Cours du Samedi 6 Décembre - Groupe avancé.

Introduction : Commençons par quelques rappels :
- Les ensembles couramment utilisés : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$.
- Produit cartésien de deux ensembles A et B : $A \times B = \{(x, y), x \in A, y \in B\}$.
- Intersection de deux ensembles A et B : $A \cap B = \{x, x \in A$ et $x \in B\}$.
- Réunion de deux ensembles A et B : $A \cup B = \{x, x \in A$ ou $x \in B\}$.
- Somme de deux ensembles A et B : $A + B = \{a + b, a \in A, b \in B\}$.

I) Groupes et espaces vectoriels.

1) Groupes.

Définition. Un groupe est la donnée d'un ensemble G et d'une loi de composition interne notée $*$ définie de la manière suivante :

$$\begin{array}{rccl} * : & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x * y \end{array}$$

et telle que $(G, *)$ vérifie les trois propriétés suivantes :
(1) (Elément neutre) Il existe e dans G tel que $\forall\, x \in G$, $e * x = x * e = x$.
(2) (Associativité) Pour tous x, y, $z \in G$, $(x * y) * z = x * (y * z) = x * y * z$.
(3) (Elément inverse) Pour tout x dans G, il existe x' dans G tel que : $x * x' = x' * x = e$. On pourra noter : $x' = x^{-1}$ à ne pas confondre avec la notation $\dfrac{1}{x}$.
Si de plus $\forall\, x$, $y \in G$, $x * y = y * x$, on dit que la loi $*$ est commutative et que $(G, *)$ est un groupe commutatif ou abélien.

Exemples : $(\mathbb{Z}, +)$ est un groupe abélien. En effet, la loi $+$ est bien une loi de composition interne de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$ (la somme de deux entiers relatifs est un entier relatif), $0 \in \mathbb{Z}$ est élément neutre pour la loi $+$, $+$ est associative et pour tout $x \in \mathbb{Z}$, il existe $y \in \mathbb{Z}$ tel que : $x + y = y + x = 0$: on prend $y = -x$. Enfin, la loi $+$ est commutative.

Par contre, $(\mathbb{N}, +)$ n'est pas un groupe. En effet, $2 \in \mathbb{N}$ mais 2 n'a pas d'inverse dans $\mathbb{N}$ muni de $+$ car $-2 \notin \mathbb{N}$.

Propriétés. Soit $(G, *)$ un groupe.
1) L'élément neutre de G est unique.
2) L'inverse y d'un élément x de G est unique.
3) L'inverse de l'inverse de x est x.
4) Pour tous x,$y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1}$.
5) Pour tous x, y, $z \in G$, si $x * y = x * z$ alors $y = z$.

Preuves.
1) Soient e et e' deux éléments neutres de G.
e' est élément neutre de G donc $e' * e = e * e' = e$ (c'est le point (1) de la définition pour $x = e$).
e est élément neutre de G donc $e * e' = e' * e = e'$. Ainsi, $e = e'$.
2) Soit $x \in G$ d'inverses : $y \in G$ et $z \in G$.
On a alors : $x * y = e$ ainsi $z * x * y = z * e = z$ de plus, $z * x = e$ donc $z * x * y = e * y = y$ ainsi $y = z$.
3) Soit $x \in G$.
On a : $(x^{-1})^{-1} * x^{-1} = e$ puisque $(x^{-1})^{-1}$ est l'inverse de x^{-1}.
De plus, $x * x^{-1} = e$ (car x est l'inverse de x^{-1}) donc par unicité de l'inverse (propriété 2), on a : $x = (x^{-1})^{-1}$.
4) Soient x, $y \in G$. On note : $x^{-1} \in G$ l'inverse de x et $y^{-1} \in G$ celui de y.
On a : $(x * y)^{-1} * (x * y) = e$ donc : $(x * y)^{-1} * (x * y) * y^{-1} = e * y^{-1} = y^{-1}$.
Par associativité de $*$, on a : $(x * y) * y^{-1} = x * (y * y^{-1}) = x * y * y^{-1} = x$. Dès lors, on obtient : $(x*y)^{-1} * (x*y) * y^{-1} = (x*y)^{-1} * x = y^{-1}$ ainsi, $(x*y)^{-1} * x * x^{-1} = y^{-1} * x^{-1}$ donc : $(x*y)^{-1} = y^{-1} * x^{-1}$.
5) Soient x, y, $z \in G$ tels que : $x * y = x * z$. On a alors : $x^{-1} * x * y = x^{-1} * x * z$ donc $y = z$.

