire si on trouve un mercredi où il ne fait pas nuageux à Pékin. On a la cause, mais on n'a pas l'effet.

Bref, on voit que

$$\text{non (si } P, \text{ alors } Q) = P \text{ et (non } Q)$$

En passant à la négation, et en remplaçant (si P, alors Q) par la notation $P \Rightarrow Q$, on obtient

$$(P \Rightarrow Q) = (\text{(non } P) \text{ ou } Q)$$

L'implication peut donc être exprimée à l'aide de la disjonction et de la négation.

L'équivalence $\Longleftrightarrow$

Enfin, il nous reste à parler de **l'équivalence** (P si et seulement si Q), que l'on note ($P \iff Q$).
Par définition, la phrase (P si et seulement si Q) est vraie exactement dans les deux cas suivants :
1. P et Q sont vraies ; 2. P et Q sont fausses.
Une autre façon de dire les choses : la phrase (P si et seulement si Q) est vraie lorsque P et Q ont la même valeur de vérité. On remplacera dorénavant le signe = utilisé ci-dessus par le symbole $\iff$. Ce symbole traduit l'égalité en logique, il est très important.

Théorème 1.1. *La phrase ($P \iff Q$) a le même sens que la phrase ($(P \Rightarrow Q)$ et $(Q \Rightarrow P)$). En notation symbolique :*

$$(P \iff Q) \iff ((P \Rightarrow Q) \text{ et } (Q \Rightarrow P))$$

Preuve. La phrase P est vraie ou fausse. La phrase Q est vraie ou fausse. Cela fait donc $2 \times 2 = 4$ possibilités.

1. P est vraie et Q est vraie :

Dans ce cas, la phrase ($P \Leftrightarrow Q$) est vraie. De même, les deux phrases $P \Rightarrow Q$ et $Q \Rightarrow P$ sont également vraies, donc leur conjonction aussi. Les deux phrases de l'énoncé sont vraies.

2. P est fausse et Q est vraie :
Maintenant, la phrase $(P \Leftrightarrow Q)$ est fausse. La phrase $(Q \Rightarrow P)$ est également fausse, donc la conjonction de l'énoncé est forcément fausse. Les deux phrases de l'énoncé sont fausses.
3. P est vraie et Q est fausse :
C'est la situation symétrique de la situation précédente. On trouvera donc que les deux phrases de l'énoncé sont fausses.
4. P est fausse et Q est fausse.
La phrase $(P \Leftrightarrow Q)$ est vraie. On voit aussi que $(P \Rightarrow Q)$,$(Q \Rightarrow P)$ sont toutes deux vraies (il suffit de le vérifier avec la formule "$(P \Rightarrow Q) \iff$ ((non P) ou Q)"). Les deux phrases de l'énoncé sont vraies. □

Ce théorème explique pourquoi on écrit $(P \Leftrightarrow Q)$ aussi sous la forme (P si et seulement si Q).
En effet, (P si Q), c'est (si Q, alors P). D'un autre côté, (P seulement si Q) c'est (si P, alors Q). En réunissant les deux, on voit que

$$((P \text{ si } Q) \text{ et } (P \text{ seulement si } Q))$$

exprime la même chose que

$$((Q \Rightarrow P) \text{ et } (P \Rightarrow Q)).$$

1.3 Tables de vérité

Nous avons rencontré 5 opérateurs logiques : négation, disjonction, conjonction, implication, équivalence.

Le premier opérateur, la négation, est **unaire** (on prend la négation d'**une** phrase). Les quatre autres opérateurs sont **binaires** (il faut deux phrases pour les écrire).

Pour chacun de ces opérateurs, nous allons dresser la table de vérité, qui envisage toutes les possibilités de «vrai» et «faux».

Dans les tables ci-dessous, nous notons 1 à la place de «vrai» et 0 à la place de «faux».

P	non P
1	0
0	1

P	Q	P ou Q
1	1	1
1	0	1
0	1	1
0	0	0

P	Q	P et Q
1	1	1
1	0	0
0	1	0
0	0	0

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

P	Q	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

1.4 Règles de commutativité, d'associativité, de distributivité

Les deux relations ci-dessous sont claires :

$$\begin{aligned} P \text{ ou } Q &\iff Q \text{ ou } P \\ P \text{ et } Q &\iff Q \text{ et } P \end{aligned}$$

Elles traduisent la symétrie des tables de vérité pour les opérateurs de disjonction et de conjonction. On parle aussi de **la commutativité** de ces opérateurs. Elle exprime que l'ordre des phrases n'a pas d'importance.

On remarquera que l'implication n'est pas commutative. On ne peut pas échanger la cause et l'effet.

On a aussi les relations évidentes :

$$\begin{aligned} P \text{ ou } (Q \text{ ou } R) &\iff (P \text{ ou } Q) \text{ ou } R \\ P \text{ et } (Q \text{ et } R) &\iff (P \text{ et } Q) \text{ et } R \end{aligned}$$

Ce sont les propriétés **d'associativité** des opérateurs de disjonction et de conjonction. Elles expriment le fait que les parenthèses ne sont pas nécessaires. On pourra donc écrire, sans qu'il y ait ambiguïté, la phrase (P ou Q ou R), respectivement la phrase (P et Q et R).

Il faut faire attention lorsqu'on mélange la disjonction et la conjonction. On peut se convaincre facilement des relations

$$\begin{aligned} P \text{ ou } (Q \text{ et } R) &\iff (P \text{ ou } Q) \text{ et } (P \text{ ou } R) \\ P \text{ et } (Q \text{ ou } R) &\iff (P \text{ et } Q) \text{ ou } (P \text{ et } R) \end{aligned}$$

Ce sont les relations de **distributivité** de la conjonction par rapport à la disjonction.

1.5 Réciproque et contraposée

Nous avons déjà vu que les phrases $(P \Rightarrow Q)$, $(Q \Rightarrow P)$ n'ont pas le même sens. On dit que la phrase $(Q \Rightarrow P)$ est **la réciproque** de $(P \Rightarrow Q)$.

Si on connaît la valeur de vérité de $(P \Rightarrow Q)$, on ne peut pas en déduire la valeur de vérité de sa réciproque $(Q \Rightarrow P)$.

> **Exemple.** La réciproque de «Si x est un réel positif, alors $2x$ est un réel positif» est vraie. Mais la réciproque de «Si x est un réel positif, alors $x+1$ est un réel positif» est fausse.

Lorsqu'on veut démontrer qu'une équivalence $(P \iff Q)$ est vraie, on peut démontrer séparément les phrases $(P \Rightarrow Q)$ et sa réciproque $(Q \Rightarrow P)$. Cela se justifie par la formule

$$(P \iff Q) \iff ((P \Rightarrow Q) \text{ et } (Q \Rightarrow P))$$

Il ne faut pas confondre la réciproque de $(P \Rightarrow Q)$ avec **la contraposée de** $(P \Rightarrow Q)$.

> **Définition.** *La* **contraposée de** $(P \Rightarrow Q)$ *est la phrase* $((\text{non } Q) \Rightarrow (\text{non } P))$.

> **Théorème 1.2 (théorème de la contraposée).**
> *La phrase* $(P \Rightarrow Q)$ *est équivalente à sa contraposée.*

> **Preuve.**
>
> $$\begin{aligned} (P \Rightarrow Q) &\iff ((\text{non } P) \text{ ou } Q) \\ &\iff ((\text{non } (\text{non } Q)) \text{ ou } (\text{non } P)) \\ &\iff ((\text{non } Q) \Rightarrow (\text{non } P)) \end{aligned}$$
>
> □

Grâce au théorème de la contraposée, on peut démontrer la phrase «Si P est vraie, alors Q est vraie» en démontrant plutôt «Si Q est fausse, alors P est fausse». C'est parfois intéressant.

2 Quantificateurs et théorèmes

2.1 Les deux quantificateurs

Les vérités mathématiques sont de deux types :
Il y a celles qui affirment que dans un ensemble, **il existe un élément** qui possède une certaine propriété.
Et il y a celles qui affirment que dans un ensemble, **tous les éléments** possèdent une certaine propriété.

Les phrases du premier type se notent avec **le quantificateur existentiel** $(\exists)$, les phrases du second type avec **le quantificateur universel** $(\forall)$**.**

> Voici un exemple pour le quantificateur existentiel.
>
> $$\exists x \in \mathbb{C}, x^2 + 1 = 0$$
>
> Et un autre utilisant le quantificateur universel.
>
> $$\forall x \in \mathbb{C}, x\bar{x} = |x|^2$$

Il est intéressant de noter que le quantificateur existentiel remplace en quelque sorte le symbole «ou», et que le quantificateur universel remplace le symbole «et». Par exemple, la phrase

$$\exists k \in \{1, 2, \ldots, n\}, k^2 - k - 12 = 0$$

dit la même chose que

$$(1^2 - 1 - 12 = 0) \text{ ou } (2^2 - 2 - 12 = 0) \text{ ou } \cdots \text{ ou } (n^2 - n - 12 = 0).$$

On laissera le lecteur assidu écrire

$$\forall n \in \{4, 6, 8, \cdots, 10^{888}\}, n \text{ est la somme de deux nombres premiers}$$

à l'aide de l'opérateur «et».

2.2 Négation des quantificateurs

Etudions à présent les négations des phrases commençant par un quantificateur. Nous savons que

$$\text{non } (\forall x \in E, P(x)) \Leftrightarrow \exists x \in E, (\text{non } P(x))$$

et

$$\text{non } (\exists x \in E, P(x)) \Leftrightarrow \forall x \in E, (\text{non } P(x))$$

Dès lors, on peut combiner ces règles pour trouver la négation de phrases plus compliquées. Ainsi, par exemple, la négation de la phrase

$$\forall a \in \mathbb{R}^*, \forall b \in \mathbb{R}, \forall c \in \mathbb{R}, \exists x \in \mathbb{C}, (ax^2 + bx + c = 0)$$

(phrase qui affirme que toute équation polynomiale de degré 2 admet une solution complexe) est

$$\exists a \in \mathbb{R}^*, \exists b \in \mathbb{R}, \exists c \in \mathbb{R}, \forall x \in \mathbb{C}, (ax^2 + bx + c \neq 0)$$

2.3 Théorèmes et démonstrations

Un théorème est simplement une phrase vraie. Quand on dit que P est un théorème, cela signifie que la phrase P est vraie.

Comment savoir si une phrase est vraie ? Par une démonstration. Pour montrer qu'une phrase est vraie, il faut prouver qu'elle découle de phrases plus simples dont on sait déjà qu'elle sont vraies. Ces phrases plus simples sont des théorèmes établis auparavant, ou des axiomes (des choses qu'on admet comme étant vraies).

> Un exemple typique : On doit montrer : $\forall x \in E, P(x)$. Cela veut dire : La phrase «Si $x \in E$, alors $P(x)$» est vraie. On peut le démontrer par exemple comme suit. Si nous savons déjà que les trois phrases «Si $x \in E$, alors $R(x)$», «Si $R(x)$, alors $Q(x)$», «Si $Q(x)$, alors $P(x)$» sont toutes vraies, alors l'enchaînement de ces phrases permet de dire que la phrase du début est également vraie. Elle devient alors théorème, et nous pourrons l'utiliser par la suite pour démontrer d'autres théorèmes.

2.4 Conjectures et contre-exemples

Il existe des phrases dont on se sait pas si elles sont vraies ou fausses, parce qu'on ne connaît pas de démonstration. Ce sont **les conjectures**.

> **Exemple.** La conjecture de Goldbach : Tout nombre pair $\geqslant 4$ est la somme de deux nombres premiers. Aujourd'hui, personne ne sait si cette phrase est vraie ou fausse. Il s'agit d'une conjecture.

Une conjecture P peut avoir deux destins radicalement différents. Soit quelqu'une trouve une démonstration, et alors la conjecture devient théorème. Soit quelqu'un trouve une démonstration de (non P), et alors la conjecture est fausse. C'est ce qui est arrivé par exemple à une vieille conjecture de Fermat, qui pensait que

$$\forall n \in \mathbb{N}, 2^{2^n} + 1 \text{ est premier}$$

Il est vrai que pour $n = 0, 1, 2, 3, 4$, on trouve des nombres premiers. Mais $2^{2^5} + 1 = 2^{32} + 1$ n'est pas premier, car il est divisible par 641 (découverte due au mathématicien Euler). Cette phrase de Fermat n'est plus une conjecture, elle est devenue une phrase fausse depuis Euler.

Pour montrer qu'une phrase A du type «$\forall x \in E, P(x)$» est fausse, il suffit de trouver un élément $x \in E$ tel que $P(x)$ soit faux. On dit alors que x est **un contre-exemple pour la phrase** A. L'existence d'un contre-exemple implique que A est fausse.

Ainsi, $n = 5$ est un contre-exemple pour la phrase «$\forall n \in \mathbb{N}, 2^{2^n} + 1$ est premier».

3 Ensembles et éléments

3.1 Complémentaire, union, intersection

Rappelons brièvement quelques constructions élémentaires qu'on fait avec les ensembles.

Si E et F sont deux ensembles, on appelle **complémentaire de F dans E** l'ensemble des éléments de E qui n'appartiennent pas à F. On le note $E - F$ (ou $E \setminus F$).

$$E - F = \{x \in E | x \notin F\}$$

On peut aussi définir **l'union (ou la réunion) de E et F**. C'est l'ensemble des éléments qui appartiennent à au moins un des ensembles E, F. On le note $E \cup F$ (on lit : «E union F»).

$$E \cup F = \{x | x \in E \text{ ou } x \in F\}$$

Reste **l'intersection de E et F**. C'est l'ensemble des éléments qui appartiennent aux deux ensembles E, F. On le note $E \cap F$ (on lit : «E inter F»).

$$E \cap F = \{x | x \in E \text{ et } x \in F\}$$

Rappelons quelques-unes des règles les plus couramment utilisées.

$$\begin{aligned}
E - (E - F) &= E \cap F \\
E \cup F &= F \cup E \\
E \cap F &= F \cap E \\
E \cup (F \cup G) &= (E \cup F) \cup G \\
E \cap (F \cap G) &= (E \cap F) \cap G \\
E \cup (F \cap G) &= (E \cup F) \cap (E \cup G) \\
E \cap (F \cup G) &= (E \cap F) \cup (E \cap G) \\
E - (F \cup G) &= (E - F) \cap (E - G) \\
E - (F \cap G) &= (E - F) \cup (E - G)
\end{aligned}$$

On utilise parfois **la différence symétrique** de deux ensembles E, F. C'est l'ensemble des éléments qui appartiennent à exactement un des ensembles E, F. On le note $E \Delta F$.

$$E \Delta F = \{x | x \in E \text{ et } x \notin F\} \cup \{x | x \in F \text{ et } x \notin E\} = (E - F) \cup (F - E)$$

On remarque que

$$\begin{aligned}
E \Delta F &= (E \cup F) - (E \cap F) \\
E \Delta F &= F \Delta E
\end{aligned}$$

La seconde égalité justifie le nom «différence symétrique» donné à l'opérateur Δ.

3.2 Sous-ensembles d'un ensemble

Si E est un ensemble, on dit que F est **un sous-ensemble de** E si tous les éléments de F appartiennent à E. On note alors $F \subset E$.

$$F \subset E \Leftrightarrow (\forall x \in F, x \in E) \Leftrightarrow (\forall x, x \in F \Rightarrow x \in E)$$

On dit aussi que F est **une partie** de E.

Remarquons que si $F \subset E$, alors $E - (E - F) = F$.

Rappelons aussi **la règle de transitivité** : Si $E \subset F$ et $F \subset G$, alors $E \subset G$.

L'ensemble des parties d'un ensemble E est noté $\mathcal{P}(E)$ (observer que $\mathcal{P}$ est la première lettre de «partie»).

Exemple.

$$P(\{\clubsuit, \spadesuit\}) = \{\, \varnothing, \{\clubsuit\}, \{\spadesuit\}, \{\clubsuit, \spadesuit\}, \,\}$$

3.3 Produit cartésien d'ensembles

Soient E et F deux ensembles. On appelle **produit cartésien de** E **et** F (et on note $E \times F$) l'ensemble de tous les couples (x, y), où $x \in E, y \in F$:

$$E \times F = \{(x, y) | x \in E \text{ et } y \in F\}$$

On peut définir de manière plus générale le produit cartésien $E_1 \times E_2 \times \cdots \times E_n$ (où $n \geqslant 2$) comme étant l'ensemble de tous les n-uplets $(x_1, x_2, \cdots, x_n)$, où pour tout $i \in \{1, \ldots, n\}$, $x_i \in E_i$.

On pose aussi

$$E^n = \underbrace{E \times E \times \cdots \times E}_{n}$$

Exemple. $\mathbb{R}^3$ est l'ensemble de tous les triplets (x, y, z) de réels. On peut le voir comme l'ensemble des points de l'espace.

3.4 Familles indexées par un ensemble

Soient E et I des ensembles. **Une famille à valeurs dans** E **indexée par** I est une collection $(x_i)_{i \in I}$ d'éléments de E «numérotés» par les éléments de l'ensemble I. On appelle les éléments de l'ensemble I **les indices** (parce que traditionnellement, on les écrit en indice, c'est-à-dire en bas à droite).

Exemple. Une famille à valeurs dans $\mathbb{R}$ et indexée par l'ensemble $I = \{A, 1, +\}$ est une collection de trois réels (x_A, x_1, x_+). Bien sûr, on indexe beaucoup plus souvent par l'ensemble $\{1, 2, 3\}$.

Notation. *On note E^I l'ensemble de toutes les familles à valeurs dans E et indexée par I.*

Il faut remarquer que

$$E^{\{1,2,\ldots,n\}} = \underbrace{E \times E \times \cdots \times E}_{n} = E^n$$

Exemple. L'ensemble $\mathbb{R}^{\mathbb{N}}$ est l'ensemble de toutes les suites $(u_n)_{n \in \mathbb{N}}$ à valeurs dans $\mathbb{R}$.

3.5 Union et intersection : généralisation

Avec la définition précédente de l'union et de l'intersection, on peut former l'union et l'intersection de $2, 3, \ldots, n$ ensembles. Mais comment faire pour définir l'union et l'intersection d'un nombre infini d'ensembles ?

Soit E un ensemble. On veut considérer un nombre quelconque (éventuellement infini) de parties de E et définir leur union et leur intersection.

On peut voir cette collection de sous-ensembles de E comme une famille $(A_i)_{i\in I}$ à valeurs dans $\mathcal{P}(E)$ indexée par un ensemble I. Si I est infini, cela signifie qu'on a une famille infinie de sous-ensembles de E.

On va définir maintenant l'union de la famille $(A_i)_{i\in I}$ (notée $\bigcup_{i\in I} A_i$).
On va aussi définir l'intersection de la famille $(A_i)_{i\in I}$ (notée $\bigcap_{i\in I} A_i$) :

$$\begin{aligned}\bigcup_{i\in I} A_i &:= \{x \in E | \exists i \in I, x \in A_i\}\\ \bigcap_{i\in I} A_i &:= \{x \in E | \forall i \in I, x \in A_i\}\end{aligned}$$

Si I est un ensemble fini, on retrouve bien entendu les définitions précédentes de l'union et de l'intersection.

Exemple. $\bigcup_{n\in\mathbb{N}^*}]-\frac{1}{n}, 1-\frac{1}{n}[=]-1, 1[$ et $\bigcap_{n\in\mathbb{N}^*}]-\frac{1}{n}, 1-\frac{1}{n}[= \varnothing$

4 Les opérateurs logiques et les opérateurs des ensembles

Il existe une jolie correspondance entre les opérateurs de la logique et les opérateurs de la théorie des ensembles.

Soit E un ensemble. Pour tout $x \in E$, on considère une phrase $P(x)$ qui peut être vraie ou fausse. On note V_P l'ensemble des éléments x de E pour lesquels $P(x)$ est vraie :

$$V_P := \{x \in E | P(x) \text{ est vraie } \}$$

On peut voir P comme une famille de phrases indexée par E.

Quel est le lien entre V_P et $V_{\text{non } P}$? Ici (non P) est la famille qui associe à tout x la phrase non $(P(x))$.

Il est clair que

$$V_{\text{non } P} = E - V_P$$

La négation logique correspond au complémentaire d'un ensemble.

Regardons maintenant les quatre opérateurs logiques binaires. On commence par la disjonction ou la conjonction.

$$\begin{aligned}V_{P \text{ ou } Q} &= V_P \cup V_Q\\ V_{P \text{ et } Q} &= V_P \cap V_Q\end{aligned}$$

Avec cela, on comprend bien pourquoi la réunion/l'intersection des ensembles et la disjonction/conjonction de la logique obéissent à des règles semblables.

Pour l'implication on obtient

$$V_{P\Rightarrow Q} = V_{(\text{non } P) \text{ ou } Q} = V_{\text{non } P} \cup V_Q = (E - V_P) \cup V_Q$$

Etudions enfin l'équivalence logique

$$\begin{aligned}V_{P\Leftrightarrow Q} &= \{x \in E | (P(x) \Leftrightarrow Q(x)) \text{ est vraie } \}\\ &= (V_P \cap V_Q) \cup (V_{\text{non } P} \cap V_{\text{non } Q})\\ &= (V_P \cap V_Q) \cup ((E - V_P) \cap (E - V_Q))\\ &= (V_P \cap V_Q) \cup (E - (V_P \cup V_Q))\\ &= E - ((E - (V_P \cap V_Q)) \cap (V_P \cup V_Q))\\ &= E - (V_P \Delta V_Q)\end{aligned}$$

L'équivalence logique correspond au complémentaire de la différence symétrique.

On peut remarquer pour conclure que la différence symétrique des ensembles correspond à

$$\text{«}P \textbf{ ou exclusif } Q\text{»},$$

qui est par définition vraie si **exactement une** des phrases P, Q est vraie. On voit alors que la phrase «P équivalent à Q» dit la même chose que «non (P ou exclusif Q)», ce qui est confirmé par la traduction de l'équivalence au niveau des ensembles.

5 Applications

5.1 Généralités

Définition. *Soient E, F des ensembles.* **Une application (ou : une fonction) de E vers F** *est une correspondance qui associe à chaque $x \in E$ un unique élément $y \in F$. On appelle cet élément y* **l'image de x par l'application**. *Si on note l'application par un symbole (par exemple f), on écrit $y = f(x)$ pour dire «L'image de l'élément $x \in E$ par l'application f est l'élément $y \in F$».*

L' ensemble E est appelé **ensemble de départ de f.**
L' ensemble F est appelé **ensemble d'arrivée de f.**

Si $y \in F$, on dit que $x \in E$ est **un antécédent de y par f** *si $f(x) = y$.*

Le graphe de l'application *f est l'ensemble $\{(x, f(x)) | x \in E\}$. C'est un sous-ensemble de $E \times F$.*

Exemple. Considérons la fonction $f : \mathbb{R} \to \mathbb{R}_+ : x \mapsto x^2 + 1$.
Son ensemble de départ est $\mathbb{R}$.
Son ensemble d'arrivée est $\mathbb{R}_+$.
L'image de 3 par f est 10.
Le nombre -3 est un antécédent de 10 par f. Le nombre 3 est aussi un antécédent de 10 par f.
Le nombre 0 n'a pas d'antécédent par f.
L'image de 0 par f est 1.

Une application est la même chose qu'une famille à valeurs dans F indexée par E. Si on note $\mathcal{F}(E, F)$ l'ensemble de toutes les applications de E vers F, on a bien sûr

$$\mathcal{F}(E, F) = F^E$$

Définition. *Soit $f : E \to F$ une application.*
Si A est un sous-ensemble de E, **la restriction de f à A** *est l'application, notée $f|_A$, de A dans F, et définie par*

$$\forall x \in A, f|_A(x) = f(x).$$

Si E est un sous-ensemble de A, **un prolongement de f à A** *est une application de A vers un ensemble contenant F, et dont la restriction à E est l'application f.*

Exemples.
L'application $g : [-\pi/2, \pi/2] \to \mathbb{R} : t \mapsto \sin t$ est la restriction de $f : \mathbb{R} \to \mathbb{R} : t \mapsto \sin t$ à $[-\pi/2, \pi/2]$.
L'application $g : \mathbb{C} \to \mathbb{C} : z \mapsto e^z$ est un prolongement de l'application $f : \mathbb{R} \to \mathbb{R} : x \mapsto e^x$.

Définition. *Soit $f : E \to F$ une application.*

1. Si A est une partie de E, on appelle **image de A par f** *et on note $f(A)$ l'ensemble des images de tous les éléments de A :*

$$f(A) = \{f(x) | x \in A\} = \{y \in F | \exists x \in A, f(x) = y\}$$

L'ensemble $f(A)$ est un sous-ensemble de F. On appelle **image de f** *l'ensemble $f(E)$.*

2. Si B est une partie de F, on appelle **image inverse de B par f** *et on note $f^*(B)$ l'ensemble des antécédents de tous les éléments de B.*

$$f^*(B) = \{x \in E | f(x) \in B\} = \{x \in E | \exists y \in B, f(x) = y\}$$

L'ensemble $f^*(B)$ est un sous-ensemble de E.

5.2 Injections, surjections, bijections. Composée.

Définition. *Soit f une application de E vers F.*
1. On dit que f est **une injection (ou : une application injective)** *si tout élément de F possède au plus un antécédent par f.*
2. On dit que f est **une surjection (ou : une application surjective)** *si tout élément de F possède au moins un antécédent par f.*
3. On dit que f est **une bijection (ou : une application bijective)** *si tout élément de F possède exactement un antécédent par f.*

Une bijection est donc une application qui est injective et surjective.

Pour montrer qu'une application est bijective, on peut prouver séparément qu'elle est injective et qu'elle est surjective.

La condition d'injectivité de f peut encore s'écrire

$$\forall x, x' \in E, (f(x) = f(x') \Rightarrow x = x')$$

Cette condition dit : si un élément $y \in F$ possède deux antécédents x et x', alors x et x' sont égaux. L'élément $y \in F$ possède au plus un antécédent.

La surjectivité peut s'écrire

$$\forall y \in F, \exists x \in E, f(x) = y$$

ou aussi

$$f(E) = F$$

Exemples. 1. La fonction $f(x) : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ n'est pas injective, car $f(-1) = f(1)$. Elle n'est pas non plus surjective, car $-1 \in \mathbb{R}$ n'a pas d'antécédent par f.

2. La fonction $f(x) : \mathbb{R} \to \mathbb{R}_+ : x \mapsto x^2$ n'est pas injective (pourquoi ?), mais elle est surjective : Tout $y \in \mathbb{R}_+$ a au moins un antécédent par f (par exemple $\sqrt{y}$).

3. La fonction $f(x) : \mathbb{R}_+ \to \mathbb{R}_+ : x \mapsto x^2$ est injective et surjective. Elle est donc bijective.

Définition.
Si $f : E \to F$ et $g : F \to G$ sont deux applications, on appelle **composée de g et f,** *et on note $g \circ f$, l'application de E vers G définie par*

$$\forall x \in E, (g \circ f)(x) = g(f(x))$$

Le symbole $g \circ f$ se lit «g rond f».

On peut changer un petit détail dans la définition de la composée de deux applications. Il suffit de demander que l'ensemble d'arrivée de f soit un sous-ensemble de l'ensemble de départ de g. Evidemment, la composée $g \circ f$ ne dépend que de f et de la restriction de g à l'image de f.

Définition. *Si $f : E \to F$ est une bijection, on appelle* **réciproque de f,** *et on note f^{-1}, l'application de F vers E qui envoie $y \in E$ sur son unique antécédent par f.*

Si f est une bijection, on a $\forall x \in E, f^{-1}(f(x)) = x$ et $\forall y \in F, f(f^{-1}(y)) = y$.

Définition. *L'application $E \to E$ qui envoie tout $x \in E$ sur x est appelé* **l'identité sur E.** *On la note* id_E.

On peut donc dire

$$f^{-1} \circ f = \mathrm{id}_E, \qquad f \circ f^{-1} = \mathrm{id}_F$$

Exemple.
La réciproque de la bijection $f : \mathbb{R} \to \mathbb{R}_+^* : x \mapsto e^x$ est la fonction $f^{-1} : \mathbb{R}_+^* \to \mathbb{R} : y \mapsto \ln y$.

Théorème 1.3.
1. La composée de deux injections est une injection.
2. La composée de deux surjections est une surjection.
3. La composée de deux bijections est une bijection.

Preuve. 1. Soient $f : E \to F$ et $g : F \to G$ deux injections. On doit montrer que $g \circ f$ est une injection. Nous allons le faire en montrant que si $(g \circ f)(x) = (g \circ f)(x')$, alors $x = x'$. On suppose que $(g \circ f)(x) = (g \circ f)(x')$. Mais alors $g(f(x)) = g(f(x'))$. Comme g est une injection, on peut dire que $f(x) = f(x')$. Mais f aussi est une injection. D'où $x = x'$ et c'est fini.

2. Soient $f : E \to F$ et $g : F \to G$ deux surjections. On doit montrer que $g \circ f$ est une surjection. Soit $z \in G$. On doit montrer qu'il existe $x \in E$ avec $(g \circ f)(x) = z$. Comme g est une surjection, il existe $y \in F$ avec $g(y) = z$. Et comme f est une surjection, il existe $x \in E$ avec $f(x) = y$. Mais alors $(g \circ f)(x) = g(f(x)) = g(y) = z$ et c'est fini.

3. Si f et g sont deux bijections, alors f et g sont en particulier des injections, et par 1. on peut alors affirmer que $g \circ f$ est une injection. Mais f, g sont aussi des surjections, et par 2. on peut affirmer que $g \circ f$ est aussi une surjection. Donc $g \circ f$ est une bijection. □

Si $f : E \to F$ et $g : F \to G$ sont deux bijections, il est clair que

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

On fera très attention à l'ordre dans lequel on écrit f et g.

Théorème 1.4 (associativité de la composée). *Soient $f : E \to F, g : F \to G, h : G \to H$ trois applications. Alors*

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Preuve. Soit $x \in E$ un élément quelconque. On écrit

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(\ h(x)\ ) = f(\ g(h(x))\ ) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$$

Les deux applications $(f \circ g) \circ h$ et $f \circ (g \circ h)$ sont égales. □

Lorsque $f : E \to F$ est une injection, il suffit de modifier son ensemble d'arrivée pour que f devienne une bijection.

Théorème 1.5. *Si $f : E \to F$ est une injection, alors l'application $\tilde{f} : E \to f(E)$ définie par*

$$\forall x \in E, \tilde{f}(x) = f(x)$$

est une bijection.

Preuve. Si $\tilde{f}(x) = \tilde{f}(x')$, alors $f(x) = f(x')$, et comme f est une injection, on a $x = x'$. Donc $\tilde{f}$ est une injection. Cette fonction $\tilde{f}$ est aussi une surjection, car par définition de $f(E)$, tout $y \in f(E)$ a un antécédent dans E. □

Remarque : $\tilde{f}$ n'est pas une restriction de f. L'ensemble de départ n'a pas changé par rapport à celui de f. C'est l'ensemble d'arrivée qui a changé.

Exemple. On appelle E l'ensemble des étudiants de l'École Centrale de Pékin.
L'application $f : E \to \mathbb{N}$ est par définition celle qui à tout étudiant de E associe son numéro d'étudiant. L'application f est injective, parce que deux étudiants distincts n'ont jamais le même numéro. En revanche, f n'est pas surjective, car il existe des nombres entiers qui ne sont pas des numéros d'étudiants.
Si on remplace f par

$$\tilde{f} : \begin{array}{ccc} E & \to & f(E) \\ x & \mapsto & f(x) = \text{numéro de l'étudiant } x \end{array}$$

on obtient une bijection de l'ensemble des étudiants vers l'ensemble des entiers qui sont des numéros d'étudiants.

6 Ensembles finis

Définition. *On dit qu'un ensemble E est* **un ensemble fini** *s'il existe un entier $n \in \mathbb{N}$ et une bijection $f : E \to [[1, n]] = \{1, \dots, n\}$.*

Par convention, $[[1, 0]]$ est l'ensemble vide.

Si E est un ensemble fini, l'entier n est unique. On appelle cet entier **le cardinal de** E. On le note $\mathrm{Card}(E)$ ou $\mathrm{Card}\, E$ ou $|E|$. L'ensemble vide $\varnothing$ est un ensemble fini de cardinal 0.

Les résultats suivants sont clairs.

1. Si E est un ensemble fini, et $E' \subset E$, alors E' est aussi un ensemble fini, et $|E'| \leqslant |E|$.
2. Si E est un ensemble fini, $E' \subset E$ et $|E'| = |E|$, alors $E' = E$.
3. Si E, F sont finis, et $\varphi : E \to F$ est une injection, alors $|E| \leqslant |F|$.
4. Si E, F sont finis, $\varphi : E \to F$ est une injection et $|E| = |F|$, alors φ est une bijection.
5. Si E, F sont finis, et $\psi : E \to F$ est une surjection, alors $|E| \geqslant |F|$.
6. Si E, F sont finis, $\psi : E \to F$ est une surjection et $|E| = |F|$, alors ψ est une bijection.
7. Si E, F sont finis, et $\Phi : E \to F$ est une bijection, alors $|E| = |F|$.
8. Si E, F sont finis, et $|E| = |F|$, alors il existe une bijection $\Phi : E \to F$.
9. Si E, F sont finis, alors $E \times F$ est fini, et $|E \times F| = |E| \cdot |F|$.
10. Si E, F sont finis, alors $\mathcal{F}(E, F)$ et F^E sont finis, et
$$|\mathcal{F}(E, F)| = \left|F^E\right| = |F|^{|E|}.$$
11. Si E est fini, alors $\mathcal{P}(E)$, l'ensemble de tous les sous-ensembles de E, est fini, et
$$|\mathcal{P}(E)| = 2^{|E|}.$$
12. Si E, F sont deux ensembles finis, et $E \cap F = \varnothing$, alors $E \cup F$ est fini, et
$$|E \cup F| = |E| + |F|.$$

Les propriétés 9 et 12 sur $E \times F$ et $E \cup F$ se généralisent évidemment à des ensembles du type $E_1 \times \cdots \times E_p$ ou $E_1 \cup \cdots \cup E_p$. Dans le deuxième cas, il faut supposer que les ensembles $(E_i)_{1 \leqslant i \leqslant p}$ sont deux à deux disjoints : $\forall i, j \in [[1, p]], (i < j \Rightarrow E_i \cap E_j = \varnothing)$.

7 Vocabulaire du chapitre

La logique
un ensemble
une négation
une disjonction
une conjonction
le principe du tiers exclu
une double négation
une implication
une équivalence
une contradiction
par l'absurde
une causalité
symbolique
unaire
binaire
commutatif
associatif
distributif
la réciproque
la contraposée
un quantificateur
un théorème
existentiel
universel
une démonstration
une preuve
une conjecture
un contre-exemple
un ensemble
un élément
le complémentaire
l'union
la réunion
l'intersection
la différence symétrique
un sous-ensemble
une partie
transitif
un produit cartésien
une famille d'éléments
un opérateur
ou exclusif
une application
une fonction
l'image d'un élément
l'ensemble de départ
l'ensemble d'arrivée
un antécédent
le graphe
une restriction
un prolongement
l'image d'un ensemble
l'image inverse d'un ensemble
une injection
une surjection
une bijection
une composée
la fonction réciproque
l'identité
le cardinal d'un ensemble

8 Exercices

1. Soit E un ensemble. On suppose que $\forall x, y \in E, x = y$. Que peut-on dire de E ?

2. Soit E un ensemble. On suppose que $\forall x, y \in E, x \neq y$. Que peut-on dire de E ?

3. Soient E, F deux ensembles. On suppose que $\forall x \in E, \exists y \in F, x = y$. Que dire des ensembles E et F ?

4. Soient E, F deux ensembles. On suppose que $\exists x \in E, \forall y \in F, x = y$. Que dire des ensembles E et F ?

5. Soient E_1, E_2, E_3 trois ensembles. Trouver une bijection de $(E_1 \times E_2) \times E_3$ vers $E_1 \times (E_2 \times E_3)$.

6. On suppose que $P \Rightarrow Q$ est vraie, et Q est fausse. Que peut-on dire ?

7. Trouver un contre-exemple à la conjecture «Si x, y sont deux réels avec $x \notin \mathbb{Q}$ et $y \notin \mathbb{Q}$, alors $x + y \in \mathbb{Q}$».

8. Combien y a-t-il de sous-ensembles de $\{0, 1, 2, 3\} \times \{4, 5, 6, 7, 8\}$?

9. Trouver une application $f : \mathbb{N} \to \mathbb{N}$ injective, mais pas surjective. Trouver une application $f : \mathbb{N} \to \mathbb{N}$ surjective, mais pas injective.

10. Soit Ω un ensemble, et A, B, C trois sous-ensembles de Ω. Montrer les équivalences

$$A \subset B \cap C \iff (A \subset B) \text{ et } (A \subset C), \qquad A \subset B \cup C \iff A - B \subset C.$$

Chapitre 2. Groupes. Anneaux. Corps

1 Groupes

1.1 Définition d'un groupe

Nous connaissons tous l'opération + sur les nombres entiers. Elle possède en particulier les propriétés suivantes :

– Si a, b sont des entiers, alors $a + b$ est un entier
– Si a, b, c sont des entiers, alors $a + (b + c) = (a + b) + c$
– L'entier 0 a la propriété : $\forall a \in \mathbb{Z}, a + 0 = 0 + a = a$
– Pour tout entier a, il existe un entier b avec $a + b = b + a = 0$

Bien sûr, ces propriétés sont très simples. Nous allons voir qu'elles se retrouvent dans beaucoup de situations, pour d'autres ensembles que $\mathbb{Z}$ et pour d'autres opérations que la somme.

Définition. *Un groupe est un ensemble G et une opération binaire interne $*$ sur G qui vérifie les trois propriétés suivantes :*
1. Associativité : $\forall x, y, z \in G, x * (y * z) = (x * y) * z$
2. Element neutre : $\exists e \in G, \forall x \in G, x * e = e * x = x$
3. Inverse : $\forall x \in G, \exists y \in G, x * y = y * x = e$.

Commentaires.
1. Une opération binaire interne est une opération qui associe à deux éléments x, y de G un élément $x * y$ de G ; elle est dite binaire parce qu'elle a besoin de deux éléments pour exister ; elle est dite interne parce que si x, y sont dans G, $x * y$ est aussi dans G
2. La première propriété, l'associativité, montre que si on fait au moins deux opérations, les parenthèses ne sont pas nécessaires. On pourra écrire, sans qu'il y ait ambiguïté, des expressions comme $x * y * z$ ou $a * b * c * d$.
3. L'élément neutre (qui est toujours unique, comme nous allons le voir) dans notre exemple de $\mathbb{Z}$ avec l'addition est bien sûr le nombre entier 0.
4. Si x est donné, nous allons voir que l'inverse de x est unique. On le note en général x^{-1}, de sorte que $x * x^{-1} = x^{-1} * x = e$. Dans notre exemple de $\mathbb{Z}$, l'inverse du nombre entier a est le nombre entier $-a$.

Notation.
Dorénavant nous allons noter xy au lieu de $x * y$. Il faut garder à l'esprit que xy n'est pas nécessairement une multiplication entre deux nombres, mais une notation pour une situation plus générale. D'ailleurs, pour l'exemple de la somme dans $\mathbb{Z}$, xy désigne la somme de x et y.

1.2 Premières propriétés

Théorème 2.1.
1. Dans un groupe, il y a exactement un élément neutre.
2. Dans un groupe, tout élément a exactement un inverse.
3. Si x, y sont deux éléments d'un groupe, alors $(xy)^{-1} = y^{-1}x^{-1}$
4. L'inverse de e est e.

Preuve. 1. On sait qu'il a au moins un élément neutre e. Si e' est aussi un élément neutre, alors $e' = e'e$ car e est un élément neutre. Mais $e'e = e$ car e' est un élément neutre. Donc $e' = e$, ce qui montre l'unicité de l'élément neutre.
2. Soit x un élement de G. On suppose que x a deux inverses y et y'. Nous allons montrer que $y = y'$. En effet

$$y' = y'e = y'(xy) = (y'x)y = ey = y$$

(Par conséquent, l'écriture x^{-1} n'a pas d'ambiguïté)

3. L'élément $y^{-1}x^{-1}$ est l'inverse de xy. En effet

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$$

et

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = e$$

4. $ee = ee = e$, donc e est son propre inverse □

Commentaires.
1. On pourra dorénavant dire «**le** neutre» d'un groupe. Si $x \in G$, on peut aussi dire «**l'**inverse» de x. Le théorème ci-dessus montre en effet que ces objets sont uniques.
2. Attention à l'ordre dans la formule pour l'inverse d'un produit !

1.3 Exemples

1. $(\mathbb{Z}, +)$ est un groupe. L'élément neutre est 0, et l'inverse de a est le nombre $-a$.

2. De même, $(\mathbb{Q}, +), (\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes.

3. $(\mathbb{N}, +)$ n'est pas un groupe, car il n'existe pas d'élément $n \in \mathbb{N}$ avec $1 + n = 0$.

4. $([-1, 1], +)$ n'est pas un groupe, car $1 + 1 \notin [-1, 1]$.

5. $(\mathbb{R}_+^*, \cdot)$ est un groupe d'élément neutre 1, et l'inverse de x est le nombre $\dfrac{1}{x}$.

6. $(\mathbb{R}^*, \cdot)$ est un groupe.

7. $(\mathbb{R}, \cdot)$ n'est pas un groupe, car il n'existe pas d'élément $x \in \mathbb{R}$ avec $0 \cdot x = 1$.

8. On note U l'ensemble des nombres complexes de module 1. La multiplication des nombres complexes est une opération interne sur U, car si z, z' sont de module 1, alors zz' est aussi de module 1. Ensuite l'associativité est évidente, l'élément neutre est le nombre complexe 1, et tout $z \in U$ possède un inverse dans U, à savoir $\dfrac{1}{z}$. Donc $(U, \cdot)$ est un groupe.

1.4 Groupes commutatifs. Groupes non commutatifs

Dans les exemples ci-dessous, les groupes ont tous la propriété $xy = yx$. Cette propriété ne fait pas partie de la définition d'un groupe, mais elle est souvent vraie.

Définition. *Un groupe* **commutatif** *est un groupe G dans lequel on a $\forall x, y \in G, xy = yx$.*

Un groupe commutatif peut aussi être appelé groupe **abélien**, en hommage au mathématicien *Abel*.
Un groupe qui n'est pas commutatif est appéle groupe **non commutatif** ou **non abélien**.

Exemple : Un groupe non commutatif.
On prend un entier $n \geqslant 3$, et on considère l'ensemble S_n de toutes les **bijections** de $E = \{1, \ldots, n\}$ vers $E = \{1, \ldots, n\}$. L'ensemble S_n est de cardinal $n!$. Si f, g sont deux bijections de E vers E, la composée $f \circ g$ est aussi une bijection de E vers E. Donc l'opération $\circ$ est une opération binaire interne sur S_n. Montrons que $(S_n, \circ)$ est un groupe. L'associativité est évidente, car l'opération $\circ$ est toujours associative. L'élément neutre pour $\circ$ est la bijection identité, qui envoie tout élément $x \in E$ sur x. L'inverse de la bijection f est sa bijection réciproque. On a montré que $(S_n, \circ)$ est un groupe. Mais ce n'est pas un groupe commutatif. En effet, considérons la bijection $f : E \to E$ qui est définie par

$$f(1) = 2, f(2) = 3, f(3) = 1, \qquad f(n) = n \text{ pour } n \geqslant 4$$

Considérons également la bijection $g : E \to E$ définie par

$$g(1) = 2, g(2) = 1, \qquad g(n) = n \text{ pour } n \geqslant 3$$

On voit que $(f \circ g)(1) = f(2) = 3$ et $(g \circ f)(1) = g(2) = 1$. Donc $f \circ g \neq g \circ f$, ce qui montre que $(S_n, \circ)$ n'est pas un groupe commutatif (pour $n \geqslant 3$). Le groupe $(S_n, \circ)$ est appelé **le groupe symétrique sur n éléments**. C'est un groupe non commutatif pour $n \geqslant 3$. Lorsque $n = 1$ ou $n = 2$, c'est un groupe commutatif.