2) Espaces vectoriels.

Dans ce qui suit on notera $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ ($\mathbb{K}$ est appelé : corps des scalaires). Dans les exemples, on ne parlera que d'espaces vectoriels sur $\mathbb{R}$.

Définition. On appelle $\mathbb{K}$-espace vectoriel (ou espace vectoriel sur $\mathbb{K}$) tout ensemble non vide E muni de deux lois : $+$ et $\times$ vérifiant :
1) $(E, +)$ est un groupe commutatif (i.e : $+$ est une loi de composition interne de $E \times E$ dans E, $+$ est associative, E possède un unique élément neutre, tout élément de E a un unique inverse et $+$ est commutative).
2) Pour tout $(\lambda, \mu) \in \mathbb{K}^2$, pour tout $x \in E$, $\lambda \times (\mu \times x) = (\lambda\mu) \times x$ et $1 \times x = x$.
3) $\times$ est distributive par rapport à $+$ dans E et dans $\mathbb{K}$.

Les éléments d'un $\mathbb{K}$-espace vectoriel sont appelés vecteurs et les éléments de $\mathbb{K}$ sont appelés scalaires.

Exemples.
1) Pour tout $n \in \mathbb{N}^*$, $\mathbb{R}^n$ est un $\mathbb{R}$-espace vectoriel.
2) $\mathbb{R}[X]$: l'ensemble des polynômes à coefficients réels est un $\mathbb{R}$-espace vectoriel.
3) Pour tout $n \in \mathbb{N}$, $\mathbb{R}_n[X]$ est l'ensemble des polynômes à coeffients réels et de degré inférieur ou égal à n. C'est un $\mathbb{R}$-espace vectoriel.

Remarque : $\mathbb{R}^n$ et $\mathbb{R}_n[X]$ sont des espaces vectoriels sur $\mathbb{R}$ de dimensions finies et $\mathbb{R}[X]$ est un $\mathbb{R}$-espace vectoriel de dimension infinie. On étudiera par la suite la notion de dimension d'un espace vectoriel.

En général, il est peu pratique de démontrer qu'un ensemble donné est un $\mathbb{K}$-espace vectoriel avec la définition, il est plus facile de montrer qu'un ensemble est un sous-espace vectoriel d'un espace vectoriel connu.

Définition. Soient E un $\mathbb{K}$-espace vectoriel et F un sous-ensemble de E. On dit que F est un sous-espace vectoriel de E (dorénavant abrégé : s.e.v) si F vérifie les conditions suivantes :
1) $0 \in F$.
2) $\forall\, x, y \in F$, $x + y \in F$ (F est stable par addition).
3) $\forall\, x \in F$, $\forall\, \lambda \in \mathbb{K}$, $\lambda x \in F$ (F est stable par la multiplication par un scalaire).

Remarques.
1) Tout s.e.v d'un $\mathbb{K}$-espace vectoriel est un $\mathbb{K}$-espace vectoriel.
2) Les points 2 et 3 de la définition peuvent être fusionnés en un seul : au lieu de montrer que F est stable par addition et par multiplication par un scalaire, on peut montrer que $\forall\, x, y \in F$, $\forall\, \lambda, \mu \in \mathbb{K}$, $\lambda x + \mu y \in F$, autrement dit : que F est stable par combinaisons linéaires.

Exercice 1.

On se place dans $E = \mathbb{R}^2$ (qui est un $\mathbb{R}$-espace vectoriel).
Soit $F = \{(x, y) \in \mathbb{R}^2 : x + y = 0\}$. Montrer que F est un sous-espace vectoriel de E.

Solution de l'exercice 1. On a bien sûr : $(0, 0) \in F$.
Soient $\lambda, \mu \in \mathbb{R}$, $u = (x, y)$ et $v = (x', y') \in F$.
On a : $\lambda u + \mu v = (\lambda x + \mu x', \lambda y + \mu y')$. Montrons que $\lambda u + \mu v \in F$ i.e : $\lambda x + \mu x' + \lambda y + \mu y' = 0$.
Comme, u et v appartiennent à F, on a : $x + y = 0$ et $x' + y' = 0$. On a alors : $\lambda x + \mu x' + \lambda y + \mu y' = \lambda(x + y) + \mu(x' + y') = 0$ donc $\lambda u + \mu v \in F$ donc F est un sous-espace vectoriel de E.

Exercice 2. On considère l'ensemble appelé E des polynômes à coefficients réels de degré inférieur ou égal à 3 tels que $P(1) = 0$.
Montrer que E est un sous-espace vectoriel de $\mathbb{R}_3[X]$. (On rappelle que $\mathbb{R}_3[X]$ est l'ensemble des polynômes à coefficients réels de degré inférieur ou égal à 3 et que c'est un $\mathbb{R}$-espace vectoriel).

Solution de l'exercice 2. Il est clair que le polynôme nul appartient à E et que $E \subset \mathbb{R}_3[X]$.
Soient λ, $\mu \in \mathbb{R}$, P, $Q \in E$. On a alors : $P(1) = Q(1) = 0$. Montrons que $\lambda P + \mu Q \in E$ i.e que : $(\lambda P + \mu Q)(1) = 0$. On a : $(\lambda P + \mu Q)(1) = \lambda P(1) + \mu Q(1) = 0$ donc $\lambda P + \mu Q \in E$ et E est un s.e.v de $\mathbb{R}_3[X]$.

Exercice 3. Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Montrer que $F \cup G$ est un sous-espace vectoriel de E si et seulement si $F \subset G$ ou $G \subset F$.

Solution de l'exercice 3. Si $F \subset G$ alors $F \cup G = G$ donc $F \cup G$ est un s.e.v de E. De même si $G \subset F$ alors $F \cup G = F$ donc $F \cup G$ est un s.e.v de E. On a donc prouvé une implication.
Réciproquement, supposons que $F \cup G$ est un s.e.v de E et raisonnons par l'absurde. Supposons alors que $F \not\subset G$ et $G \not\subset F$. Prenons x dans $F \setminus G$ et $y \in G \setminus F$. Alors $x + y \in F \cup G$ puisque $F \cup G$ est un s.e.v. Donc $x + y \in F$ ou $x + y \in G$. Si $x + y \in F$ alors $y = x + y - x \in F$ (car F est un s.e.v de E), ce qui n'est pas le cas. De même, si $x + y \in G$ alors $x = x + y - y \in G$ (car G est un s.e.v de E), ce qui est impossible. On obtient donc une contradiction et l'autre implication.

Propriété. Soit E un $\mathbb{K}$-espace vectoriel. Soient F et G deux s.e.v de E.
Alors, $F + G$ et $F \cap G$ sont des s.e.v de E.

Preuve.