1.5 Sous-groupes et morphismes

Définition.
Soit $(G,\cdot)$ un groupe. Un **sous-groupe de** *G est un sous-ensemble H de G qui possède les propriétés suivantes :*
1. $e \in H$ (e est le neutre du groupe G)
2. $\forall x, y \in H, xy \in H$ (propriété de stabilité de H par l'opération de groupe)
3. $\forall x \in H, x^{-1} \in H$ (propriété de stabilité de H par passage à l'inverse)

Exemples.
$(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$.
$(\mathbb{Q},+)$ est un sous-groupe de $(\mathbb{R},+)$.
$(\mathbb{R},+)$ est un sous-groupe de $(\mathbb{C},+)$.
$(\{+1,-1\},\cdot)$ est un sous-groupe de $(U,\cdot)$ (U est l'ensemble des nombres complexes de module 1).
$(U,\cdot)$ est un sous-groupe de $(\mathbb{C}-\{0\},\cdot)$.

Le résultat suivant est très simple à démontrer. C'est pourquoi nous en laissons la preuve au lecteur.

Théorème 2.2. *Si H est un sous-groupe de G, alors H, muni de l'opération de G, est un groupe.*

Définition. *Soient $(G,\cdot),(H,*)$ deux groupes.* **Un morphisme de groupes** *est une application $f : G \to H$ qui vérifie*
$$\forall x, y \in G, f(x \cdot y) = f(x) * f(y)$$

Important : Pour former $x \cdot y$, on utilise l'opération de G, et pour former $f(x) * f(y)$, celle de H.

Exemples.
1. L'application $\exp : \mathbb{R} \to \mathbb{R}_+^* : x \mapsto e^x$ est un morphisme de groupes de $(\mathbb{R},+)$ vers $(\mathbb{R}_+^*,\cdot)$, car $e^{x+y} = e^x \cdot e^y$.
2. L'application $\mathbb{R}_+^* \to \mathbb{R} : x \mapsto \ln x$ est un morphisme de groupes de $(\mathbb{R}_+^*,\cdot)$ vers $(\mathbb{R},+)$.

Définition.
Un isomorphisme de groupes *est un morphisme de groupes qui est bijectif.*
Un endomorphisme de groupe *est un morphisme d'un groupe vers le même groupe.*
Un automorphisme de groupe *est un endomorphisme de groupe qui est bijectif.*
Deux groupes G, H sont appelés **isomorphes** *s'il existe un isomorphisme de groupes de G vers H.*

Exemples.
1. L'application $\exp : \mathbb{R} \to \mathbb{R}_+^* : x \mapsto e^x$ est un isomorphisme de groupes de $(\mathbb{R},+)$ vers $(\mathbb{R}_+^*,\cdot)$. Donc les groupes $(\mathbb{R},+)$ et $(\mathbb{R}_+^*,\cdot)$ sont isomorphes.
2. Si a est un entier, l'application $\mathbb{Z} \to \mathbb{Z} : n \mapsto an$ est un endomorphisme du groupe $(\mathbb{Z},+)$.
C'est un automorphisme si et seulement si $a = \pm 1$.

Théorème 2.3. *Soit G un groupe, et x, y, z trois éléments quelconques de G.*
1. Si $xz = yz$, alors $x = y$.
2. Si $zx = zy$, alors $x = y$.

Preuve. 1. On suppose $xz = yz$. Mais alors $(xz)z^{-1} = (yz)z^{-1}$. Donc $x(zz^{-1}) = y(zz^{-1})$, ce qui donne $x = y$. Pour la partie 2. on procède de manière analogue. □.

Théorème 2.4. *Soit $f : G \to H$ un morphisme de groupes. Alors*
1. $f(e_G) = e_H$
2. $\forall x \in G, f(x^{-1}) = f(x)^{-1}$

Preuve.
1. On a $e_H f(e_G) = f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$, la dernière égalité étant vraie parce f est un morphisme. En vertu du théorème qui précède, on peut dire $e_H = f(e_G)$.
2. On part de $xx^{-1} = x^{-1}x = e_G$. Donc $f(xx^{-1}) = f(x^{-1}x) = f(e_G) = e_H$. Comme f est un morphisme, $f(x)f(x^{-1}) = f(x^{-1})f(x) = e_H$. On peut en déduire que $f(x^{-1})$ est l'inverse de $f(x)$.
□

1.6 Noyau et image d'un morphisme de groupes

Définition. *Soit $f : G \to H$ un morphisme de groupes.*
Le noyau de *f, noté* $\ker f$*, est l'ensemble des éléménts de G qui sont envoyés sur e_H.*
L'image de *f, notée $Im\ f$ est l'ensemble des images des éléments de G par f.*

$$\ker f = \{x \in G | f(x) = e_H\} \subset G \qquad Im\ f = \{f(x) | x \in G\} \subset H$$

Dire que $y \in \text{Im } f$ est équivalent à : $y \in H$ et $\exists x \in G, f(x) = y$.

Théorème 2.5. *Soit $f : G \to H$ un morphisme de groupes.*
Alors $\ker f$ *est un sous-groupe de G et $Im\ f$ est un sous-groupe de H.*

Preuve. Montrons d'abord que $\ker f$ est un sous-groupe de G.
L'élément neutre de G appartient au noyau, car $f(e_G) = e_H$.
Si x, y sont dans le noyau, alors $f(xy) = f(x)f(y) = e_H e_H = e_H$, donc xy est aussi dans le noyau.
Si x est dans le noyau, alors $f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H$.
Nous avons bien montré que $\ker f$ est un sous-groupe de G.
Montrons maintenant que Im f est un sous-groupe de H.
L'élément neutre de H appartient dans l'image, car $e_H = f(e_G)$.
Si x, y sont dans l'image, alors on peut écrire $x = f(a), y = f(b)$, avec $a, b \in G$. Donc $xy = f(a)f(b) = f(ab)$, et comme $ab \in G$, on voit que xy est dans l'image.
Si x est dans l'image, alors $f(a) = x$ pour un certain a et alors $x^{-1} = f(a^{-1})$, ce qui achève la preuve. □

Si on a un morphisme de groupes entre deux groupes G et H, on construit donc facilement de nouveaux groupes en considérant le noyau et l'image de ce morphisme. On obtient un sous-groupe de G (le noyau) et un sous-groupe de H (l'image). En voici une application :

Théorème 2.6. *Pour tout $n \geqslant 1$, l'ensemble des racines n-èmes de l'unité, muni de la multiplication des nombres complexes, est un groupe commutatif.*

Rappel. Une racine n-ème de l'unité est un nombre complexe tel que $z^n = 1$.

Preuve. On sait que $(\mathbb{C}^* = \mathbb{C} - \{0\}, \cdot)$ est un groupe commutatif, d'élément neutre 1. L'application $f : \mathbb{C} \to \mathbb{C} : z \mapsto z^n$ est un endomorphisme du groupe $(\mathbb{C}^*, \cdot)$, car on a clairement $(zz')^n = z^n z'^n$. Donc le noyau de cet endomorphisme est un sous-groupe de $(\mathbb{C}^*, \cdot)$. Mais le noyau est exactement l'ensemble des nombres complexes non nuls z tels que $z^n = 1$. C'est exactement l'ensemble des racines n-èmes de l'unité. C'est donc un sous-groupe de $(\mathbb{C}^*, \cdot)$. Donc, si on munit cet ensemble de la multiplication des nombres complexes, on obtient un groupe, qui est également commutatif, car il est sous-groupe d'un groupe commutatif. □

On note U_n le groupe des racines n-èmes de l'unité. Il possède exactement n éléments. Ce sont les nombres complexes z de la forme $z = e^{\frac{2\pi i k}{n}}$, avec $k \in \mathbb{Z}$. Bien entendu, si on remplace k par $k + n$, on obtient le même nombre complexe z, car $e^{2\pi i} = 1$.

2 Anneaux

2.1 Définition d'un anneau

Nous avons déjà vu que l'ensemble $\mathbb{Z}$, avec l'opération de somme, est un groupe commutatif. Mais sur les entiers, il y a une autre opération binaire interne, la multiplication. Elle a notamment les propriétés suivantes

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativité)
$a \cdot 1 = 1 \cdot a = a$ (neutre pour la multiplication)
$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ et
$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributivité de la multiplication par rapport à l'addition)

Nous rencontrerons souvent ce type de propriété avec deux lois binaires internes. Nous allons donner une définition très générale, qui correspond à des ensembles appelés **anneaux**.

Définition. *Soit A un ensemble muni de deux lois binaires internes, notées $+$ et $\cdot$*
On dit que $(A,+,\cdot)$ est **un anneau** *si les propriétés suivantes sont satisfaites :*
1. $(A,+)$ est un groupe commutatif
2. L'opération $\cdot$ est associative
3. Il existe un élément $m \in A$ tel que $\forall x \in A, x \cdot m = m \cdot x = x$
4. $\forall x,y,z \in A, x \cdot (y+z) = (x \cdot y) + (x \cdot z)$ et $(x+y) \cdot z = (x \cdot z) + (y \cdot z)$.

Définition. *On dit qu'un anneau est* **commutatif** *si la loi $\cdot$ est commutative.*

Remarques.
1. Dans la notation mathématique, on décide que la deuxième opération (souvent appelée la multiplication) est **prioritaire** sur la première opération (souvent appelée l'addition). C'est pourquoi on peut écrire $x \cdot y + x \cdot z$ au lieu de $(x \cdot y) + (x \cdot z)$.
2. Comme pour les groupes, on montre que l'élément m tel que $m \cdot x = x \cdot m = x$ est unique. On l'appelle **le neutre pour la multiplication** $\cdot$

2.2 Exemples

$(\mathbb{Z},+,\cdot)$ est un anneau commutatif. Il en est de même de $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ et $(\mathbb{C},+,\cdot)$.

Il existe des exemples un peu plus étranges. Ainsi, si E est un ensemble, et $\mathcal{P}(E)$ l'ensemble des sous-ensembles de E, alors $(\mathcal{P}(E),\Delta,\cap)$ est un anneau. L'opération Δ est la différence symétrique, et $\cap$ l'intersection. On pourra vérifier les détails. En particulier, on verra que l'élément neutre pour Δ est $\varnothing$, que l'inverse de $A \subset E$ pour Δ est A, et que l'élément neutre pour $\cap$ est E. Cet anneau est un anneau commutatif. Plus tard, nous verrons des exemples d'anneaux non commutatifs.

2.3 Premières propriétés

Théorème 2.7. *Soit $(A,+,\cdot)$ un anneau. On note 0 l'élément neutre de l'opération $+$, et on note $-x$ l'inverse de x pour cette même opération $+$.*
1. $\forall x \in A, \quad 0 \cdot x = x \cdot 0 = 0$
2. $\forall x,y \in A, \quad x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$

Preuve. 1. Par distributivité $x \cdot (0+0) = x \cdot 0 + x \cdot 0$. Cela peut aussi s'écrire $x \cdot 0 + 0 = x \cdot 0 + x \cdot 0$. En ajoutant l'inverse (par rapport à la loi $+$) de $x \cdot 0$ on trouve $0 = x \cdot 0$. On prouve de la même manière que $0 = 0 \cdot x$.
2. On utilise $(-x) \cdot y + x \cdot y = (-x+x) \cdot y = 0$. □

Théorème 2.8. *Soit $(A,+,\cdot)$ un anneau, et $a_1,\dots,a_m$, $b_1,\dots,b_n$ des éléments de A.*
Si I est un ensemble fini, et $(x_i)_{i\in I}$ une famille d'éléments de A indexée par I, on note $\sum_{i\in I} x_i$ la somme (pour l'opération $+$ de A) de tous les éléments x_i. Comme $+$ est une opération commutative, l'ordre des termes n'a pas d'importance.
Alors on a la formule

$$\left(\sum_{i=1}^{m} a_i\right) \cdot \left(\sum_{j=1}^{n} b_j\right) = \sum_{(i,j)\in[[1,m]]\times[[1,n]]} a_i \cdot b_j$$

Puisque l'ordre dans la somme n'a pas d'importance, on peut aussi écrire

$$\left(\sum_{i=1}^{m} a_i\right) \cdot \left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_i \cdot b_j\right)$$

et

$$\left(\sum_{i=1}^{m} a_i\right) \cdot \left(\sum_{j=1}^{n} b_j\right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_i \cdot b_j\right)$$

Preuve. Utiliser la distributivité de l'anneau. □

2.4 Inversibles d'un anneau

Définition. *Soit $(A,+,\cdot)$ un anneau. On note 1 l'élément neutre pour $\cdot$.* **Un élément inversible de** *A est un élément $x \in A$ tel qu'il existe $y \in A$ avec $x \cdot y = y \cdot x = 1$.*

Exemples.
1. Dans l'anneau $\mathbb{Z}$, il y a exactement deux éléments inversibles, à savoir 1 et -1.
2. Dans l'anneau $(\mathcal{P}(E), \Delta, \cap)$, il y a un seul élément inversible, à savoir E.
3. Dans l'anneau $\mathbb{Q}$, tous les éléments différents de 0 sont inversibles.

Théorème 2.9. *Soit $(A,+,\cdot)$ un anneau.*
1. Le produit de deux éléments inversibles de A est un élément inversible de A.
2. L'opération $\cdot$ est une opération de groupe sur l'ensemble des éléments inversibles de A.

Preuve. 1. Soient x, x' deux éléments inversibles de A, alors il existe des éléments y, y' de A avec $xy = yx = x'y' = y'x' = 1$. Mais alors $(xx')(y'y) = 1$ et $(y'y)(xx') = 1$, donc xx' est bien inversible.
2. L'opération $\cdot$ est donc binaire interne sur l'ensemble des éléments inversibles. Il est ensuite très facile de montrer qu'il s'agit d'une opération de groupe sur cet ensemble. □

Définition. *Si A est un anneau, on appelle* **groupe des inversibles de** *A l'ensemble des éléments inversibles de A, muni de la deuxième opération de A. On note ce groupe A^o.*

Exemples.
1. $\mathbb{Z}^o = (\{+1,-1\},\cdot)$. Ce groupe est isomorphe à $(U_2,\cdot)$.
2. $\mathbb{Q}^o = (\mathbb{Q}^*,\cdot)$. De même $\mathbb{R}^o = (\mathbb{R}^*,\cdot)$.

2.5 Le binôme de Newton

Rappelons que le symbole C_n^k désigne le nombre $\dfrac{n!}{k!(n-k)!}$, où k, n sont deux entiers avec $0 \leqslant k \leqslant n$.

Théorème 2.10. *Soient x, y deux éléments d'un anneau commutatif A et n un entier naturel. Alors*

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k} = y^n + nxy^{n-1} + \frac{n(n-1)}{2}x^2y^{n-2} + \cdots + nx^{n-1}y + x^n$$

Remarque. Le terme $C_n^k x^k y^{n-k}$ signifie qu'on additionne C_n^k fois l'élément $x^k y^{n-k}$ de l'anneau A (les entiers de $\mathbb{Z}$ ne font pas forcément partie de l'anneau A).

Preuve. Par récurrence sur n. Si $n = 0$, $(x+y)^n = (x+y)^0 = 1$ et $\displaystyle\sum_{k=0}^{0} C_n^k x^k y^{n-k} = C_0^0 x^0 y^0 = 1$, donc la propriété est vraie pour $n = 0$.
Supposons maintenant que la formule est vraie pour un entier donné n, et prouvons qu'alors elle est aussi vraie pour $n+1$. On peut donc dire que

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

Si on multiplie l'équation par $x+y$ on trouve

$$(x+y)^{n+1} = (x+y)\sum_{k=0}^{n} C_n^k x^k y^{n-k} = x(\sum_{k=0}^{n} C_n^k x^k y^{n-k}) + y(\sum_{k=0}^{n} C_n^k x^k y^{n-k})$$

On poursuit le calcul par les règles de distributivité

$$(x+y)^{n+1} = \sum_{k=0}^{n} xC_n^k x^k y^{n-k} + \sum_{k=0}^{n} yC_n^k x^k y^{n-k}$$

Comme on suppose que A est commutatif on a le droit d'écrire

$$(x+y)^{n+1} = \sum_{k=0}^{n} C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^{n} C_n^k x^k y^{n+1-k}$$

Changeons de variable dans le premier terme

$$(x+y)^{n+1} = \sum_{k=1}^{n+1} C_n^{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} C_n^k x^k y^{n+1-k} = y^{n+1} + \sum_{k=1}^{n} (C_n^{k-1} + C_n^k) x^k y^{n+1-k} + x^{n+1}$$

Or on sait que $C_n^{k-1} + C_n^k = C_{n+1}^k$. D'où

$$(x+y)^{n+1} = y^{n+1} + \sum_{k=1}^{n} C_{n+1}^k x^k y^{n+1-k} + x^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}$$

Ceci démontre la propriété pour l'exposant $n+1$. La preuve par récurrence s'achève ici. □

Généralisation.
Dans la preuve, on a seulement utilisé que $xy = yx$. Donc on n'a pas besoin d'exiger que A soit commutatif, mais seulement que $xy = yx$ pour les deux éléments qui figurent dans la formule du binôme de Newton.

Corollaire 2.11. *Pour tout $n \geqslant 0$, on a $\sum_{k=0}^{n} C_n^k = 2^n$. Pour tout $n \geqslant 1$, on a $\sum_{k=0}^{n} (-1)^k C_n^k = 0$.*

Preuve. Pour la première relation, on applique le binôme de Newton avec $x = y = 1$. Pour la seconde, on prend $x = -1, y = 1$. □

2.6 Factorisation de $x^n - y^n$

Théorème 2.12. *Soient x, y deux éléments $(A, +, \cdot)$ un anneau commutatif (ou plus généralement deux éléments d'un anneau quelconque avec $x \cdot y = y \cdot x$). Alors pour tout entier $n \geqslant 1$, on a*

$$x^n - y^n = (x-y) \cdot \sum_{k=0}^{n-1} x^k y^{n-1-k}$$

Preuve.
Il suffit de développer le membre de droite par distributivité, appliquer $xy = yx$ et simplifier. □

Remarques.
1. La célèbre égalité $(x+y)(x-y) = x^2 - y^2$ est simplement le cas $n = 2$ du théorème ci-dessus.
2. Si $y = 1$, on trouve $x^n - 1 = (x-1)(x^{n-1} + \cdots + 1)$.

3 Corps

3.1 Définition et exemples

Définition.
Un corps *est un anneau $(A, +, \cdot)$ non réduit à $\{0_A\}$ dans lequel tout $x \in A - \{0_A\}$ est inversible.*
Un corps est donc un anneau A pour lequel $(A - \{0\}, \cdot)$ est un groupe.
On dit qu'un corps est **commutatif** *si la loi $\cdot$ est commutative.*

Exemples. Les anneaux $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sont tous les trois des corps commutatifs.
L'anneau $(\mathbb{Z}, +, \cdot)$ n'est pas un corps, car $2 \neq 0$ et 2 n'est pas inversible dans $\mathbb{Z}$, c'est-à-dire il n'existe pas d'entier n avec $2 \cdot n = n \cdot 2 = 1$.

Commentaire. Nous avons vu trois objets algébriques, d'abord les groupes, puis les anneaux et enfin les corps. Dans un groupe $(G, +)$ on peut «ajouter» et «soustraire» (faire $x + y$ et $x + (-y)$). Dans un anneau, on peut «ajouter», «soustraire» (comme dans un groupe) mais aussi «multiplier» (faire $x \cdot y$). Enfin, dans un corps, on peut «ajouter», «soustraire», «multiplier» et «diviser (par autre chose que 0)». La division de x par $y \neq 0$ dans un corps, c'est par définition $x \cdot y^{-1}$ (ou $y^{-1} \cdot x$), avec y^{-1} qui désigne l'inverse de y. Cet inverse existe précisément parce qu'on est dans un corps.

3.2 Sommes de progressions géométriques

Rappelons qu'une progression géométrique est une suite de nombres non nuls $a_0, a_1, \ldots$ telle que le rapport $\frac{a_{n+1}}{a_n}$ soit constant. Ce rapport est appelé **la raison de la progression géoémtrique**. Le résultat ci-dessous nous donne une formule pour des sommes d'un nombre fini de termes dans une progression géométrique. Nous allons l'énoncer dans un cadre très général, à savoir celui d'un corps quelconque.

Théorème 2.13. *Soit K un corps, n un entier $\geqslant 1$ et $q \in K$ avec $q \neq 1_K$. Alors*
$\sum_{k=0}^{n-1} q^k = 1 + q + q^2 + \cdots + q^{n-1} = (q^n - 1) \cdot (q-1)^{-1} = (q-1)^{-1} \cdot (q^n - 1)$
Ici $(q-1)^{-1}$ désigne l'inverse multiplicatif de $q-1$, qui existe car K est un corps et $q - 1 \neq 0$.

Remarque. Dans les corps usuels commutatifs, c'est-à-dire $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, on écrira évidemment $\frac{q^n - 1}{q-1}$ au lieu de $(q^n - 1) \cdot (q-1)^{-1}$.

Preuve. Comme K est un anneau, et que $q \cdot 1 = 1 \cdot q$, on peut appliquer le résultat de factorisation de $q^n - 1^n$. On aura

$$q^n - 1 = q^n - 1^n = (q-1)(1 + q + \cdots + q^{n-1})$$

et aussi

$$q^n - 1 = (1 + q + \cdots + q^{n-1})(q-1)$$

Si on multiplie la première équation à gauche par $(q-1)^{-1}$, et la seconde équation à droite par $(q-1)^{-1}$, on obtient les résultats voulus. □

Application. Calculer $2^a + 2^{a+1} + \cdots + 2^b$, où a, b sont deux entiers de $\mathbb{Z}$ avec $a \leqslant b$.

On reconnaît une progression géométrique de raison 2. On peut écrire

$$2^a + 2^{a+1} + \cdots + 2^b = 2^a(2^0 + 2^1 + \cdots + 2^{b-a}) = 2^a \frac{2^{b-a+1} - 1}{2-1} = 2^{b+1} - 2^a$$

4 Vocabulaire du chapitre

Un groupe	abélien	l'image
un anneau	le groupe symétrique	prioritaire
un corps	un sous-groupe	inversible
un entier	un morphisme	le groupe des inversibles
une opération interne	un isomorphisme	le binôme de Newton
neutre	un automorphisme	une factorisation
inverse	un endomorphisme	une progression géométrique
le module	isomorphes	la raison
commutatif	le noyau	

5 Exercices

1. Soient a, b deux éléments quelconques d'un corps K. Résoudre dans K l'équation $ax + b = 0$ d'inconnue x. Résoudre dans K l'équation $xa + b = 0$.

2. Soit $n \geqslant 2$ et $\omega \in \mathbb{C} - \{1\}$ tel que $\omega^n = 1$. Combien y a-t-il de valeurs pour ω ? Calculer $1 + \omega + \omega^2 + \cdots + \omega^{n-1}$.

3. Soit G un groupe. On note

$$Z(G) = \{x \in G | \forall y \in G, xy = yx\}.$$

Montrer que $Z(G)$ est un sous-groupe de G. Que peut-on dire de G si on a l'égalité $Z(G) = G$?

4. Soit $(G, \times)$ un groupe fini. Montrer que pour tout $g \in G$, il existe un entier $n > 0$ tel que

$$g^n = \underbrace{g \times g \times \cdots \times g}_{n} = e.$$

5. Dans un anneau commutatif, calculer $(a+b+c)(-a+b+c)(a-b+c)(a+b-c)$.

6. Dans un anneau commutatif, factoriser $xy(y-x)+yz(z-y)+zx(x-z)$.

7. Dans un corps, montrer qu'on a l'implication

$$a_1a_2\cdots a_n=0 \Rightarrow a_1=0 \text{ ou } a_2=0 \text{ ou } \cdots \text{ ou } a_n=0.$$

8. Soit K un corps commutatif. On suppose que $a,b\in K$ et $x,y\in K-\{0\}$. Donner une écriture factorisée pour

$$a\cdot x^{-1}+b\cdot y^{-1}.$$

9. Soit K un corps commutatif et $x\in K-\{0_K,1_K\}$ (x différent des deux neutres de K). Simplifier

$$\frac{1}{1-\dfrac{1}{1-\dfrac{1}{1-x}}}.$$

10. Dans un corps non commutatif K, on prend a,b avec b non nul. Quel est le sens de l'écriture $\dfrac{a}{b}$?

11. Dans un anneau commutatif, calculer

$$(a-b)(a^2+ab+b^2)(a^6+a^3b^3+b^6)(a^{18}+a^9b^9+b^{18}).$$

12. Pourquoi le nombre de bijections de $[\![1,n]\!]$ vers lui-même est-il égal à $n!$?

13. Montrer : S'il existe un isomorphisme de groupes $\varphi : G_1\to G_2$, alors il existe aussi un isomorphisme de groupes $\psi : G_2\to G_1$.

Chapitre 3. Espaces vectoriels

1 Définition d'espace vectoriel

Définition. *Soit $(K,+,\cdot)$ un corps commutatif.* **Un espace vectoriel sur le corps** K *est un ensemble V, muni d'une loi de composition interne notée $+$, et d'une multiplication externe (une loi qui associe à tout couple (r,v) (où $r\in K$, $v\in V$) un élément noté $r\cdot v$ de V), et qui vérifie les propriétés ci-dessous :*

1) $(V,+)$ *est un groupe commutatif*
2) $\forall v\in V,$ $\quad 1\cdot v=v$
3) $\forall (r,r')\in K,\forall v\in V,$ $\quad (r\cdot r')\cdot v=r\cdot(r'\cdot v)$
4) $\forall r\in K,\forall (v,v')\in V,$ $\quad r\cdot(v+v')=r\cdot v+r\cdot v'$
5) $\forall (r,r')\in K,\forall v\in V,$ $\quad (r+r')\cdot v=r\cdot v+r'\cdot v$

Les éléments de l'espace vectoriel V sont appelés **vecteurs.**

Les éléments du corps K sont appelés **scalaires.**

En pratique, le corps K est souvent le corps $(\mathbb{R},+,\cdot)$ des nombres réels, ou le corps $(\mathbb{C},+,\cdot)$ des nombres complexes.

Exemples.
1. Soit K un corps commutatif quelconque. On prend $V=K$, on munit V de l'addition de K, et on définit la multiplication externe par

$$r\cdot v := r\cdot_K v$$

où $\cdot_K$ est la multiplication dans K. Alors les propriétés ci-dessus sont toutes vraies, et on peut donc dire que l'ensemble K est un espace vectoriel sur K.

2. Soit K un corps commutatif, et soient V,W deux espaces vectoriels sur le corps K. Nous pouvons alors faire du produit cartésien $V\times W$ un espace vectoriel sur K, en définissant l'addition et la multiplication externe comme suit :

$$\begin{aligned}\forall (v,w)\in V\times W,(v',w')\in V\times W, &\qquad (v,w)+(v',w')=(v+_V v', w+_W w')\\ \forall r\in K,\forall (v,w)\in V\times W, &\qquad r\cdot(v,w)=(r\cdot_V v, r\cdot_W w)\end{aligned}$$

3. Avec 1. et 2. nous pouvons donc faire de $K\times K\times\cdots\times K$ (n fois) un espace vectoriel sur K. On le note K^n. Ainsi, par exemple, $\mathbb{R}^n$ est un espace vectoriel sur $\mathbb{R}$, $\mathbb{C}^n$ est un espace vectoriel sur $\mathbb{C}$, $\mathbb{Q}^n$ est un espace vectoriel sur $\mathbb{Q}$.
Le cas $n=0$ donne aussi un espace vectoriel sur K. C'est l'ensemble $\{0\}$, sur lequel l'addition interne est définie par $0+0=0$ et la multiplication externe par $r\cdot 0=0$. Bien sûr, ce n'est pas un espace vectoriel très intéressant, car il n'a qu'un seul élément.

4. Soit X un ensemble, et V un espace vectoriel sur un corps commutatif K. On considère l'ensemble $\mathcal{F}(X,V)$ de toutes les applications de X dans V. On peut définir une addition interne sur $\mathcal{F}(X,V)$ par la loi

$$\forall f,g\in\mathcal{F}(X,V),\qquad f+g: X\to V: x\mapsto f(x)+_V g(x)$$

On peut aussi définir une multiplication externe par

$$\forall r\in K,\forall f\in\mathcal{F}(X,V),\qquad r\cdot f: X\to V: x\mapsto r\cdot(f(x))$$

Il est facile de vérifier que $\mathcal{F}(X,V)$ est alors un espace vectoriel sur K.
En particulier $\mathcal{F}(\mathbb{R},\mathbb{R})$ est un espace vectoriel sur $\mathbb{R}$. De même $\mathcal{F}([0,1],\mathbb{R}^n)$ est un espace vectoriel sur $\mathbb{R}$.

5. Considérons $\mathbb{C}$ avec l'addition usuelle, et avec la multiplication externe par des scalaires $r\in\mathbb{R}$ définie par la restriction à $\mathbb{R}$ de la multiplication usuelle sur $\mathbb{C}$. On obtient alors un espace vectoriel sur $\mathbb{R}$.
De la même façon, $\mathbb{R}$ est un espace vectoriel sur le corps $\mathbb{Q}$.

2 Propriétés élémentaires

Théorème 3.1. *Soit V un espace vectoriel sur un corps commutatif K. On note 0_V le neutre du groupe $(V,+)$, et on note 0_K le neutre du groupe additif 0_K. Alors*
1. $\forall v \in V, \qquad 0_K \cdot v = 0_V$
2. $\forall r \in K, \qquad r \cdot 0_V = 0_V$
3. $\forall r \in K, v \in V, \qquad (-r)\cdot v = r \cdot (-v) = -(r \cdot v)$
4. Si $r \in K, v \in V$ *et* $r \cdot v = 0_V$, *alors* $r = 0_K$ *ou* $v = 0_V$.

Preuve. 1. Par les propriétés d'un espace vectoriel, on a

$$(0_K + 0_K)\cdot v = 0_K \cdot v + 0_K \cdot v$$

et donc

$$0_K \cdot v = 0_K \cdot v + 0_K \cdot v$$

En ajoutant l'opposé du vecteur $0_K \cdot v$ aux deux membres de l'équation, on aura

$$0_V = 0_K \cdot v$$

2. La preuve est similaire.

3. On a

$$(r + (-r))\cdot v = r \cdot v + (-r)\cdot v$$

On sait grâce à 1. que le membre de gauche est égal à 0_V. Donc les vecteurs $r \cdot v$ et $(-r)\cdot v$ sont opposés, ce qui signifie

$$(-r)\cdot v = -(r \cdot v)$$

D'un autre côté, on a

$$r \cdot (v + (-v)) = r \cdot v + r \cdot (-v)$$

Le membre de gauche est égal à 0_V par 2. Donc les vecteurs $r \cdot v$ et $r \cdot (-v)$ sont opposés, ce qui signifie

$$r \cdot (-v) = -(r \cdot v)$$

Ceci achève la preuve.
4. L'hypothèse dit que $r \cdot v = 0_V$. On suppose $r \neq 0_K$. Il suffit alors de montrer que $v = 0_V$.
Comme K est un corps, et que r n'est pas le neutre additif de l'addition, il existe un inverse multiplicatif r^{-1} de r. Si on multiplie l'équation $r \cdot v = 0_V$ par cet inverse on trouve successivement

$$\begin{aligned} r^{-1}\cdot(r\cdot v) &= r^{-1}\cdot 0_V \\ (r^{-1}\cdot r)\cdot v &= 0_V \\ 1\cdot v &= 0_V \\ v &= 0_V \end{aligned}$$

□

3 Sous-espaces vectoriels

Définition. *Soit V un espace vectoriel sur un corps commutatif K.*
Un sous-espace vectoriel de *V est un sous-ensemble W de V qui vérifie les propriétés suivantes :*
i) $0_V \in W$
ii) $\forall w_1, w_2 \in W, \qquad w_1 + w_2 \in W$
iii) $\forall r \in K, \forall w \in W, \qquad r \cdot w \in W$.

Remarques.
1. La condition «ii) et iii)» est équivalente à : $\forall r_1, r_2 \in K, \forall w_1, w_2 \in W, r_1 \cdot w_1 + r_2 \cdot w_2 \in W$.

2. Un sous-espace vectoriel de V est un sous-groupe W de $(V,+)$ tel que $\forall r \in K, \forall w \in W, r \cdot w \in W$.
Cette dernière condition est appelée **la stabilité de W par la multiplication externe.**

Exemples.
1. Prenons $V = \mathbb{R}^2$, qui est un espace vectoriel sur le corps $\mathbb{R}$ des nombres réels.
a) $W = \{0\}$ est un sous-espace vectoriel de V.
b) $W = \{(x, 0) | x \in \mathbb{R}\}$ est un sous-espace vectoriel de V.
c) $W = \{(x, y) | x + 2y = 0\}$ est un sous-espace vectoriel de V.
d) $W = \{(x, y) | x + 2y = 1\}$ n'est pas un sous-espace vectoriel de V.
e) $W = \{(x, 0) | x \in \mathbb{Q}\}$ n'est pas un sous-espace vectoriel de V.

2. Prenons $V = \mathcal{F}(\mathbb{R}, \mathbb{R})$, qui est un espace vectoriel sur $\mathbb{R}$.
a) $W = \{f \in V | f \text{ est continue}\}$ est un sous-espace vectoriel de V.
b) $W = \{f \in V | f \text{ est dérivable}\}$ est un sous-espace vectoriel de V.
c) $W = \{f \in V | f \text{ est de classe } C^2\}$ est un sous-espace vectoriel de V.
d) $W = \{f \in V | f(1) = 0\}$ est un sous-espace vectoriel de V.
e) $W = \{f \in V | f(1) \geqslant 0\}$ n'est pas un sous-espace vectoriel de V.

Remarque. Si W est un sous-espace vectoriel de l'espace vectoriel V (sur le corps commutatif K), alors W est lui-même un espace vectoriel (avec la même addition et la même multiplication externe que V).

> **Théorème 3.2.** *Soit V un espace vectoriel sur un corps commutatif K. Soit $(W_i)_{i \in I}$ une famille de sous-espaces vectoriels W_i de V. Alors l'intersection de tous les W_i, c'est-à-dire*
>
> $$\bigcap_{i \in I} W_i$$
>
> *est aussi un sous-espace vectoriel de V.*
>
> **Preuve.** Appelons A l'intersection $\bigcap_{i \in I} W_i$. Pour montrer que A est un sous-espace vectoriel de V, nous allons vérifier que $0_V \in A$ et ensuite que $\forall r_1, r_2 \in K, \forall v_1, v_2 \in A, r_1 v_1 + r_2 v_2 \in A$.
>
> Comme tous les W_i sont des sous-espaces vectoriels de V, on a $0_V \in W_i$ pour tout $i \in I$.
> Donc $0_V \in A$.
>
> Prenons v_1, v_2 dans A. Alors $v_1, v_2 \in W_i$ pour tout $i \in I$. Comme W_i est un sous-espace vectoriel, on peut dire que $r_1 v_1 + r_2 v_2 \in W_i$. Or ceci est vrai pour tout W_i. Donc $r_1 v_1 + r_2 v_2 \in A$. □

On dit parfois que la propriété «être un sous-espace vectoriel de V» est stable par intersection.

Grâce à ceci, nous pouvons donner notre prochaine définition.

> **Définition.** *Soit V un espace vectoriel, et $A \subset V$ une partie quelconque de V.*
> **Le sous-espace vectoriel engendré par** *A est l'intersection de tous les sous-espaces vectoriels qui contiennent l'ensemble A. On le note $\langle A \rangle$ ou* $\mathrm{Vect}(A)$.

En d'autres mots, on regarde la famille $(W_i)_{i \in I}$ de tous les sous-espaces vectoriels de V tels que $A \subset W_i$, et on pose $\langle A \rangle = \bigcap_{i \in I} W_i$.
Bien sûr, $\langle A \rangle$ est un sous-espace vectoriel de V, on a $A \subset \langle A \rangle$, et $\langle A \rangle$ est le plus petit sous-espace vectoriel de V qui contient A. En particulier : Si W est un sous-espace vectoriel contenant A, alors W contient aussi $\langle A \rangle$.

Exemples. Prenons $V = \mathbb{R}^2$ sur le corps $\mathbb{R}$.
1. Si $A = \{(x, 0) | x \in \mathbb{R}\}$, $\quad \langle A \rangle = A$.
2. Si $A = \{(1, 0)\}$, $\quad \langle A \rangle = \{(x, 0) | x \in \mathbb{R}\}$.
3. Si $A = \varnothing$, $\quad \langle A \rangle = \{(0, 0)\}$.
4. Si $A = \{(1, 0), (0, 1)\}$, $\quad \langle A \rangle = \mathbb{R}^2$.

3.1 Somme de sous-espaces vectoriels. Décomposition en somme directe

Définition. *Soit V un espace vectoriel sur un corps commutatif K, et soient $W_1, \dots, W_n$ des sous-espaces vectoriels de V.* **La somme des sous-espaces vectoriels** *$W_1, \dots, W_n$ est l'ensemble $\{w_1 + \cdots + w_n | \forall i \in [[1,n]], w_i \in W_i\}$. On note cet ensemble $W_1 + \cdots + W_n$ ou encore $\sum_{i=1}^{n} W_i$.*

Théorème 3.3. *$W_1 + \cdots + W_n$ est un sous-espace vectoriel de V.*

Preuve.
1. Si on prend $w_1 = \cdots = w_n = 0_V$, on voit bien que $0_V \in W_1 + \cdots + W_n$.
2. Ensuite, prenons deux éléments x, x' de $W_1 + \cdots + W_n$. On a

$$x = \sum_{i=1}^{n} w_i, \qquad x' = \sum_{i=1}^{n} w_i'.$$

Dès lors, $x + x' = \sum_{i=1}^{n} (w_i + w_i')$. Dans le membre de droite, la parenthèse $(w_i + w_i')$ est un élément de W_i (car W_i est un sous-espace vectoriel). Donc $x + x' \in W_1 + \cdots + W_n$.

3. Enfin, soit $r \in K$ et $x = \sum_{i=1}^{n} w_i \in W_1 + \cdots + W_n$. Alors

$$r \cdot x = \sum_{i=1}^{n} r \cdot w_i.$$

Comme $r \cdot w_i \in W_i$ pour tout $i \in [[1,n]]$, il en découle que $r \cdot x \in W_1 + \cdots + W_n$. □

Définition. *Soit V un espace vectoriel, et soient $W_1, \dots, W_n$ des sous-espaces vectoriels de V. On dit que V* **se décompose en somme directe de** *$W_1, \dots, W_n$, ou que V* **est la somme directe de** *$W_1, \dots, W_n$, si on a*
i) $W_1 + \cdots + W_n = V$,
ii) $\forall (w_1, \dots, w_n) \in W_1 \times \cdots \times W_n, (w_1 + \cdots + w_n = 0_V \Rightarrow w_1 = \cdots = w_n = 0_V)$.
Lorsque V se décompose en somme directe de $W_1, \dots, W_n$, on écrit $V = W_1 \oplus \cdots \oplus W_n$ ou encore $V = \bigoplus_{i=1}^{n} W_i$.
Lorsque $n = 2$, c'est-à-dire $V = W_1 \oplus W_2$, on dit que W_1 est **un supplémentaire** *de W_2, et que W_2 est* **un supplémentaire** *de W_1.*

Remarques.
1. Si $V = W_1 \oplus W_2$, alors $V = W_2 \oplus W_1$.
2. En général, il est **faux** de dire que $V = W_1 \oplus W_2$ implique $V = W_1 \cup W_2$. Il peut exister des vecteurs $v \in V$ avec $v \notin W_1$ et $v \notin W_2$.

Théorème 3.4. *Soit V un espace vectoriel, et $W_1, \dots, W_n$ des sous-espaces vectoriels de V.*
Les deux phrases ci-dessous sont équivalentes :
i) $V = W_1 \oplus \cdots \oplus W_n$,
ii) Pour tout $v \in V$, il existe un unique n-uplet $(w_1, \dots, w_n) \in W_1 \times \cdots \times W_n$ tel que $v = w_1 + \cdots + w_n$.

Preuve. Montrons d'abord que si (i) est vraie, alors (ii) est vraie.
Puisque $V = W_1 + \cdots + W_n$, il est clair que pour tout $v \in V$ il existe un n-uplet $(w_1, \cdots, w_n) \in W_1 \times \cdots \times W_n$ tel que $v = w_1 + \cdots + w_n$. Il suffit de montrer que ce n-uplet est unique. Si on suppose que

$$v = w_1 + \cdots + w_n \qquad \text{et} \qquad v = w_1' + \cdots + w_n'$$

avec $w_1, w_1' \in W_1$, …, $w_n, w_n' \in W_n$, alors on peut soustraire les deux équations et en déduire que

$$0_V = \sum_{i=1}^{n} (w_i - w_i').$$

Or pour tout i, on a $w_i - w_i' \in W_i$ (car W_i est un sous-espace vectoriel). Par définition d'une somme directe on trouve alors

$$\forall i \in [[1,n]], w_i - w_i' = 0_V,$$

et donc $w_i = w_i'$ pour tout i. C'est l'unicité du n-uplet.

Maintenant, prouvons que si (ii) est vraie, alors (i) est vraie.
Puisque nous supposons l'existence d'un n-uplet $(w_1, \dots, w_n) \in W_1 \times \cdots \times W_n$ tel que $v = w_1 + \cdots + w_n$, on peut déjà dire que $W_1 + \cdots + W_n = V$.
Ensuite, comme $0_V = \underbrace{0_V + \cdots + 0_V}_{n}$, et qu'il y a unicité d'une telle décomposition, on voit que

$$0_V = w_1 + \cdots + w_n \Rightarrow w_1 = \cdots = w_n = 0_V.$$

□

Théorème 3.5. *On a une décomposition en somme directe de deux sous-espaces $V = W_1 \oplus W_2$ si et seulement si*

$$\begin{cases} V = W_1 + W_2 \\ W_1 \cap W_2 = \{0\}. \end{cases}$$

Preuve. Supposons $V = W_1 \oplus W_2$. Par définition il vient alors $V = W_1 + W_2$. Soit $x \in W_1 \cap W_2$. Il suffit de prouver que $x = 0_V$. Nous avons évidemment $0 = x + (-x)$. Or $x \in W_1$ et $-x \in W_2$ (puisque W_2 est un sous-espace vectoriel contenant x). Par définition d'une somme directe, on trouve alors $x = -x = 0$.
Réciproquement, supposons $V = W_1 + W_2$ et $W_1 \cap W_2 = \{0\}$. Il suffit de montrer que si $0 = w_1 + w_2$ avec $w_1 \in W_1$ et $w_2 \in W_2$, alors $w_1 = w_2 = 0$. Mais $0 = w_1 + w_2$ donne $-w_2 = w_1$. Donc $w_1 \in W_1$ et $w_1 = -w_2 \in W_2$, de sorte que $w_1 \in W_1 \cap W_2 = \{0\}$. D'où $w_1 = 0$ et ensuite $w_2 = 0$. □

Attention : Si le nombre de sous-espaces est $n \geqslant 3$, on ne peut plus dire que

$$\begin{cases} V = W_1 + \cdots + W_n \\ \forall i \neq j, W_i \cap W_j = \{0\} \end{cases}$$

implique $V = W_1 \oplus \cdots \oplus W_n$.

4 Applications linéaires

Définition. *Soient V, W deux espaces vectoriels sur un même corps commutatif K.*
Une application linéaire de V dans W *est une application $f : V \to W$ vérifiant :*
i) $\forall v, v' \in V$, $\quad f(v + v') = f(v) + f(v')$
ii) $\forall r \in K, \forall v \in V$, $\quad f(r \cdot v) = r \cdot f(v)$

Exemple. L'application $\mathbb{R}^2 \to \mathbb{R}^3 : (x, y) \mapsto (3x + 2y,\ x - y,\ y)$ est une application linéaire.