1) Montrons que $F + G$ est un s.e.v de E.
Déjà, $(0,0) = (0,0) + (0,0)$ et $(0,0)$ appartient à F et à G donc il appartient à $F + G$.
Soient $\lambda, \mu \in \mathbb{K}$, $u, v \in F+G$. Montrons que $\lambda u + \mu v \in F+G$ i.e : que $\lambda u + \mu v$ peut s'écrire comme somme d'un élément de F et d'un élément de G. Comme u et v appartiennent à $F + G$, on en déduit qu'il existe $u_1, v_1 \in F$ et $u_2, v_2 \in G$ tels que : $u = u_1 + u_2$ et $v = v_1 + v_2$. Dès lors, $\lambda u + \mu v = \lambda(u_1 + u_2) + \mu(v_1 + v_2) = \lambda u_1 + \mu v_1 + \lambda u_2 + \mu v_2$. Comme u_1, $v_1 \in F$, λ, $\mu \in \mathbb{K}$ et F est un s.e.v de E, on a : $\lambda u_1 + \mu v_1 \in F$. De même, on montre que : $\lambda u_2 + \mu v_2 \in G$. Donc $\lambda u + \mu v$ s'écrit bien comme une somme d'un élément de F et d'un élément de G donc il appartient à $F + G$. Ainsi, $F + G$ est un s.e.v de E.
2) Montrons que $F \cap G$ est un s.e.v de E.
$0 \in F$ et $0 \in G$ donc $0 \in F \cap G$.
Soient λ, $\mu \in \mathbb{K}$, u, $v \in F \cap G$. Alors $u \in F$ et $v \in F$ donc $\lambda u + \mu v \in F$ car F est un s.e.v de E. De plus, $u \in G$ et $v \in G$, donc $\lambda u + \mu v \in G$ car G est un s.e.v de E. Ainsi, $\lambda u + \mu v \in F \cap G$. Donc $F \cap G$ est un s.e.v de E.

Définition : sous-espace vectoriel engendré par une famille de vecteurs. Soient E un $\mathbb{K}$-espace vectoriel et $e_1, ..., e_n$ n vecteurs de E. On note $Vect(e_1, ..., e_n)$ le s.e.v engendré par les vecteurs $e_1, ..., e_n$: c'est l'ensemble des combinaisons linéaires des e_i, $1 \leq i \leq n$. On peut écrire : $x \in Vect(e_1, ..., e_n) \Leftrightarrow x = \sum\limits_{i=1}^{n} \lambda_i e_i$, $\lambda_i \in \mathbb{K}, \forall\, i \in \{1, ..., n\}$.

Exemple. On considère : $E = \mathbb{R}^2$ et $F = \{(x, y) \in \mathbb{R}^2 : x - y = 0\}$.
On a : $F = \{(x, y) \in \mathbb{R}^2 : x = y\} = \{(x, x), x \in \mathbb{R}\} = \{x(1, 1), x \in \mathbb{R}\} = Vect\{(1, 1)\}$.
Tous les vecteurs de F sont alors des combinaisons linéaires du vecteur $(1, 1)$.

Exercice 4.
On note : $E = \mathbb{R}^3$.
On considère les ensembles F et G tels que : $F = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0, x + y = 0\}$ et $G = \{(x, y, z) \in \mathbb{R}^3 : x + 2y - 3z = 0\}$. Déterminer les vecteurs qui engendrent F et ceux qui engendrent G.

Solution de l'exercice 4. On a : $F = \{(x, y, z) \in \mathbb{R}^3 : z = 0, y = -x, x = x\} = \{(x, -x, 0), x \in \mathbb{R}\} = \{x(1, -1, 0), x \in \mathbb{R}\} = Vect\{(1, -1, 0)\}$.
Par ailleurs, $G = \{(x, y, z) \in \mathbb{R}^3 : x = -2y + 3z, y = y, z = z\} = \{(-2y + 3z, y, z), y, z \in \mathbb{R}\} = \{(-2y, y, 0) + (3z, 0, z), y, z \in \mathbb{R}\} = Vect\{(-2, 1, 0), (3, 0, 1)\}$.

II) Applications linéaires.

Définition. Soient E et F deux $\mathbb{K}$-espaces vectoriels.
On dit que $f : E \longrightarrow F$ est linéaire si :
1) $\forall\, x, y \in E$, $f(x+y) = f(x) + f(y)$.
2) $\forall\, x \in E$, $\forall\, \lambda \in \mathbb{K}$, $f(\lambda x) = \lambda f(x)$.
On note $\mathcal{L}(E, F)$, l'ensemble des applications linéaires de E dans F.