Remarques.
1. Si $f : V \to W$ est une application linéaire, on a $f(0_V) = 0_W$, comme on peut le voir par exemple en prenant $r = 0_K$ dans la condition ii).
2. Une application $f : V \to W$ est linéaire si et seulement si $f(rv + r'v') = rf(v) + r'f(v')$ pour tout couple de scalaires (r, r') de K et tout couple de vecteurs (v, v') de V.
3. L'application $f : V \to W$, définie par $f(v) = 0_W$ pour tout $v \in V$, est une application linéaire. On l'appelle **l'application nulle de V dans W**.

Théorème 3.6. *Soit K un corps commutatif, et m, n deux entiers naturels.*
Soit $f : K^m \to K^n$ une application.
f est linéaire $\Leftrightarrow$ il existe une famille de scalaires $(A_{(i,j)})$ indexée par $[\![1,n]\!] \times [\![1,m]\!]$ telle que

$$\forall (x_1, x_2, \ldots, x_m) \in K^m, \qquad f(x_1, x_2, \ldots, x_m) = \left(\sum_{i=1}^{m} A_{(1,i)} x_i, \sum_{i=1}^{m} A_{(2,i)} x_i, \sum_{i=1}^{m} A_{(3,i)} x_i, \ldots, \sum_{i=1}^{m} A_{(n,i)} x_i \right)$$

Preuve. L'implication $\Longleftarrow$ est simplement une vérification de la définition des applications linéaires.
Montrons maintenant l'implication $\Longrightarrow$. On suppose que f est linéaire. On considère les m vecteurs

$$\begin{array}{rcl} f(1,0,0,\ldots,0) & = & \left(A_{(1,1)}, A_{(2,1)}, A_{(3,1)}, \ldots, A_{(n,1)}\right) \\ f(0,1,0,\ldots,0) & = & \left(A_{(1,2)}, A_{(2,2)}, A_{(3,2)}, \ldots, A_{(n,2)}\right) \\ \vdots & & \vdots \\ f(\ldots,0,1,0,\ldots) & = & \left(A_{(1,j)}, A_{(2,j)}, A_{(3,j)}, \ldots, A_{(n,j)}\right) \\ \vdots & & \vdots \\ f(0,0,0,\ldots,1) & = & \left(A_{(1,m)}, A_{(2,m)}, A_{(3,m)}, \ldots, A_{(n,m)}\right) \end{array}$$

Il est sous-entendu que dans l'égalité du milieu, le chiffre 1 est en position numéro j.
Avec cette définition des scalaires $A_{(i,j)}$, on aura

$$\begin{array}{rcl} f(x_1, x_2, \ldots, x_m) & = & f\left(x_1 \cdot (1,0,0,\ldots,0) + x_2 \cdot (0,1,0,\ldots,0) + \cdots + x_m \cdot (0,0,\cdots,1)\right) \\ & = & x_1 \cdot f(1,0,0,\ldots,0) + x_2 \cdot f(0,1,0,\ldots,0) + \cdots + x_m \cdot f(0,0,\cdots,1) \\ & = & x_1 \cdot \left(A_{(1,1)}, A_{(2,1)}, A_{(3,1)}, \ldots, A_{(n,1)}\right) + x_2 \cdot \left(A_{(1,2)}, A_{(2,2)}, A_{(3,2)}, \ldots, A_{(n,2)}\right) + \cdots \\ & & \cdots + x_m \cdot \left(A_{(1,m)}, A_{(2,m)}, A_{(3,m)}, \ldots, A_{(n,m)}\right) \\ & = & \left(\sum_{i=1}^{m} A_{(1,i)} x_i, \sum_{i=1}^{m} A_{(2,i)} x_i, \sum_{i=1}^{m} A_{(3,i)} x_i, \ldots, \sum_{i=1}^{m} A_{(n,i)} x_i \right) \end{array}$$

□

Définition.
Un endomorphisme d'un espace vectoriel V *est une application linéaire de V dans V.*
Un isomorphisme d'un espace vectoriel V **vers un espace vectoriel** W *est une application linéaire bijective de V vers W.*
Un automorphisme d'un espace vectoriel V *est un endomorphisme bijectif de V.*

Exemples.
1. **L'application identité** de V dans V, définie par $\forall v \in V, f(v) = v$, est un endomorphisme de V. C'est même un automorphisme de V. On la note souvent id_V.
2. Plus généralement, si r est un scalaire, on appelle **homothétie de rapport** r **sur** V l'application $f : V \to V$ définie par $f(v) = rv$. L'homothétie de rapport r est un endomorphisme de V, et $f = r \cdot \mathrm{id}_V$.

Théorème 3.7. *Soient V, W, X des espaces vectoriels sur un corps commutatif K.*
1. La somme de deux applications linéaires de V vers W est une application linéaire de V vers W.
2. Si f est une application linéaire de V vers W, alors pour tout $\lambda \in K$, l'application $\lambda \cdot f$, définie par $(\lambda \cdot f)(v) = \lambda \cdot (f(v))$, est une application linéaire de V vers W.
3. Si $f : V \to W$ et $g : W \to X$ sont deux applications linéaires, alors $g \circ f$ est une application linéaire de V vers X.
4. Si $f : V \to W, f' : V \to W, g : W \to X$ sont des applications linéaires, et $\lambda, \lambda' \in K$, alors

$$g \circ (\lambda \cdot f + \lambda' \cdot f') = \lambda \cdot (g \circ f) + \lambda' \cdot (g \circ f')$$

5. Si $f : V \to W, g : W \to X, g' : W \to X$ sont des applications linéaires, et $\lambda, \lambda' \in K$, alors

$$(\lambda \cdot g + \lambda' \cdot g') \circ f = \lambda \cdot (g \circ f) + \lambda' \cdot (g' \circ f)$$

6. La réciproque d'un isomorphisme linéaire $f : V \to W$ est un isomorphisme linéaire de W vers V.

Preuve. 1. Soient f, f' deux applications linéaires de V vers W. On a pour tout couple (v_1, v_2) de vecteurs de V et tout couple (r_1, r_2) de scalaires

$$\begin{aligned}(f+f')(r_1v_1+r_2v_2) &= f(r_1v_1+r_2v_2)+f'(r_1v_1+r_2v_2)\\ &= r_1f(v_1)+r_2f(v_2)+r_1f'(v_1)+r_2f'(v_2)\\ &= r_1f(v_1)+r_1f'(v_1)+r_2f(v_2)+r_2f'(v_2)\\ &= r_1(f+f')(v_1)+r_2(f+f')(v_2)\end{aligned}$$

2. Pour tout couple (v_1, v_2) de vecteurs de V et tout couple (r_1, r_2) de scalaires, on a

$$\begin{aligned}(\lambda\cdot f)(r_1v_1+r_2v_2) &= \lambda\cdot f(r_1v_1+r_2v_2)\\ &= \lambda\cdot(r_1f(v_1)+r_2f(v_2))\\ &= r_1((\lambda\cdot f)(v_1))+r_2((\lambda\cdot f)(v_2))\end{aligned}$$

3. Pour tout couple (v_1, v_2) de vecteurs de V et tout couple (r_1, r_2) de scalaires, on a

$$\begin{aligned}(g\circ f)(r_1v_1+r_2v_2) &= g(f(r_1v_1+r_2v_2))\\ &= g(r_1f(v_1)+r_2f(v_2))\\ &= r_1g(f(v_1))+r_2g(f(v_2))\\ &= r_1(g\circ f)(v_1)+r_2(g\circ f)(v_2)\end{aligned}$$

4. Pour tout vecteur v de V,

$$\begin{aligned}g\circ(\lambda\cdot f+\lambda'\cdot f')(v) &= g(\lambda f(v)+\lambda' f'(v))\\ &= \lambda g(f(v))+\lambda' g(f'(v))\\ &= (\lambda(g\circ f)+\lambda'(g\circ f'))(v)\end{aligned}$$

5. Cette égalité est toujours vraie, même si f, g, g' ne sont pas des applications linéaires.
6. Soit $f : V \to W$ un isomorphisme, et f^{-1} sa réciproque. On se donne deux vecteurs quelconques w_1, w_2 de W et deux scalaires r_1, r_2. Comme f est linéaire, on peut dire

$$f(r_1f^{-1}(w_1)+r_2f^{-1}(w_2)) = r_1f(f^{-1}(w_1))+r_2f(f^{-1}(w_2))$$

et on en déduit

$$\begin{aligned}f(r_1f^{-1}(w_1)+r_2f^{-1}(w_2)) &= r_1w_1+r_2w_2\\ r_1f^{-1}(w_1)+r_2f^{-1}(w_2) &= f^{-1}(r_1w_1+r_2w_2)\end{aligned}$$

Ceci montre que f^{-1} est linéaire. □

Notation. Soient V, W deux espaces vectoriels sur un même corps commutatif K.
On note $\mathcal{L}(V, W)$ l'ensemble de toutes les applications linéaires de V vers W.
On note $\mathcal{L}(V)$ l'ensemble de tous les endomorphismes de V.

Théorème 3.8. *Les ensembles $\mathcal{L}(V, W)$ et $\mathcal{L}(V)$, munis de l'addition interne des applications et de la multiplication externe par un scalaire, sont des espaces vectoriels sur K.*

Preuve. Nous savons que pour tout ensemble X, l'ensemble $\mathcal{F}(X, W)$ (avec les opérations usuelles) est un espace vectoriel sur K, car W est un espace vectoriel. En particulier, $\mathcal{F}(V, W)$ est un espace vectoriel.
Pour prouver que $\mathcal{L}(V, W)$ est un espace vectoriel, il suffit de montrer qu'il s'agit d'un sous-espace vectoriel de $\mathcal{F}(V, W)$.
Or on sait que :
1. L'application nulle est linéaire.
2. La somme de deux applications linéaires est encore linéaire.
3. Le produit d'une application linéaire par un scalaire quelconque est encore linéaire.
Ces trois observations font de $\mathcal{L}(V, W)$ un sous-espace vectoriel de $\mathcal{F}(V, W)$.

Pour $\mathcal{L}(V)$, il suffit d'observer que c'est $\mathcal{L}(V, V)$, et que le résultat qui le concerne n'est qu'un cas particulier de ce qui précède. □

5 Noyau et image d'une application linéaire

Définition. *Soit f une application linéaire d'un espace vectoriel V vers un espace vectoriel W.*
Le noyau de *f est l'ensemble $\{v \in V | f(v) = 0_W\}$. C'est un sous-ensemble de V qu'on note* $\ker f$.
L'image de *f est l'ensemble $\{f(v) | v \in V\}$. C'est un sous-ensemble de W qu'on note* $\mathrm{im} f$.

Théorème 3.9. *Soit $f : V \to W$ une application linéaire.*
1. Le noyau de f est un sous-espace vectoriel de V.
2. L'image de f est un sous-espace vectoriel de W.
3. Le noyau de f est $\{0\}$ si et seulement si f est injective.
4. L'image de f est W si et seulement si f est surjective.

Preuve. 1. $0 \in \ker f$, car $f(0) = 0$. En plus, si v, v' appartiennent au noyau, et que r, r' sont deux scalaires quelconques, alors

$$f(rv + r'v') = rf(v) + r'f(v') = 0,$$

ce qui montre que $rv + r'v'$ appartient également au noyau.

2. $0 \in \mathrm{im} f$, car $0 = f(0)$. Supposons que w, w' appartiennent à l'image de f. On peut écrire $w = f(v), w' = f(v')$, où v, v' sont des vecteurs de V. Prenons deux scalaires quelconques r, r'. Alors

$$rw + r'w' = rf(v) + r'f(v') = f(rv + r'v')$$

Puisque $rv + r'v' \in V$, on voit que $rw + r'w' \in \mathrm{im} f$.

3. Supposons f injective. Si $f(v) = 0$, alors $f(v) = f(0)$ et donc $v = 0$. Cela prouve que $\ker f = \{0\}$. Réciproquement supposons $\ker f = \{0\}$. Si $f(v) = f(v')$, alors par linéarité on trouve $f(v - v') = 0$ et donc $v - v' \in \ker f = \{0\}$, ce qui signifie $v = v'$. L'application f est injective.

4. est évident □

En mathématiques, on est souvent en présence d'équations du type $f(x) = w$, où $f : V \to W$ est une application linéaire. L'ensemble des vecteurs $x \in V$ qui vérifient cette équation est facile à décrire.

Théorème 3.10. *Soit $f : V \to W$ une application linéaire. Soit $w \in W$ un vecteur donné. On note*

$$S = \{x \in V | f(x) = w\}$$

Alors S est soit l'ensemble vide, soit un ensemble de la forme $\{x_0 + v | v \in \ker f\}$, où x_0 est une solution particulière de l'équation $f(x_0) = w$.

Preuve. On suppose que S est non vide, car sinon la preuve est finie. Puisque S est non vide, il existe $x_0 \in V$ tel que $f(x_0) = w$. On a alors

$$\begin{aligned}
& f(x) = w \\
\Leftrightarrow \quad & f(x) = f(x_0) \\
\Leftrightarrow \quad & f(x) - f(x_0) = 0 \\
\Leftrightarrow \quad & f(x - x_0) = 0 \\
\Leftrightarrow \quad & x - x_0 \in \ker f \\
\Leftrightarrow \quad & \exists v \in \ker f, x = x_0 + v
\end{aligned}$$

□

Exemple. Soit $f : \mathbb{R}^2 \to \mathbb{R}^3 : x = (a, b) \mapsto f(x) = (a + b, -a - b, 2a + 2b)$. L'application f est linéaire. On voit facilement que $\mathrm{im} f = \{(t, -t, 2t) \in \mathbb{R}^3 | t \in \mathbb{R}\}$. Si par exemple $w = (1, 2, 0)$, alors $w \notin \{(t, -t, 2t) \in \mathbb{R}^3 | t \in \mathbb{R}\}$ et l'équation $f(x) = (1, 2, 0)$ n'a pas de solution $x \in \mathbb{R}^2$. En revanche, si $w = (1, -1, 2)$, alors l'équation $f(x) = (1, -1, 2)$ possède des solutions. Comme $f(1, 0) = (1, -1, 2)$ et $\ker f = \{(a, -a) | a \in \mathbb{R}\}$, l'ensemble de toutes les solutions est

$$\{(1, 0) + (a, -a) | a \in \mathbb{R}\}.$$

6 Projecteurs

Définition. *Soit $V = W_1 \oplus \cdots \oplus W_n$ une décomposition de V en somme directe de n sous-espaces vectoriels de V. Soit $j \in [[1, n]]$.*
La projection (ou le projecteur) sur W_j par rapport à la décomposition $V = W_1 \oplus \cdots \oplus W_n$ *est l'application $p_j : V \to V$ définie par*

$$\forall v \in V, p(v) = w_j$$

où $v = \sum_{i=1}^{n} w_i$ est l'unique décomposition de v dans $W_1 + \cdots + W_n$.

Exemple. Soit $V = \mathbb{R}^2 = \{(x, 0)|x \in \mathbb{R}\} \oplus \{(0, y)|y \in \mathbb{R}\} = W_1 \oplus W_2$.
La projection sur W_1 par rapport à la décomposition $V = W_1 \oplus W_2$ est l'endomorphisme de $\mathbb{R}^2 : (x, y) \mapsto (x, 0)$.
La projection sur W_2 par rapport à la décomposition $V = W_1 \oplus W_2$ est l'endomorphisme de $\mathbb{R}^2 : (x, y) \mapsto (0, y)$.

Théorème 3.11. *Les projecteurs $p_1, p_2, \ldots, p_n$ sont des endomorphismes de V.*

Preuve. Fixons $j \in [[1, n]]$. Nous allons montrer que $p_j : V \to V$ est linéaire.
Soient x, x' deux vecteurs quelconques de V. On considère leurs décompositions uniques dans la somme directe $V = W_1 \oplus \cdots \oplus W_n$:

$$x = w_1 + \cdots + w_n, \qquad x' = w'_1 + \cdots + w'_n$$

Par somme on obtient alors

$$x + x' = (w_1 + w'_1) + \cdots + (w_n + w'_n)$$

Bien sûr, on peut dire que pour tout $i \in [[1, n]]$, on a $w_i + w'_i \in W_i$, de sorte que l'écriture ci-dessus est l'unique décomposition de $x + x'$. Donc

$$p_j(x + x') = w_j + w'_j = p_j(x) + p_j(x').$$

Soit $r \in K$ un scalaire. On trouve alors

$$r \cdot x = r \cdot w_1 + \cdots + r \cdot w_n$$

Pour tout $i \in [[1, n]]$, on a $r \cdot w_i \in W_i$, de sorte que l'écriture ci-dessus est l'unique décomposition de $r \cdot x$. Donc

$$p_j(r \cdot x) = r \cdot w_j = r \cdot p_j(x).$$

L'application p_j est bien linéaire. □

Les projecteurs $p_1, \ldots, p_n$ associés à la décomposition $V = W_1 \oplus \cdots \oplus W_n$ possèdent les propriétés suivantes :
(i) $p_1 + \cdots + p_n = \mathrm{id}_V$,
(ii) $\forall i, j \in [[1, n]], p_i \circ p_j = \begin{cases} p_i & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$.
L'image du projecteur p_j est le sous-espace vectoriel W_j de V .
Le noyau du projecteur p_j est le sous-espace vectoriel $W_1 + \cdots + W_{j-1} + W_{j+1} + \cdots + W_n$ de V.
On peut donc dire que $V = \ker p_j \oplus \mathrm{im}\, p_j$.

7 Familles libres/génératrices. Bases

Définition. *Soit V un espace vectoriel sur un corps commutatif K, et soit $(v_1, \ldots, v_n)$ une famille finie de vecteurs de V. On dit que cette famille de vecteurs est* **une famille libre de** *V si pour toute famille de scalaires $(\lambda_1, \ldots, \lambda_n)$ on a l'implication*

$$\sum_{i=1}^{n} \lambda_i \cdot v_i = 0_V \Rightarrow \forall i \in [[1, n]], \lambda_i = 0_K$$

Si $(v_i)_{i \in I}$ est une famille infinie de vecteurs de V, on dit que cette famille est **libre** *si toute sous-famille finie de $(v_i)_{i \in I}$ est libre. Une sous-famille finie de $(v_i)_{i \in I}$ est un famille de la forme $(v_j)_{j \in J}$, où J est un sous-ensemble fini de I.*

Exemples.
1. Dans $V = \mathbb{R}^2$, la famille de deux vecteurs $((1,0),(2,3))$ est une famille libre.
En effet, si $\lambda_1(1,0) + \lambda_2(2,3) = (0,0)$ on aura le système

$$\lambda_1 + 2\lambda_2 = 0, \qquad 3\lambda_2 = 0,$$

qui entraîne évidemment que $\lambda_1 = \lambda_2 = 0$. Cela montre bien que $((1,0),(2,3))$ est une famille libre de V.

En revanche, la famille $((1,0),(2,3),(3,2))$ n'est pas libre car on a (par exemple)

$$5 \cdot (1,0) + 2 \cdot (2,3) - 3 \cdot (3,2) = (0,0)$$

et la famille de scalaires $(5,2,-3)$ n'est pas la famille nulle.

2. Prenons $V = \mathcal{F}(\mathbb{R},\mathbb{R})$. C'est un espace vectoriel sur $\mathbb{R}$. Prenons la famille $(f_i)_{i\in\mathbb{Z}}$ indexée par $\mathbb{Z}$ ci-dessous : La fonction f_i est la fonction qui vaut 0 sur $\mathbb{R} - \{i\}$ et qui vaut 1 en i. Montrons que la famille $(f_i)_{i\in\mathbb{Z}}$ est une famille libre de V. Soit $J \subset \mathbb{Z}$ un sous-ensemble fini, et supposons que $(\lambda_j)_{j\in J}$ soit une famille de réels telle que

$$\sum_{j\in J} \lambda_j f_j = 0$$

Soit $n \in J$. On a alors en particulier

$$0 = \sum_{j\in J} \lambda_j f_j(n) = \lambda_n$$

Or n est un élément quelconque de J. Nous pouvons alors dire que pour tout entier $n \in J$, le réel λ_n vaut zéro. Cela signifie que la famille $(f_j)_{j\in J}$ est une famille libre de vecteurs de V. Par définition, la famille $(f_i)_{i\in\mathbb{Z}}$ est alors une famille libre.

Remarques.
1. Si (v_i) est une famille libre, alors toute famille obtenue en permutant les vecteurs est encore une famille libre.
2. Une famille qui contient le vecteur nul n'est jamais une famille libre.
3. Une famille qui contient plusieurs fois le même vecteur n'est jamais une famille libre.
4. Toute sous-famille d'une famille libre est encore une famille libre.

Vocabulaire. Lorsqu'une famille de vecteurs n'est pas libre, on dit qu'il s'agit d'**une famille liée**.

> **Définition.** *Soit V un espace vectoriel sur un corps commutatif K, et soit $(v_1,\dots,v_n)$ une famille finie de vecteurs de V. On dit que la famille de vecteurs $(v_1,\dots,v_n)$ est* **une famille génératrice de** *V si pour tout vecteur $x \in V$, il existe une famille de scalaires $(\lambda_1,\dots,\lambda_n)$ telle que*
>
> $$x = \sum_{i=1}^{n} \lambda_i \cdot v_i.$$
>
> *Si $(v_i)_{i\in I}$ est une famille infinie de vecteurs de V, on dit que la famille de vecteurs $(v_i)_{i\in I}$ est* **une famille génératrice de** *V si pour tout vecteur $x \in V$, il existe un sous-ensemble fini $J \subset I$ et une famille de scalaires $(\lambda_j)_{j\in J}$ telle que*
>
> $$x = \sum_{j\in J} \lambda_j \cdot v_j.$$

Une famille de vecteurs $(v_i)_{i\in I}$ est génératrice si et seulement si $\mathrm{Vect}(\{v_i | i \in I\}) = V$.

Remarques. 1. La famille formée de tous les vecteurs d'un espace vectoriel V est une famille génératrice de V.
2. Toute sur-famille d'une famille génératrice de V est encore une famille génératrice de V (une sur-famille d'une famille (v_i) est une famille dont (v_i) est une sous-famille).

Exemples. 1. Dans $V = \mathbb{R}^2$, la famille à deux vecteurs $((1,0),(1,1))$ est une famille génératrice, car tout vecteur $(x,y) \in V = \mathbb{R}^2$ peut s'écrire

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

2. En revanche, la famille à deux vecteurs $((1,0),(-1,0))$ n'est pas génératrice, car - par exemple - le vecteur $(0,1)$ ne peut pas s'écrire sous la forme $\lambda_1 \cdot (1,0) + \lambda_2 \cdot (-1,0)$.

Définition. *Soit V un espace vectoriel sur un corps commutatif K, et soit $(v_i)_{i\in I}$ une famille de vecteurs de V indexée par un ensemble I. On dit que la famille de vecteurs (v_i) est* **une base de** *V si la famille est à la fois libre et génératrice.*

Exemple fondamental. On considère l'espace vectoriel K^n sur le corps K (ici n est un entier naturel). Alors la famille à n vecteurs

$$((1,0,0,\dots,0),(0,1,0,\dots,0),(0,0,1,\dots,0),\dots,(0,0,0,\dots,1))$$

est une base de K^n. En effet, il est facile de voir que cette famille est libre et génératrice.
Cette base particulière est appelée **la base canonique de** K^n.

Théorème 3.12 et définition. *Soit V un espace vectoriel sur un corps commutatif K, et soit $(v_1,\dots,v_n)$ une famille de vecteurs de V. La famille $(v_1,\dots,v_n)$ est une base de V si et seulement si pour tout vecteur $x\in V$, il existe une famille unique de scalaires $(\lambda_1,\dots,\lambda_n)$ telle que*

$$x=\sum_{i\in I}\lambda_i\cdot v_i.$$

Lorsque $(v_1,\dots,v_n)$ est une base, on appelle l'unique famille $(\lambda_1,\dots,\lambda_n)\in K^n$ **les coordonnées du vecteur** *x* **par rapport à la base** *$(v_1,\dots,v_n)$.*

Preuve. Partie «si» : Il faut montrer que la famille est libre et génératrice. Il est clair que la famille est génératrice. Il reste à montrer qu'elle est libre. On suppose que

$$\sum_{i=1}^{n}\lambda_i\cdot v_i=0_V$$

Or il est évident que $\displaystyle\sum_{i=1}^{n}0_K\cdot v_i=0_V$. Par l'hypothèse d'unicité, on peut alors déduire que les familles $(\lambda_1,\dots,\lambda_n)$ et $(0_K,\dots,0_K)$ sont égales. En d'autres termes, $\forall i\in[[1,n]],\lambda_i=0_K$.

Partie «seulement si» : On suppose maintenant que la famille est libre et génératrice. Comme elle est génératrice, l'existence d'une famille de scalaires $(\lambda_1,\dots,\lambda_n)$ est évidente. Il reste à montrer l'unicité de cette famille.
Supposons que l'on ait, pour un vecteur $x\in V$ fixé :

$$x=\sum_{i=1}^{n}\lambda_i\cdot v_i=\sum_{i=1}^{n}\mu_i\cdot v_i$$

Alors on peut écrire par soustraction :

$$\sum_{i=1}^{n}(\lambda_i-\mu_i)\cdot v_i=0_V$$

Mais la famille (v_i) est par hypothèse une famille libre ; il faut alors que pour tout $i\in[[1,n]]$, on ait $\lambda_i-\mu_i=0$. D'où $\lambda_i=\mu_i$, et c'est fini. □

En particulier, si $V=K^n$ et $(v_1,\dots,v_n)$ est la base canonique de K^n, alors les coordonnées d'un vecteur quelconque $x=(x_1,\dots,x_n)\in K^n$ par rapport à la base canonique est la famille $(x_1,\dots,x_n)$. Attention : Ici v_1 est un vecteur (élément de K^n), mais x_1 est un scalaire (élément de K).

8 Dimension d'un espace vectoriel

Théorème 3.13.
1. Tout espace vectoriel possède une base.
2. Si un espace vectoriel V possède une base finie $(e_1, \dots, e_n)$, alors toutes les bases de V sont des familles finies de n vecteurs.

Preuve. Voir annexes.

Définition.
Si un espace vectoriel V admet une base finie, on dit que V est **de dimension finie**. *On appelle* **dimension de** V, *et on note* $\dim V$, *le nombre de vecteurs d'une base quelconque de V.*
Si on espace vectoriel n'a pas de base finie, on dit qu'il est **de dimension infinie**.

En effet, le théorème 3.13 montre que si un espace vectoriel V n'a pas de base finie, alors toute base (qui existe par la partie 1) est nécessairement infinie.

Exemple.
L'espace vectoriel K^n sur le corps est de dimension n, car la base canonique possède n vecteurs. Toutes les bases de K^n ont exactement n vecteurs.
L'espace vectoriel $\mathbb{C}$ sur le corps $\mathbb{R}$ est de dimension 2, car $(1, i)$ est une base de $\mathbb{C}$ sur le corps $K = \mathbb{R}$. En revanche, l'espace vectoriel $\mathbb{C}$ sur le corps $\mathbb{C}$ est de dimension 1.

Théorème 3.14.
1. Soit V un espace vectoriel, et $(v_i)_{i\in I}$ une famille libre de V. Alors il existe une base de V qui est une sur-famille de $(v_i)_{i\in I}$.
2. Soit V un espace vectoriel, et $(v_i)_{i\in I}$ une famille génératrice de V. Alors il existe une base de V qui est une sous-famille de $(v_i)_{i\in I}$.

Preuve. Voir annexes.

En particulier, un espace vectoriel est de dimension finie si et seulement s'il possède un famille génératrice finie.

Un espace vectoriel est de dimension infinie si et seulement s'il possède une famille libre infinie.

Exemples. L'espace vectoriel $\mathcal{F}(\mathbb{R}, \mathbb{R})$ sur $\mathbb{R}$ est de dimension infinie. En effet, dans la section 7, nous avons construit une famille infinie libre $(f_i)_{i\in\mathbb{Z}}$ de vecteurs de $\mathcal{F}(\mathbb{R}, \mathbb{R})$. De la même façon, l'espace vectoriel de toutes les suites réelles (sur le corps $\mathbb{R}$ des réels) est un espace vectoriel de dimension infinie.

Théorème 3.15.
1. Soit V de dimension finie, et $(v_1, \dots, v_p)$ une famille libre. Alors $p \leqslant \dim V$.
2. Soit V de dimension finie, et $(v_1, \dots, v_{\dim V})$ une famille libre.
Alors cette famille est une base de V.
3. Soit V de dimension finie, et $(v_1, \dots, v_q)$ une famille génératrice. Alors $q \geqslant \dim V$.
4. Soit V de dimension finie, et $(v_1, \dots, v_{\dim V})$ une famille génératrice.
Alors cette famille est une base de V.

Preuve. Pour 1 et 2, il suffit d'utiliser la première partie de 3.14. Pour 3 et 4, il suffit d'utiliser la deuxième partie de 3.14. □

Théorème 3.16.
Soit V un espace vectoriel de dimension finie, et $W \subset V$ un sous-espace vectoriel de V. Alors W est de dimension finie, et $\dim W \leqslant \dim V$. L'égalité a lieu si et seulement si $W = V$.

Preuve. On choisit une base b de W (elle existe). La famille b est évidemment une famille libre de V. On sait qu'il existe alors une base (forcément finie) de V dont b est une sous-famille. Donc b est une famille finie, et $\dim W \leqslant \dim V$.
Si $W = V$, il est évident que $\dim W = \dim V$. Réciproquement, si $\dim W = \dim V = n$, toute base $(e_1, \dots, e_n)$ de W est une famille libre de V ayant $\dim V$ vecteurs, donc cette base est aussi une base de V, et en particulier une famille génératrice de V. Pour tout $v \in V$, il existe alors des scalaires $(\lambda_1, \dots, \lambda_n)$ avec $v = \sum_{i=1}^{n} \lambda_i \cdot e_i$. Comme pour tout i, on a $e_i \in W$ et que W est un sous-espace, on trouve $v \in W$. D'où $V \subset W$. Comme $W \subset V$ par hypothèse, on trouve $W = V$. □

Théorème 3.17.
Soit V un espace vectoriel, et $W \subset V$ un sous-espace vectoriel de V. Alors il existe un sous-espace vectoriel supplémentaire à W dans V, c'est-à-dire un sous-espace W' tel que $W \oplus W' = V$.

Preuve. On choisit une base $b = (v_i)_{i\in I}$ de W (elle existe). La famille b est évidemment une famille libre de V. On sait qu'il existe alors un ensemble $J \supset I$ et une base $(v_j)_{j\in J}$ de V (théorème 3.14). Soit W' le sous-espace vectoriel engendré par l'ensemble $\{v_k | k \in J - I\}$. Prouvons que $W \oplus W' = V$. D'abord $W + W' = V$. En effet pour tout $x \in V$, il existe un sous-ensemble fini $L \subset J$ et une famille de scalaires $(\lambda_l)_{l\in L}$ avec

$$x = \sum_{l\in L} \lambda_l v_l = \sum_{l\in L\cap I} \lambda_l v_l + \sum_{l\in L\cap(J-I)} \lambda_l v_l.$$

Le premier terme est dans W, le second terme dans W'. Ensuite $W \cap W' = \{0\}$. En effet, si $x \in W \cap W'$, alors il existe deux sous-ensembles finis $M \subset I, N \subset J - I$ et des familles de scalaires $(\mu_m)_{m\in M}$, $(\nu_n)_{n\in N}$ telles que

$$x = \sum_{m\in M} \mu_m \cdot v_m = \sum_{n\in N} \nu_n v_n.$$

Par soustraction, on trouve

$$0_V = \sum_{m\in M} \mu_m \cdot v_m + \sum_{n\in N} (-\nu_n) v_n.$$

Le membre de droite est une somme finie sur l'ensemble $M \cup N \subset J$. Comme $M \cap N = \varnothing$, et que la famille $(v_j)_{j\in J}$ est libre, on en déduit que $\forall m \in M, \mu_m = 0$ et $\forall n \in N, \nu_n = 0$. Donc $x = 0$. □

En général W' n'est pas unique, parce qu'il existe de nombreuses façon de compléter la famille libre $(v_i)_{i\in I}$ en une base de V.

Théorème 3.18. *Soit V un espace vectoriel de dimension finie, et $W_1, \dots W_n$ des sous-espaces vectoriels de V tels que*

$$V = W_1 \oplus \cdots \oplus W_n.$$

Alors $\dim V = \dim W_1 + \cdots + \dim W_n$.

Preuve. Pour chaque $j \in [[1, n]]$, on choisit une base $(e_1^j, \dots, e_{\dim W_j}^j)$ de W_j. Prouvons que la famille

$$\left(e_1^1, \dots, e_{\dim W_1}^1, e_1^2, \dots, e_{\dim W_2}^2, \dots, e_1^n, \dots, e_{\dim W_n}^n\right)$$

est une base de V. Comme $V = W_1 + \ldots + W_n$, il est clair qu'elle est génératrice. Reste à montrer qu'elle est libre.
Supposons qu'on ait une famille de scalaires $\left(\lambda_1^1, \dots, \lambda_{\dim W_1}^1, \lambda_1^2, \dots, \lambda_{\dim W_2}^2, \dots, \lambda_1^n, \dots, \lambda_{\dim W_n}^n\right)$ telle que

$$0_V = \sum_{i_1=1}^{\dim W_1} \lambda_{i_1}^1 e_{i_1}^1 + \cdots + \sum_{i_n=1}^{\dim W_n} \lambda_{i_n}^n e_{i_n}^n.$$

Le membre de droite est une somme de n vecteurs, et pour tout $j \in [[1, n]]$, le j-ème terme appartient au sous-espace W_j. Par hypothèse, on a alors

$$\forall j \in [[1, n]], \sum_{i_j=1}^{\dim W_j} \lambda_{i_j}^j e_{i_j}^j = 0$$

Et comme $(e_1^j, \dots, e_{\dim W_j}^j)$ est une famille libre de W_j, on peut conclure que les $\lambda_{i_j}^j$ nuls pour tout $j \in [[1, n]]$ et tout $i_j \in [[1, \dim W_j]]$. La famille proposée est bien une base. Le nombre de vecteurs de cette base est égal à

$$\dim W_1 + \cdots + \dim W_n.$$

Ce nombre est alors la dimension de V. □

Théorème 3.19. *Soit V un espace vectoriel et W_1, W_2 des sous-espaces vectoriels de dimension finie de V. Alors $W_1 + W_2$ est de dimension finie, et on a la formule*

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

Preuve. Clairement $W_1 \cap W_2$ est un sous-espace de dimension finie de W_1. Il existe alors un supplémentaire E_1 de $W_1 \cap W_2$ dans W_1, de sorte que $W_1 = (W_1 \cap W_2) \oplus E_1$. De la même façon, il existe un sous-espace E_2 de W_2 tel que $W_2 = (W_1 \cap W_2) \oplus E_2$. Prouvons que

$$W_1 + W_2 = E_1 \oplus (W_1 \cap W_2) \oplus E_2.$$

Manifestement, $E_1, (W_1 \cap W_2), E_2$ sont des sous-espaces de $W_1 + W_2$. Il faut d'abord montrer que $W_1 + W_2 \subset E_1 + (W_1 \cap W_2) + E_2$. En effet, soit $w_1 + w_2 \in W_1 + W_2$. Comme $W_1 = E_1 + W_1 \cap W_2$, il existe $e_1 \in E_1$ et $i_1 \in W_1 \cap W_2$ avec $w_1 = e_1 + i_1$. De même, il existe $e_2 \in E_2$ et $i_2 \in W_1 \cap W_2$ avec $w_2 = e_2 + i_2$. Par addition, on trouve

$$w_1 + w_2 = e_1 + (i_1 + i_2) + e_2,$$

et comme $W_1 \cap W_2$ est un sous-espace, il vient $i_1 + i_2 \in W_1 \cap W_2$. Cela établit $W_1 + W_2 = E_1 \oplus (W_1 \cap W_2) \oplus E_2$.
Maintenant, prouvons que si $x_1 + i + x_2 = 0_V$ avec $x_1 \in E_1, i \in W_1 \cap W_2, x_2 \in E_2$, alors $x_1 = i = x_2 = 0_V$. En effet, on a d'abord $x_1 \in E_1 \subset W_1$. Ensuite $x_1 = -(i + x_2) \in W_2$. Donc $x_1 \in W_1 \cap W_2$. Mais on a aussi $x_1 \in E_1$; or $E_1 \cap (W_1 \cap W_2) = \{0\}$ (ces deux derniers sous-espaces sont supplémentaires dans W_1). Il en découle $x_1 = 0$. De la même façon, on prouve $x_2 = 0$. Il reste alors $0 + i + 0 = 0$ et on a également $i = 0$. Nous avons établi

$$W_1 + W_2 = E_1 \oplus (W_1 \cap W_2) \oplus E_2.$$

Par le théorème précédent, on trouve alors

$$\dim(W_1 + W_2) = \dim E_1 + \dim(W_1 \cap W_2) + \dim E_2$$

on sait aussi que $\dim W_1 = \dim(W_1 \cap W_2) + \dim E_1$ et $\dim W_2 = \dim(W_1 \cap W_2) + \dim E_2$. On arrive immédiatement à la conclusion que

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

□

Théorème 3.20. *1. Soit V un espace vectoriel de dimension finie n sur le corps commutatif K. Alors il existe un isomorphisme de K^n vers V.*

2. S'il existe un isomorphisme de K^n vers V, alors V est de dimension n.

3. Soient V et W deux espaces vectoriels isomorphes (il existe un isomorphisme de V vers W et un isomorphisme de W vers V). On suppose que l'un des deux espaces est de dimension finie. Alors V et W ont la même dimension.

4. Si V, W sont de dimension finie, et $\dim V = \dim W$, alors V et W sont isomorphes.

Preuve. 1. Soit $(e_1, \ldots, e_n)$ une base de V. On définit l'application $u : K^n \to V$ comme suit :

$$u(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \cdot e_i$$

Il est évident que u est une application linéaire. Comme (e_i) est une famille génératrice de V, il est également clair que u est surjective. Reste à montrer l'injectivité de u.

Par linéarité de u, il suffit de montrer que si $u(\lambda_1, \ldots, \lambda_n) = 0_V$, alors tous les λ_i sont nuls. Or cela est vrai, puisque la famille (e_i) est libre. Comme u est une application linéaire surjective et injective, il s'agit d'un isomorphisme d'espaces vectoriels.

2. Soit $u : K^n \to V$ un isomorphisme. On considère une base $(e_1, \dots, e_n)$ de K^n (par exemple la base canonique). On regarde maintenant la famille

$$(f_1, \dots, f_n) = (u(e_1), \dots, u(e_n))$$

Pour montrer que V est de dimension n, il suffit de se convaincre que la famille (f_i) est une base de V. Montrons d'abord qu'elle est libre.

Si $\sum_{i=1}^{n} \lambda_i \cdot f_i = \sum_{i=1}^{n} \lambda_i \cdot u(e_i) = 0_V$, alors par linéarité de u on aura

$$u\left(\sum_{i=1}^{n} \lambda_i \cdot e_i\right) = 0_V.$$

Or u est un isomorphisme, donc en particulier c'est une injection. Et comme $u(0) = 0$, on doit avoir

$$\sum_{i=1}^{n} \lambda_i \cdot e_i = 0$$

Mais la famille (e_i) est en particulier une famille libre, donc tous les λ_i sont nuls. Nous avons prouvé que la famille (f_i) est libre.

Montrons maintenant que la famille (f_i) est génératrice. Soit v vecteur quelconque de V. Puisque u est une surjection, il existe un vecteur $t \in K^n$ avec $u(t) = v$. Comme (e_i) est une famille génératrice de K^n, il existe des scalaires $(\lambda_1, \dots, \lambda_n)$ avec

$$t = \sum_{i=1}^{n} \lambda_i \cdot e_i$$

Mais alors

$$v = u(t) = u\left(\sum_{i=1}^{n} \lambda_i \cdot e_i\right) = \sum_{i=1}^{n} \lambda_i \cdot u(e_i) = \sum_{i=1}^{n} \lambda_i f_i$$

Nous avons montré que (f_i) est bien une famille génératrice. Cette famille est bien une base de V.

3. C'est une conséquence immédiate de 1. et 2.

4. Soit n la dimension commune de V et W. Par 1. les deux espaces vectoriels sont alors isomorphes à l'espace vectoriel K^n. Puisque la composée de deux isomorphismes est encore un isomorphisme, on en déduit que V et W sont isomorphes. □

9 Vocabulaire du chapitre

Un espace vectoriel	une homothétie
un vecteur	le noyau d'une application linéaire
un scalaire	l'image d'une application linéaire
un sous-espace vectoriel	un projecteur/une projection
engendré par	une famille libre
somme de sous-espaces	une famille liée
somme directe de sous-espaces	une famille génératrice
un supplémentaire	une base
une application linéaire	la base canonique de K^n
l'application nulle	les coordonnées d'un vecteur par rapport à une base
un endomorphisme	la dimension d'un espace vectoriel
un isomorphisme	un espace vectoriel de dimension finie
un automorphisme	un espace vectoriel de dimension infinie
l'identité	des espaces vectoriels isomorphes

10 Exercices

1. Démontrer le théorème : Les projecteurs $p_1, \dots, p_n$ associés à la décomposition $V = W_1 \oplus \cdots \oplus W_n$ possèdent les propriétés suivantes :

(i) $p_1 + \cdots + p_n = \mathrm{id}_V$,

(ii) $\forall i, j \in [[1, n]], p_i \circ p_j = \begin{cases} p_i & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$.

2. Soient n endomorphismes $f_1, \dots, f_n$ de V tels que

(i) $f_1 + \cdots + f_n = \mathrm{id}_V$,

(ii) $\forall i, j \in [[1, n]], f_i \circ f_j = \begin{cases} f_i & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$.

Montrer qu'il existe une décomposition en somme directe $V = \bigoplus_{i=1}^{n} W_i$ telle que pour tout j, le projecteur sur W_j par rapport à cette somme directe soit l'endomorphisme f_j.

3. Démontrer : Une famille de vecteurs $(v_i)_{i \in I}$ dans V est génératrice si et seulement si $\mathrm{Vect}(\{v_i | i \in I\}) = V$.

4. Soient f, g deux endomorphismes d'un espace vectoriel V.
Montrer que $\ker(f \circ g) \supset \ker g$, $\mathrm{im}\,(f \circ g) \subset \mathrm{im}\, f, \mathrm{im}\,(f + g) \subset \mathrm{im}\, f + \mathrm{im}\, g$.

5. Soit $(v_1, \dots, v_n)$ une famille de vecteurs de V. On définit l'application $\Phi : K^n \to V$ par

$$\Phi(\lambda_1, \dots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \cdot v_i.$$

Montrer que Φ est une application linéaire.
Trouver une condition nécessaire et suffisante pour que Φ soit injective.
Trouver une condition nécessaire et suffisante pour que Φ soit surjective.
Trouver une condition nécessaire et suffisante pour que Φ soit bijective. Dans ce cas, que dire de $\Phi^{-1}(v)$?

6. Soient W_1, W_2 deux sous-espaces vectoriels de V avec $W_1 \cap W_2 = \{0\}$. On suppose que $(v_1^1, v_2^1, \dots, v_p^1)$ est une famille libre de W_1 et que $(v_1^2, v_2^2, \dots, v_q^2)$ est une famille libre de W_2. Montrer que

$$(v_1^1, v_2^1, \dots, v_p^1, v_1^2, v_2^2, \dots, v_q^2)$$

est une famille libre de $W_1 + W_2$.

7. Donner un exemple d'un endomorphisme f de l'espace vectoriel $\mathbb{R}^2$ tel que $f \circ f = 0$ et $f \neq 0$.
En général, si $f : V \to V$ est un endomorphisme de V avec $f \circ f = 0$, que peut-on dire des sous-espaces $\ker f$ et $\mathrm{im}\, f$?

8. Soient f, g deux endomorphismes de K^1 (espace vectoriel sur K). Montrer que $f \circ g = g \circ f$.
Pour tout $n > 1$, trouver deux endomorphismes f, g de K^n tels que $f \circ g \neq g \circ f$.

9. Montrer que la famille vide est toujours libre. Montrer que la famille vide est une famille génératrice de l'espace vectoriel $\{0\}$.