Remarque. Les points 1 et 2 de la définition peuvent être fusionnés en un seul : on dit que f est linéaire si : $\forall\, x$, $y \in E$, $\forall\, \lambda$, $\mu \in \mathbb{K}$, $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$.

Définitions. Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire.
1) On dit que f est surjective si $\forall\, y \in F$, $\exists\, x \in E$ tel que : $y = f(x)$.
2) On dit que f est injective si $\forall\, x, y \in E$, $f(x) = f(y) \Rightarrow x = y$.
3) On dit que f est bijective si f est injective et surjective.

Vocabulaire. Soit E un $\mathbb{K}$-espace vectoriel.
Une application linéaire de E dans lui-même est appelée : endomorphisme de E.
Une application linéaire bijective entre deux espaces vectoriels est un isomorphisme.
Un endomorphisme de E bijectif est un automorphisme de E.

Définition-propriété. Soit $f : E \longrightarrow F$ une application linéaire.
On appelle image de f le s.e.v de F : $\operatorname{Im} f = f(E) = \{f(x), x \in E\}$.

Preuve.

On a $f(0) = f(0+0) = f(0) + f(0)$ car f est linéaire donc $f(0) = 0$ donc $0 \in \operatorname{Im} f$.
Soient u, $v \in \operatorname{Im} f$. Alors, il existe x, $y \in E$ tels que : $f(x) = u$ et $f(y) = v$. Soient λ, $\mu \in \mathbb{K}$. On a : $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ (par linéarité de f) donc $f(\lambda x + \mu y) = \lambda u + \mu v$ et $\lambda x + \mu y \in E$ donc il existe $X = \lambda x + \mu y \in E$ tel que $f(X) = \lambda u + \mu v$ donc $\lambda u + \mu v \in \operatorname{Im} f$. Ainsi, $\operatorname{Im} f$ est un s.e.v de E.

Définition-propriété. Soit $f : E \longrightarrow F$ une application linéaire.
On appelle noyau de f le s.e.v de E : $\operatorname{Ker} f = f^{-1}(\{0\}) = \{x \in E : f(x) = 0\}$.

Preuve.

On a $f(0) = 0$ donc $0 \in \operatorname{Ker} f$. Soient x, $y \in \operatorname{Ker} f$, λ, $\mu \in \mathbb{K}$. On a alors $f(x) = f(y) = 0$. Et $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ (par linéarité de f) donc $f(\lambda x + \mu y) = 0$ ainsi, $\lambda x + \mu y \in \operatorname{Ker} f$. Par conséquent, $\operatorname{Ker} f$ est un s.e.v de E.

Propriété.
Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire.
1) f est injective si et seulement si $\operatorname{Ker} f = \{0\}$.
2) f est surjective si et seulement si $\operatorname{Im} f = F$.

Preuve.

1) Sens direct : suppons que f est injective et montrons que $\operatorname{Ker} f = \{0\}$. Soit $x \in \operatorname{Ker} f$ alors $f(x) = 0 = f(0)$ donc $x = 0$ par injectivité de f.
Réciproque : supposons que $\operatorname{Ker} f = \{0\}$ et montrons que f est injective. Soient x, $y \in E$ tels que : $f(x) = f(y) \Rightarrow f(x-y) = 0$ (par linéarité de f) ainsi, $x - y \in \operatorname{Ker} f$ mais comme $\operatorname{Ker} f = \{0\}$, on en déduit que $x - y = 0 \Rightarrow x = y$.
2) Sens direct : f est surjective donc $\forall\, y \in F$, $\exists x \in E$ tel que : $y = f(x)$ mais par la définition de l'image de f, on a directement : $y \in \operatorname{Im} f$. Donc $F \subset \operatorname{Im} f$ (et l'autre inclusion étant claire car $\operatorname{Im} f$ est un s.e.v de F), on en déduit que $\operatorname{Im} f = F$.
Réciproque : supposons que $\operatorname{Im} f = F$ alors par définition de l'image, $\forall\, y \in \operatorname{Im} f$, $\exists x \in E$ tel que : $y = f(x)$,

comme $\operatorname{Im} f = F$, on en déduit que $\forall\, y \in F$, $\exists x \in E$ tel que : $y = f(x)$. Donc f est surjective.