10. Montrer : Un espace vectoriel est de dimension finie si et seulement s'il possède un famille génératrice finie. Un espace vectoriel est de dimension infinie si et seulement s'il possède une famille libre infinie.

11. a. Soit $f : V \to W$ une application linéaire injective. On suppose que $(v_1, \dots, v_m)$ est une famille libre de V. Que peut-on dire de $(f(v_1), \dots, f(v_m))$?
b. Soit $f : V \to W$ une application linéaire surjective. On suppose que $(v_1, \dots, v_m)$ est une famille génératrice de V. Que peut-on dire de $(f(v_1), \dots, f(v_m))$?

Annexes

Théorème 3.13.
1. Tout espace vectoriel possède une base.
2. Si un espace vectoriel V possède une base finie $(e_1, \ldots, e_n)$, alors toutes les bases de V sont des familles finies de n vecteurs.

Preuve. 1. Soit V un espace vectoriel sur K. On dira qu'un sous-ensemble $\mathcal{F} \subset V$ est libre si la famille $(v)_{v\in\mathcal{F}}$ est une famille libre de V. On note

$$\mathcal{L} = \{\mathcal{F} \subset V | \mathcal{F} \text{ libre}\}$$

l'ensemble de tous les sous-ensembles libres de V. Nous allons maintenant montrer que $\mathcal{L}$ est un ensemble inductif. Cela signifie ceci : Pour toute partie $\mathcal{K} \subset \mathcal{L}$ telle que

$$\forall \mathcal{F}_1, \mathcal{F}_2 \in \mathcal{K}, (\mathcal{F}_1 \subset \mathcal{F}_2 \text{ ou } \mathcal{F}_2 \subset \mathcal{F}_1),$$

il existe $\mathcal{M} \in \mathcal{L}$ avec : $\forall \mathcal{F} \in \mathcal{K}, \mathcal{F} \subset \mathcal{M}$.
Soit $\mathcal{K}$ un tel sous-ensemble de $\mathcal{L}$. Alors on peut former le sous-ensemble suivant de V :

$$\mathcal{M} = \bigcup_{\mathcal{F}\in\mathcal{K}} \mathcal{F}.$$

Il suffit de prouver que $\mathcal{M}$ est un sous-ensemble libre de V. Cela exige de prouver que tout sous-ensemble fini de $\mathcal{M}$ est un sous-ensemble libre. Soit $\{v_1, \ldots, v_n\} \subset \mathcal{M}$ un sous-ensemble fini de $\mathcal{M}$ (n est un entier variable, que l'on peut supposer non nul, car la famille vide est clairement libre). Il faut montrer que la famille $(v_1, \ldots, v_n)$ est libre. Pour tout $i \in [[1, n]]$, on a $v_i \in \mathcal{M} = \bigcup_{\mathcal{F}\in\mathcal{K}} \mathcal{F}$. Donc pour tout $i \in [[1, n]]$, il existe $\mathcal{F}_i \in \mathcal{K}$ tel que $v_i \in \mathcal{F}_i$. Considérons maintenant les n sous-ensembles $\mathcal{F}_1, \ldots, \mathcal{F}_n$ de V. On sait que pour deux quelconques d'entre eux, l'un des deux contient l'autre. Comme il y a seulement un nombre fini de tels sous-ensembles, on montre facilement (par récurrence sur le nombre de sous-ensembles) que

$$\exists j \in [[1, n]], \forall i \in [[1, n]], \mathcal{F}_i \subset \mathcal{F}_j.$$

En particulier, pour tout $i \in [[1, n]]$, on a $v_i \in \mathcal{F}_j$. Donc $\{v_1, \ldots, v_n\}$ est un sous-ensemble de $\mathcal{F}_j$, et $\mathcal{F}_j$ est libre. Or tout sous-ensemble d'un ensemble libre est encore libre. Donc $\{v_1, \ldots, v_n\}$ est libre. L'ensemble $\mathcal{L}$ est inductif.
Le lemme de Zorn (démontré ci-dessous) affirme que dans tout ensemble inductif $\mathcal{L}$, il existe un élément $\mathcal{B} \in \mathcal{L}$ **maximal**, ce qui signifie que

$$\forall \mathcal{B}' \in \mathcal{L}, (\mathcal{B} \subset \mathcal{B}' \Rightarrow \mathcal{B} = \mathcal{B}').$$

Comme $\mathcal{L}$ est inductif, il existe donc un tel élément $\mathcal{B} \in \mathcal{L}$. Ce $\mathcal{B}$ est un sous-ensemble libre de V, donc il définit une famille libre de V. Nous allons maintenant montrer que cette famille est également génératrice de V, ce qui prouvera l'existence d'une base. Soit $x \in V$ quelconque et montrons que x est engendré par $\mathcal{B}$. Si $x \in \mathcal{B}$ cela est évident. Supposons dorénavant $x \notin \mathcal{B}$. Alors l'ensemble $\{x\} \cup \mathcal{B}$ ne peut pas appartenir à $\mathcal{L}$, car cela contredirait le fait que $\mathcal{B}$ est maximal. Donc $\{x\} \cup \mathcal{B}$ définit une famille liée. Il existe alors un sous-ensemble fini $J \subset \{x\} \cup \mathcal{B}$ tel que la famille finie $(j)_{j\in J}$ est liée. Comme il est impossible que $J \subset \mathcal{B}$ (toute sous-famille d'une famille libre est libre !), il faut que $x \in J$. Il existe donc une famille non nulle de scalaires $(\lambda_j)_{j\in J}$ avec

$$\sum_{j\in J} \lambda_j \cdot j = 0_V.$$

Il est impossible que $\lambda_x = 0$, car sinon l'ensemble $J - \{x\}$ ne serait pas libre. D'où $\lambda_x \neq 0_K$ et l'égalité ci-dessus s'écrit alors

$$\lambda_x \cdot x = -\sum_{j\in J-\{x\}} \lambda_j \cdot j$$

ou encore

$$x = \sum_{j\in J-\{x\}} -\frac{\lambda_j}{\lambda_x} \cdot j$$

Comme $J - \{x\} \subset \mathcal{B}$, cela montre que x est bien engendré par $\mathcal{B}$. □

2. Pour démontrer la seconde partie, supposons par l'absurde qu'il existe une base finie $(e_1, \dots, e_n)$ de V et une autre base n'ayant pas n vecteurs (éventuellement un nombre infini de vecteurs). Comme toute base est à la fois libre et génératrice, il existe alors une famille libre finie de V et une famille génératrice finie de V telle que la famille libre possède strictement plus de vecteurs que la famille génératrice. Nous allons prouver que ceci nous amène une contradiction. En effet, soit $(x_1, \dots, x_p)$ une famille libre de V et $(y_1, \dots, y_q)$ une famille génératrice de V (avec $p > q$).
Nous démontrons ceci : S'il existe $k \in [[0, p-1]]$ et des vecteurs $z_1, \dots, z_{q-k}$ de V tels que

$$(x_1, \dots, x_k, z_1, \dots, z_{q-k})$$

soit génératrice, alors il existe des vecteurs $Z_1, \dots, Z_{q-k-1}$ tels que

$$(x_1, \dots, x_{k+1}, Z_1, \dots, Z_{q-k-1})$$

soit également génératrice.
En effet, il existe des scalaires $(\lambda_1, \dots, \lambda_k, \mu_1, \dots, \mu_{q-k})$ avec

$$x_{k+1} = \sum_{i=1}^{k} \lambda_i x_i + \sum_{j=1}^{q-k} \mu_j z_j.$$

puisque la famille $(x_1, \dots, x_k, z_1, \dots, z_{q-k})$ est génératrice. Il existe $\alpha \in [[1, q-k]]$ avec $\mu_\alpha \neq 0$, car sinon on pourrait écrire x_{k+1} comme une combinaison linéaire de $(x_1, \dots, x_k)$ ce qui est contredit par le fait que la famille $(x_1, \dots, x_p)$ est libre. On peut extraire le vecteur z_α de l'égalité ci-dessus :

$$z_\alpha = \frac{1}{\mu_\alpha} x_{k+1} - \sum_{i=1}^{k} \frac{\lambda_i}{\mu_\alpha} x_i - \sum_{j \in [[1, q-k]] - \{\alpha\}} \frac{\mu_j}{\mu_\alpha} z_j.$$

Le vecteur z_α étant engendré par la famille $(x_1, \dots, x_{k+1}, z_1, \dots, z_{\alpha-1}, z_{\alpha+1}, \dots, z_{q-k})$, et la famille $(x_1, \dots, x_k, z_1, \dots, z_{q-k})$ étant génératrice, on a prouvé que

$$(x_1, \dots, x_{k+1}, z_1, \dots, z_{\alpha-1}, z_{\alpha+1}, \dots, z_{q-k})$$

est bien une famille génératrice de V. Si nous introduisons la famille $(Z_1, \dots, Z_{q-k-1}) =$
$= (z_1, \dots, z_{\alpha-1}, z_{\alpha+1}, \dots, z_{q-k})$, on a obtenu la famille génératrice $(x_1, \dots, x_{k+1}, Z_1, \dots, Z_{q-k-1})$. Notre résultat est démontré.
Or d'après l'hypothèse, on peut choisir $k = 0$ et $(z_1, \dots, z_q) = (y_1, \dots, y_q)$. En appliquant le résultat q fois d'affilée, on montre que la famille

$$(x_1, \dots, x_q)$$

est une famille génératrice de V. Mais alors le vecteur x_p est engendré par la famille $(x_1, \dots, x_q)$ et comme $p > q$, la famille $(x_1, \dots, x_p)$ est liée. Contradiction !

Théorème 3.14.
1. Soit V un espace vectoriel, et $(v_i)_{i \in I}$ une famille libre de V. Alors il existe une base de V qui est une sur-famille de $(v_i)_{i \in I}$.
2. Soit V un espace vectoriel, et $(v_i)_{i \in I}$ une famille génératrice de V. Alors il existe une base de V qui est une sous-famille de $(v_i)_{i \in I}$.

Preuve. On refait la partie 1. du 3.13. en changeant le définition de $\mathcal{L}$. On montre que cet ensemble est encore inductif.

Théorème (Lemme de Zorn). *Tout ensemble inductif possède un élément maximal.*

Preuve (d'après Daniel Suratteau). Nous rappelons qu'un ensemble inductif est un ensemble ordonné $\mathcal{L}$ tel que toute partie de $\mathcal{L}$ totalement ordonnée possède un majorant dans $\mathcal{L}$. Avec cette définition, il est clair qu'un ensemble inductif est non vide (le vide est une partie totalement ordonnée de $\mathcal{L}$, donc admet un majorant dans $\mathcal{L}$).

Nous commençons par montrer un résultat légèrement différent, qui impliquera le lemme de Zorn. Ce résultat affirme ceci :

Soit E un ensemble ordonné non vide, dans lequel toute partie non vide et totalement ordonnée admet une borne supérieure. Alors E possède un élément maximal.

A priori l'hypothèse est plus forte ici, car dans le lemme de Zorn, on suppose seulement que toute partie totalement ordonnée possède un majorant.

Soit $\leqslant$ la relation d'ordre sur E. Nous allons montrer la contraposée du résultat. On suppose donc que E ne possède aucun élément maximal, et nous en déduirons l'existence d'une partie non vide totalement ordonnée sans borne supérieure.

Pour tout $x \in E$, l'ensemble $M_x = \{z \in E | x < z\}$ est non vide, puisque E n'admet pas d'élément maximal. Or l'axiome du choix, admis comme un des principes de base de la logique mathématique, affirme que si E est un ensemble quelconque, il existe une application $\gamma : \mathcal{P}(E) - \{\varnothing\} \to E$ telle que pour tout partie non vide X de E, on ait $\gamma(X) \in X$. Si on choisit une telle application γ, on peut construire une fonction $f : E \to E$ définie par

$$\forall x \in E, f(x) = \gamma(M_x).$$

Cette fonction vérifie $\forall x \in E, f(x) > x$. Fixons maintenant $a \in E$ (en effet, E est non vide). On note $\mathcal{T}$ l'ensemble de toutes les parties X de E qui vérifient :

1) $a \in X$,

2) $f(X) \subset X$,

3) Pour toute partie non vide S de X, si S admet une borne supérieure s dans E, alors $s \in X$.

Nous posons $H = \{x \in E | a \leqslant x\}$ l'ensemble de tous les majorants de a dans E. Alors $a \in H$. De plus pour tout $x \in H$, on a $f(x) > x \geqslant a$, donc $f(x) \in H$. On a $f(H) \subset H$. Enfin, si S est une partie non vide de H admettant une borne supérieure s dans E, alors il existe $x_0 \in S$ avec $x_0 \leqslant s$, et comme $a \leqslant x_0$, on voit que $s \in H$. Cela prouve que $H \in \mathcal{T}$, et par conséquent $\mathcal{T}$ est non vide. On peut alors définir l'ensemble A comme étant l'intersection de tous les éléments de $\mathcal{T}$. Comme les propriétés définissant $\mathcal{T}$ sont stables par intersection, on voit que $A \in \mathcal{T}$. De plus, $A \subset H$. Comme $a \in A$, on voit alors que a est le plus petit élément de A.

Dans A, nous définissons maintenant deux sous-ensembles B et C.

$$B = \{y \in A | \forall x \in A, (x < y \Rightarrow f(x) \leqslant y)\},$$

$$C = \{z \in A | \forall y \in B, (z \leqslant y \text{ ou } f(y) \leqslant z)\}.$$

Notre stratégie est de démontrer que $A = B = C$. D'abord nous montrons que $C \in \mathcal{T}$.

Pour tout $y \in B$, on a $y \in A$, donc $y \in H$, ce qui donne $a \leqslant y$. Il vient alors $a \in C$.

Soit $z \in C$. Alors $z \in A$, donc $f(z) \in A$. Si y est un élément quelconque de B, il y a trois cas à distinguer : $z < y$, $z = y$, $f(y) \leqslant z$. Dans le premier cas, la définition de B donne $f(z) \leqslant y$; dans le deuxième cas, $f(z) = f(y)$; dans le troisième cas, $f(y) \leqslant z < f(z)$. Dans les trois cas on peut dire $f(z) \leqslant y$ ou $f(y) \leqslant f(z)$. Donc $f(z) \in C$.

Soit S une partie non vide de C admettant une borne supérieure s dans E. Comme S est aussi une partie non vide de A, et que $A \in \mathcal{T}$, on a $s \in A$. Soit y un élément de B. Pour tout $z \in S$, on a $z \in C$, donc $z \leqslant y$ ou $f(y) \leqslant z$. Distinguons deux cas : (a) Pour tout $z \in S$, on a $z \leqslant y$. Alors y majore S, donc $s \leqslant y$; (b) Il existe $z_0 \in S$ tel que $z_0 \leqslant y$ est faux. Par définition de C on trouve alors $f(y) \leqslant z_0$. Comme $z_0 \leqslant s$, il vient alors $f(y) \leqslant s$. On a prouvé que $s \in C$.

Nous avons établi que $C \in \mathcal{T}$. Donc $A \subset C$. Mais comme $C \subset A$, on trouve $A = C$. Prenons maintenant $x \in A$ et $y \in B$ quelconques. Alors $x \in C$, donc $x \leqslant y$ ou $f(y) \leqslant x$. Dans le deuxième cas, on en déduit $y \leqslant x$. Nous savons maintenant : $\forall x \in A, \forall y \in B, x \leqslant y$ ou $y \leqslant x$.

Nous démontrons maintenant que $B \in \mathcal{T}$.

Pour tout $x \in A$, la condition $x < a$ est fausse car a est le plus petit élément de A. Donc l'implication $x < a \Rightarrow f(x) \leqslant a$ est vraie, ce qui donne $a \in B$.

Soit $y \in B$. Alors $y \in A$, puis $f(y) \in A$. Soit x un élément quelconque de A tel que $x < f(y)$. Comme $x \in C$, on sait que $x \leqslant y$ ou $f(y) \leqslant x$. Mais comme $x < f(y)$, il faut alors $x \leqslant y$. Si $x = y$, on trouve $f(x) = f(y)$ et donc $f(x) \leqslant f(y)$. Si $x < y$, alors par $y \in B$, on a $f(x) \leqslant y$ et comme $y < f(y)$ on trouve encore une fois $f(x) \leqslant f(y)$. Ceci prouve $f(y) \in B$.

Soit S une partie non vide de B admettant une borne supérieure s dans E. Comme précédemment, on trouve $s \in A$. Soit x un élément quelconque de A tel que $x < s$. Alors x ne majore pas S, donc il existe $y_0 \in S$ avec $y_0 \leqslant x$ faux. Or $x \in A$ et $y_0 \in B$, donc il doit être vrai que $x \leqslant y_0$. Comme $x \neq y_0$, il vient même $x < y_0$. Par la définition de B, on obtient $f(x) \leqslant y_0$. De plus $y_0 \leqslant s$, donc $f(x) \leqslant s$. Nous avons prouvé $s \in B$.

Tout ceci prouve bien que $B \in \mathcal{T}$, et donc que $A \subset B$, ainsi que $A = B$. En particulier on peut dire que $\forall x, y \in A, x \leqslant y$ ou $y \leqslant x$. La partie A est alors totalement ordonnée (et non vide).

Supposons par l'absurde que A possède une borne supérieure s dans E. Alors on aurait $s \in A$, puis $f(s) \in A$ et donc $f(s) \leqslant s$, puisque s est un majorant de A. Mais on a aussi $s < f(s)$. Contradiction.

Nous avons construit la partie A non vide, totalement ordonnée, et dépourvue de borne supérieure. Notre résultat est démontré.

Maintenant il reste à déduire le lemme de Zorn de notre résultat.

Soit $(L, \leqslant)$ un ensemble inductif (donc non vide). Notons $\mathcal{U}$ l'ensemble des parties non vides de L totalement ordonnées par $\leqslant$. Nous ordonnons l'ensemble $\mathcal{U}$ par l'inclusion $\subset$.

Soit $\mathcal{G}$ une partie non vide de $\mathcal{U}$ totalement ordonnée par l'inclusion. Nous notons S la réunion des éléments de $\mathcal{G}$. Alors $S \subset L$, S est non vide, et si $x, y \in S$, alors il existe $X, Y \in \mathcal{G}$ avec $x \in X$ et $y \in Y$. Par hypothèse, $\mathcal{G}$ est totalement ordonnée par $\subset$, donc $X \subset Y$ ou $Y \subset X$. Nous pouvons alors dire que x et y appartiennent tous deux à l'un des ensembles X ou Y. Mais X et Y sont totalement ordonnés par $\leqslant$, d'où $x \leqslant y$ ou $y \leqslant x$. Par suite, $S \in \mathcal{U}$. Donc S est un majorant (pour $\subset$) de $\mathcal{G}$. Et comme S est la réunion de tous les éléments de $\mathcal{G}$, il vient que S est en fait la borne supérieure de $\mathcal{G}$.

En outre, $\mathcal{U}$ est non vide. En effet, choisissons $l \in L$. Alors $\{l\} \in \mathcal{U}$.

On peut alors appliquer notre résultat à l'ensemble ordonné non vide $(\mathcal{U}, \subset)$, qui a bien la propriété que toute partie non vide totalement ordonnée possède une borne supérieure. Il existe donc un élément $M \in \mathcal{U}$ maximal pour l'inclusion. Comme M est une partie totalement ordonnée de L pour $\leqslant$, et que L est un ensemble inductif, il existe un majorant m de M. Soit maintenant $x \in L$ avec $m \leqslant x$. Alors x majore M, et en considérant $N = M \cup \{x\}$ (encore totalement ordonné), on trouve $M = M \cup \{x\}$, et donc $x \in M$. Comme m majore M, on trouve alors $x \leqslant m$ et par anti-symétrie $m = x$. Ceci montre bien que m est un élément maximal de L. □

Travaux dirigés d'algèbre 1

Algèbre 1

Travaux dirigés n°1

Thème : Logique

Question 1.

Lesquelles de ces affirmations sont équivalentes ?

a) Tous les chats ne sont pas gris
b) Tout chat est d'une couleur autre que gris
c) L'inclusion $\{\text{chats}\} \subset \{\text{chats gris}\}$ est fausse
d) Pour tout chat x, $x \notin \{\text{chats gris}\}$
e) Un chat n'est jamais gris
f) Aucun chat n'est gris
g) Il existe un chat qui n'est pas gris
h) Il n'existe pas de chat gris
i) L'ensembles des chats non gris est non vide
j) «Être un chat» n'implique pas «être gris»

Question 2.

Soient P_1, P_2, P_3, P_4 des phrases mathématiques.

a) On suppose que la phrase

$$(P_1 \text{ ou } P_2 \text{ ou } P_3) \text{ et } (P_1 \Rightarrow P_4) \text{ et } (P_2 \Rightarrow P_4) \text{ et } (P_3 \Rightarrow P_4)$$

est vraie. Que peut-on en déduire ?

b) On suppose que la phrase

$$(P_1 \text{ ou } P_2 \text{ ou } P_3) \text{ et } (P_1 \Rightarrow P_4) \text{ et } (P_2 \Rightarrow P_4)$$

est vraie. Que peut-on en déduire ?

Question 3.

Lesquelles de ces écritures n'ont pas de sens ?

a) $\{x + y = 0\}$
b) $\{x \in \mathbb{R} | x^2 = x + 1\}$
c) $\{x \in \mathbb{R} | \forall y \in \mathbb{R}, x + y = 0\}$
d) $\exists x, x^2 + x + 1 = 0$
e) $\exists x \in \mathbb{C}, x^2 + x + 1 = 0$
f) $\forall x \in \mathbb{R}, \forall z \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \leqslant z$
g) $\{\forall x \in \mathbb{R} | x^2 = x + 1\}$
h) $\{x \in \mathbb{R} | \exists y \in \mathbb{R}, x + y = 0\}$
i) $\{x \in \mathbb{R} | x + y = 0\}$
j) $\exists x \in \mathbb{R}, x^2 + x + 1 = 0$
k) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \leqslant z, \forall z \in \mathbb{R}$
l) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (x^2 + y^2 = 1 \Rightarrow x = \cos\theta)$

Question 4.

Soient $u_0, u_1, u_2, \ldots$ une suite de nombres réels. On considère la phrase suivante

$$\forall \epsilon \in (0, +\infty), \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (n \geqslant N \Rightarrow |u_n| \leqslant \epsilon).$$

Le fait que cette phrase soit vraie ou fausse dépend-elle de ϵ ? de n ? de N ? de la suite $u_0, u_1, u_2, \ldots$?

Donner un exemple où cette phrase est vraie, et un exemple où cette phrase est fausse.

On définit $A_\epsilon = \{n \in \mathbb{N} | \, |u_n| \leqslant \epsilon\}$, $B_N = \{n \in \mathbb{N} | n \geqslant N\}$.
Traduire la phrase ci-dessus à l'aide des ensembles A_ϵ et B_N.

Si $\epsilon \leqslant \eta$, que peut-on dire des ensembles A_ϵ et A_η ?
Si $N_1 \leqslant N_2$, que peut-on dire des ensembles B_{N_1} et B_{N_2} ?

Que peut-on dire de la phrase : $\exists \epsilon \in (0, +\infty), \{N \in \mathbb{N} | B_N \subset A_\epsilon\} = \varnothing$?

Algèbre 1

Travaux dirigés n°2

Thème : Logique, Ensembles

Question 1.

Les propositions suivantes sont-elles vraies ou fausses ?

a) Pour qu'un réel soit strictement supérieur à 3, il suffit qu'il soit strictement supérieur à 4.

b) Pour qu'un réel soit strictement supérieur à 3, il faut qu'il soit différent de 2.

c) Une condition suffisante pour qu'un réel soit supérieur ou égal à 2, est qu'il soit supérieur ou égal à 3.

d) Pour qu'un réel soit strictement supérieur à 2, il suffit que son carré soit strictement supérieur à 4.

e) Une condition nécessaire et suffisante pour qu'un entier naturel soit strictement supérieur à 1 est qu'il soit supérieur ou égal à 2.

Question 2.

Écrire les négations des propositions suivantes :

a) $\forall x \in E,\ \forall x' \in E,\ x \neq x' \Rightarrow f(x) \neq f(x')$

b) $\forall \epsilon > 0,\ \exists \eta > 0,\ \forall x \in]a, b[,\ |x - x_0| < \eta \Rightarrow |f(x) - f(x_0)| < \epsilon$

c) $\forall a \in \mathbb{Z},\ \forall b \in \mathbb{N}^*,\ \exists q \in \mathbb{Z},\ \exists r \in \mathbb{Z},\ a = bq + r$ et $0 \leqslant r < b$.

Question 3.

Soient X, Y deux ensembles quelconques. Montrer par des contre-exemples que les affirmations

$$\begin{aligned}(X - Y) \cup Y &= X \\ (X \cup Y) - Y &= X\end{aligned}$$

sont toutes deux fausses. Pour chacune des phrases, trouver une condition nécessaire et suffisante pour qu'elle soit vraie.

Question 4.

Soient A, B, C trois sous-ensembles d'un ensemble Ω. Prouver

$$A\Delta(B\Delta C) = (A\Delta B)\Delta C$$

Si $x \in A\Delta(B\Delta C)$, que peut-on dire du cardinal de l'ensemble

$$\{U \in \{A, B, C\} | x \in U\} ?$$

Question 5.

Soient A, B deux sous-ensembles d'un ensemble Ω.

a) On suppose que pour tout $x \in \Omega$, au moins une des affirmations $x \in A \cap B$, $x \notin A \cup B$ est vraie. Montrer qu'exactement une des deux affirmations est vraie. Que peut-on dire de A et B ?

b) On suppose $A \subset B$ et $\forall x \in \Omega, x \in (\Omega - B) \cup A$. Que peut-on dire de A et B ?

c) A quelle condition peut-on trouver une injection de A dans $A \times B$?
A quelle condition peut-on trouver une surjection de $A \times B$ dans A ?

Algèbre 1

Travaux dirigés n°3

Thème : Ensembles

Question 1.

Soient E_1, E_2 deux ensembles finis quelconques. Prouver

$$|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2|.$$

En déduire la formule pour trois ensembles finis quelconques :

$$|E_1 \cup E_2 \cup E_3| = |E_1| + |E_2| + |E_3| - |E_1 \cap E_2| - |E_2 \cap E_3| - |E_3 \cap E_1| + |E_1 \cap E_2 \cap E_3|.$$

Montrer par récurrence sur le nombre d'ensembles la formule générale

$$|E_1 \cup \cdots \cup E_p| = \sum_{k=1}^{p} (-1)^{k-1} \sum_{\substack{L \subset [[1,p]] \\ |L| = k}} \left| \bigcap_{l \in L} E_l \right|.$$

Montrer que pour trois ensembles finis quelconques,

$$|E_1 \Delta E_2 \Delta E_3| = |E_1| + |E_2| + |E_3| - 2|E_1 \cap E_2| - 2|E_2 \cap E_3| - 2|E_3 \cap E_1| + 4|E_1 \cap E_2 \cap E_3|.$$

Question 2.

Soit $E = \{1, 2, \ldots, 100\}$.
Trouver une fonction $f : \mathcal{P}(E) \to E$ telle que pour tout $A \in \mathcal{P}(E) - \{\varnothing\}$, on ait $f(A) \in A$.
Pourquoi est-ce qu'une telle fonction est nécessairement une surjection ?

Question 3.

Soit E, F deux ensembles finis et $\varphi : E \to F$ une application. Pour tout $y \in F$, on note $a(y)$ le nombre d'antécédents de y par φ, autrement dit

$$a(y) = \text{Card}\{x \in E | \varphi(x) = y\}.$$

On suppose que $a(y)$ est une constante A (ne dépend pas du choix y).

1. Construire une bijection de E vers $F \times \{1, \ldots, A\}$.

2. En déduire que $|E| = |F| \cdot A$.

3. Dans une cave à vins, il y a 20 cartons, et dans chaque carton se trouvent 12 bouteilles de bon vin. Au total, il y a donc 240 bouteilles dans la cave. Montrer que ceci est une illustration de la formule démontrée sous 2. Préciser ce que sont les ensembles E, F et l'application φ.

Question 4.

Soit E un ensemble fini de cardinal n. Soit $p \in \mathbb{N}$. On appelle **arrangement de p éléments de** E tout p-uplet $(x_1, \ldots, x_p) \in E^p$ d'éléments deux à deux distincts de E (c'est-à-dire : si $i \neq j$ alors $x_i \neq x_j$). On note $\mathcal{A}(p, E)$ l'ensemble de tous les arrangements de p éléments de E.

1. Donner une formule pour le cardinal de $\mathcal{A}(p, E)$.

On appelle **combinaison de p éléments de** E tout sous-ensemble de E dont le cardinal vaut p. On note $\mathcal{C}(p, E)$ l'ensemble de toutes les combinaisons de p éléments de E.

2. Montrer que $|\mathcal{A}(p, E)| = |\mathcal{C}(p, E)| \cdot p!$. En déduire une formule pour le nombre de combinaisons de p éléments de E.

3. Pour la coupe du monde de football 2010, disputée par 32 équipes, 35961 personnes ont fait un pronostic sur le vainqueur, le finaliste, le 3ème et le 4ème. Montrer qu'il existe deux personnes différentes dont les pronostics citent les 4 mêmes équipes, à l'ordre près.

Algèbre 1

Travaux dirigés n°4

Thème : Groupes

Question 1.

Soit $(G, \cdot)$ un groupe.
1. Montrer que G est abélien si et seulement si l'application $G \to G : x \mapsto x^{-1}$ est un morphisme de groupe.

2. Soit $X \subset G$. On définit le centralisateur de X comme étant l'ensemble de tous les $g \in G$ avec

$$\forall x \in X, g \cdot x = x \cdot g.$$

Prouver que le centralisateur de X est un sous-groupe de G.

Que peut-on dire d'autre du centralisateur de X lorsqu'il est contenu dans X ?

Question 2 (théorème de Lagrange).

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G. Nous allons prouver le théorème de Lagrange :
Le cardinal de H est un diviseur du cardinal de G.

On appelle **classe latérale de** H tout sous-ensemble C de G tel que

$$\exists g \in G,\ C = \{g \cdot h | h \in H\}.$$

1. Montrer que toute classe latérale de H a le même cardinal que H.
2. Montrer que tout élément de G appartient à exactement une classe latérale de H.
3. En déduire le théorème de Lagrange.

Question 3.

On définit sur $\mathbb{R}_+^*$ une opération binaire interne par

$$\forall x, y \in \mathbb{R}_+^*, \qquad x * y = \frac{xy}{x+y}$$

1. Est-ce que $*$ est une opération associative ? commutative ?
2. Est-ce que $(\mathbb{R}_+^*, *)$ est un groupe ?

Question 4.

1. Trouver tous les morphismes de $(\mathbb{Q}, +)$ vers $(\mathbb{Q}, +)$.
2. Trouver tous les morphismes de $(\mathbb{Q}, +)$ vers $(\mathbb{Z}, +)$.
3. Trouver tous les sous-groupes de $(\mathbb{Z}, +)$.

Algèbre 1

Travaux dirigés n°5

Thème : Anneaux, Corps

Question 1.

Soit E un ensemble. On considère sur $\mathcal{P}(E)$ deux opérations internes, à savoir la différence symétrique Δ et l'intersection $\cap$.

Prouver que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

Quels sont les éléments inversibles de cet anneau ?

Question 2.

Soit p un nombre premier. On appelle **progression arithmétique de raison** p tout sous-ensemble X de $\mathbb{Z}$ tel qu'il existe $n \in \mathbb{Z}$ avec

$$X = \{n + pk | k \in \mathbb{Z}\} = n + p\mathbb{Z}.$$

1. Montrer que tout entier n appartient à exactement une progression arithmétique. On note cette progression arithmétique $[n]$. Montrer que $[n] = [n']$ si et seulement si p est un diviseur de $n - n'$.

2. Combien y a-t-il de progressions arithmétiques de raison p ?

3. On appelle $\mathbb{Z}/p\mathbb{Z}$ l'ensemble de toutes les progressions arithmétiques de raison p. On définit sur cet ensemble deux opérations internes, notées $+$ et $\cdot$, définies par

$$[n_1] + [n_2] = [n_1 + n_2], \qquad [n_1] \cdot [n_2] = [n_1 n_2].$$

Montrer : Si $[n_1] = [n_1']$ et $[n_2] = [n_2']$, alors $[n_1 + n_2] = [n_1' + n_2']$ et $[n_1 n_2] = [n_1' n_2']$.

4. Montrer que $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

5. Soit x un entier quelconque non divisible par p. On suppose que p divise $xy - xz$, où y, z sont deux entiers. Prouver que $[y] = [z]$.

6. Soit x un entier non divisible par p et $[x]$ la progression arithmétique contenant x. Montrer que l'application $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ définie par $\varphi([y]) = [x] \cdot [y]$ est une surjection.

7. En déduire que $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps. Que deviennent les réponses aux questions 1 à 6 lorsque p est un entier non premier ?

Question 3.

Soit A un anneau commutatif et $n \in \mathbb{N}^*$. On considère deux familles $(x_i)_{i \in [[1,n]]}$ et $(y_j)_{j \in [[1,n]]}$ d'éléments de A. On appelle C l'ensemble des couples $(i, j) \in [[1, n]] \times [[1, n]]$ tels que $i < j$. Démontrer l'identité de Lagrange :

$$\left(\sum_{i=1}^{n} x_i y_i\right)^2 + \sum_{(i,j) \in C} (x_i y_j - x_j y_i)^2 = \left(\sum_{i=1}^{n} x_i^2\right) \cdot \left(\sum_{i=1}^{n} y_i^2\right)$$

Dans le cas $n = 3$, donner une interprétation géométrique de cette identité.

Si $A = \mathbb{R}$, démontrer l'inégalité de Minkowski

$$\sqrt{\sum_{i=1}^{n} (x_i + y_i)^2} \leqslant \sqrt{\sum_{i=1}^{n} x_i^2} + \sqrt{\sum_{i=1}^{n} y_i^2}.$$

Toujours dans le cas $A = \mathbb{R}$, que peut-on dire si

$$\left(\sum_{i=1}^{n} x_i y_i\right)^2 = \left(\sum_{i=1}^{n} x_i^2\right) \cdot \left(\sum_{i=1}^{n} y_i^2\right) \quad ?$$

Algèbre 1

Travaux dirigés n°6

Thème : Espaces vectoriels

Question 1.

On considère l'espace vectoriel (sur le corps $\mathbb{R}$) $\mathcal{F}(\mathbb{R},\mathbb{R})$ de toutes les fonctions de $\mathbb{R}$ vers $\mathbb{R}$.
Lesquels des sous-ensembles suivants sont des sous-espaces vectoriels de $\mathcal{F}(\mathbb{R},\mathbb{R})$?

1. L'ensemble des fonctions continues.
2. L'ensemble des fonctions dérivables.
3. L'ensemble des fonctions paires.
4. L'ensemble des fonctions positives.
5. L'ensemble des fonctions polynomiales.
6. L'ensemble des fonctions périodiques.
7. L'ensemble des fonctions pour lesquelles 1 et 2 ont la même image.
8. L'ensemble des fonctions f telles que $\exists K \in \mathbb{R}, \forall x \geqslant K, f(x) = 0$.
9. L'ensemble des fonctions qui s'annulent une infinité de fois.
10. L'ensemble des fonctions majorées.
11. L'ensemble des fonctions bornées.
12. L'ensemble des fonctions f telles que $f(\mathbb{R}) \subset \mathbb{Z}$.

Question 2.

Soit V un espace vectoriel sur le corps K. On rappelle que $\langle X \rangle$ est l'espace vectoriel engendré par une partie X de V. Montrer :
1. Pour tout $X, X' \subset V$, on a $X \subset X' \Rightarrow \langle X \rangle \subset \langle X' \rangle$.
2. $\langle X \rangle = X$ si et seulement si X est un sous-espace vectoriel de V.
3. $\langle \langle X \rangle \rangle = \langle X \rangle$.
4. Si $v_1, \ldots, v_k$ sont des vecteurs de V, alors

$$\langle \{v_1, \ldots, v_k\} \rangle = \left\{ \sum_{i=1}^{k} \lambda_i v_i | \lambda_1, \ldots, \lambda_k \in K \right\}.$$

5. Pour $V = \mathbb{R}^3$ avec $K = \mathbb{R}$, trouver $\langle \{(x, y, 0) | x \in \mathbb{N}, y \in \mathbb{Q}\} \rangle$.

Question 3.

Soit E un espace vectoriel sur K, et W_1, W_2, W_3 trois sous-espaces vectoriels de E.

1. Si $W_1 \subset W_2$, que vaut $W_1 + W_2$?

2. Si $W_1 + W_2 = W_2$, que peut-on dire ?

3. Si $W_1 + W_3 = W_2 + W_3$, est-ce qu'on a nécessairement $W_1 = W_2$?

4. Si $W_1 + W_2 = E$, est-ce qu'on a : $\forall v \in E, v \in W_1$ ou $v \in W_2$?

5. Que vaut $\langle W_1 \cup W_2 \cup W_3 \rangle$?

6. Que vaut $\langle W_1 \cap W_2 \cap W_3 \rangle$?

7. Lesquelles des deux inclusions ci-dessous sont vraies ?

$$W_1 \cap (W_2 + W_3) \subset W_1 \cap W_2 + W_1 \cap W_3, \qquad W_1 \cap (W_2 + W_3) \supset W_1 \cap W_2 + W_1 \cap W_3$$

Algèbre 1

Travaux dirigés n°7

Thème : Espaces vectoriels

Question 1. Soit $\mathcal{D}(\mathbb{R},\mathbb{R})$ l'ensemble des fonctions dérivables de $\mathbb{R}$ vers $\mathbb{R}$.

1. Montrer que $\mathcal{D}(\mathbb{R},\mathbb{R})$ est un sous-espace vectoriel de $\mathcal{F}(\mathbb{R},\mathbb{R})$.

2. Montrer que l'application $u : \mathcal{D}(\mathbb{R},\mathbb{R}) \to \mathcal{F}(\mathbb{R},\mathbb{R}) : f \mapsto f'$ est une application linéaire.

3. Soit g une fonction dérivable de $\mathbb{R}$ dans $\mathbb{R}$. Prouver que l'application $v_g : \mathcal{D}(\mathbb{R},\mathbb{R}) \to \mathcal{F}(\mathbb{R},\mathbb{R}) : f \mapsto f \cdot g$ est une application linéaire, et que l'image de v_g est un sous-espace vectoriel de $\mathcal{D}(\mathbb{R},\mathbb{R})$.
A quelle condition a-t-on $\mathrm{Im}(v_g) = \mathcal{D}(\mathbb{R},\mathbb{R})$?

4. Trouver un sous-ensemble infini X de $\mathcal{D}(\mathbb{R},\mathbb{R})$ tel que

$$\forall f \in X, f \notin \langle X - \{f\}\rangle.$$

Question 2.

Soit V un espace vectoriel sur un corps commutuatif K.
Montrer que $(\mathcal{L}(V), +, \circ)$ est un anneau.
Décrire les inversibles de cet anneau.
Cet anneau est-il commutatif si $V = \mathbb{R}^2$ et $K = \mathbb{R}$?

Question 3.

a) On note E l'espace vectoriel sur $\mathbb{R}$ de toutes les suites réelles (u_n) qui convergent. Justifier que E est un espace vectoriel en le voyant comme sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$.
On note F l'ensemble des suites constantes réelles, et G l'ensemble des suites convergeant vers zéro.
Montrer que F et G sont des sous-espaces vectoriels de E, puis que $E = F \oplus G$.

b) On note E l'espace vectoriel sur $\mathbb{R}$ de toutes les fonctions dérivables $f : \mathbb{R} \to \mathbb{R}$. On note F l'ensemble de toutes les fonctions f telles que

$$\exists a, b \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) = ax + b.$$

On note G l'ensemble de toutes les fonctions dérivables f telles que $f(1) = f'(1) = 0$.
Montrer que F et G sont des sous-espaces vectoriels de E, puis que $E = F \oplus G$.

Question 4.

Soit V un espace vectoriel sur K et u un endomorphisme de V. Montrer les équivalences

$$\begin{array}{ccc} \ker u = \ker u^2 & \iff & \ker u \cap \mathrm{im}\, u = \{0\} \\ \mathrm{im}\, u = \mathrm{im}\, u^2 & \iff & \ker u + \mathrm{im}\, u = E. \end{array}$$

Si $\ker u \oplus \mathrm{im}\, u = E$, montrer que

$$\ker u = \ker u^2 = \ker u^3 = \cdots \qquad \text{et} \qquad \mathrm{im}\, u = \mathrm{im}\, u^2 = \mathrm{im}\, u^3 = \cdots$$

Ici $u^2 = u \circ u, u^3 = u \circ u \circ u$ et ainsi de suite.

Algèbre 1

Travaux dirigés n°8

Thème : Espaces vectoriels

Question 1.

Soient E, F deux espaces vectoriels sur un corps K.
On note $W_E = \{(x, 0_F) | x \in E\}$ et $W_F = \{(0_E, y) | y \in F\}$. Montrer que W_E, W_F sont des sous-espaces vectoriels de $E \times F$, que E est isomorphe à W_E et que F est isomorphe à W_F. Prouver enfin que $W_E \oplus W_F = E \times F$. En déduire la formule dimensionnelle

$$\dim(E \times F) = \dim E + \dim F$$

Question 2.

1. Soit $E = F \oplus G$ une décomposition en somme directe d'un espace vectoriel sur un corps commutatif K. Soit V un espace vectoriel sur K. Trouver un isomorphisme entre les espaces vectoriels

$$\mathcal{L}(E, V) \qquad \text{et} \qquad \mathcal{L}(F, V) \times \mathcal{L}(G, V).$$

2. Soit H un espace vectoriel de dimension 1 sur K. Trouver un isomorphisme entre V et $\mathcal{L}(H, V)$.

3. Si $(e_1, \ldots, e_m)$ est une base d'un espace vectoriel U (sur le corps K), montrer que

$$U = Ke_1 \oplus \cdots \oplus Ke_m.$$

Ici $Ke_j = \{\lambda e_j | \lambda \in K\}$.

4. Soient U, V deux espaces vectoriels de dimensions respectives m, n.
Trouver la dimension de l'espace vectoriel $\mathcal{L}(U, V)$.

Question 3.

Soit V un espace vectoriel sur K et $X \in \mathcal{P}(V)$.

1. Trouver tous les sous-espaces vectoriels W de V tels que $X \subset W$ et X est une partie génératrice de W.

2. On suppose que $X \in \mathcal{P}(V)$ possède la propriété suivante : Si $Y \subset X$ et $\langle Y \rangle = \langle X \rangle$, alors $X = Y$.
Démontrer que X est une partie libre de V.

Question 4.

Soit V un espace vectoriel de dimension finie sur un corps commutatif K, et $u \in \mathcal{L}(V)$.

Pour tout $n \in \mathbb{N}$, on définit $u^n = \underbrace{u \circ \cdots \circ u}_{n}$. Par convention, u^0 est l'identité sur V.

1. Prouver que la suite $(\dim \ker u^n)_{n \in \mathbb{N}}$ est croissante.

On fixe $n \geqslant 1$. On sait qu'il existe un sous-espace vectoriel S de $\ker u^{n+1}$ tel que

$$\ker u^{n+1} = \ker u^n \oplus S.$$

2. Pourquoi sait-on cela ?

3. Quelle est la dimension de S ?

4. Montrer que $u(S) \cap \ker u^{n-1} = \{0\}$.

5. En déduire que $\dim u(S) \leqslant \dim \ker u^n - \dim \ker u^{n-1}$.

6. Montrer que $u : S \to u(S)$ est une bijection.

7. En déduire que $\dim \ker u^{n+1} - \dim \ker u^n \leqslant \dim \ker u^n - \dim \ker u^{n-1}$.

8. Soit N le plus petit entier tel que $\dim \ker u^N = \dim \ker u^{N+1}$. Pourquoi N existe-t-il ?
Montrer que $N \leqslant \dim V$ et que $\forall n \geqslant N$, $\ker u^n = \ker u^{n+1}$.