Exercice 5. On considère l'application suivante :

$$f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y) & \longmapsto & (x+y, 2x+2y) \end{array}$$

1) Montrer que f est un endomorphisme de $\mathbb{R}^2$.
2) Déterminer $\operatorname{Im} f$ et $\operatorname{Ker} f$.
3) L'application linéaire f est-elle injective ? Surjective ? Bijective ?

Solution de l'exercice 5.
1) Soient $\lambda, \mu \in \mathbb{R}$ et $u = (x,y)$, $v = (x', y') \in \mathbb{R}^2$.
On a : $f(\lambda u + \mu v) = f(\lambda x + \mu x', \lambda y + \mu y') = (\lambda x + \mu x' + \lambda y + \mu y', 2(\lambda x + \mu x') + 2(\lambda y + \mu y')) = (\lambda(x + y), \lambda(2x+2y)) + (\mu(x'+y'), \mu(2x'+2y')) = \lambda f(u) + \mu f(v)$ donc f est linéaire.
f est une application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^2$ donc f est un endomorphisme de $\mathbb{R}^2$.
2) Déterminons $\operatorname{Im} f$: soit $v = (a,b) \in \operatorname{Im} f \Rightarrow \exists u = (x,y) \in \mathbb{R}^2$, $v = f(u) \Rightarrow \begin{cases} x+y = a \\ 2x+2y = b \end{cases} \Rightarrow$ $\begin{cases} x+y = a \\ b = 2a \end{cases}$ ainsi, on obtient que : si $v = (a,b) \in \operatorname{Im} f$, alors $b = 2a$. Réciproquement, si (a,b) vérifie : $b = 2a$ alors $f(2a, -a) = (a,b)$ donc $(a,b) \in \operatorname{Im} f$. Ainsi, $\operatorname{Im} f = Vect\{(1,2)\}$.
Déterminons $\operatorname{Ker} f$: soit $u = (x,y) \in \operatorname{Ker} f \Leftrightarrow f(x,y) = 0 \Leftrightarrow \begin{cases} x+y = 0 \\ 2x+2y = 0 \end{cases} \Leftrightarrow \begin{cases} y = -x \\ x = x \end{cases}$.
En conclusion, on a : $\operatorname{Ker} f = Vect\{(1,-1)\}$.
3) On a : $\operatorname{Ker} f \neq \{0\}$ et $\operatorname{Im} f \neq \mathbb{R}^2$ donc f n'est ni injective, ni surjective, ni bijective.

III) Familles de vecteurs et dimension d'un espace vectoriel.

Définitions. Soit E un $\mathbb{K}$-espace vectoriel.
1) On dit qu'une famille $F = \{e_1, ..., e_n\}$ $(n \in \mathbb{N}^*)$ de vecteurs de E est une famille génératrice de E si tous les vecteurs de E peuvent s'écrire comme combinaisons linéaires des vecteurs de la famille F, i.e : $\forall\, x \in E$, $\exists(\lambda_1, ..., \lambda_n) \in \mathbb{K}^n$ tel que : $x = \lambda_1 e_1 + ... + \lambda_n e_n = \sum\limits_{i=1}^{n} \lambda_i e_i$.
2) On dit qu'une famille $F = \{e_1, ..., e_n\}$ $(n \in \mathbb{N}^*)$ de vecteurs de E est une famille libre si on a : $\forall\, \lambda_1, ..., \lambda_n \in \mathbb{K}$, $\lambda_1 e_1 + ... + \lambda_n e_n = 0 \Rightarrow \lambda_1 = \lambda_2 = ... = \lambda_n = 0$. On dit que les vecteurs $e_1, ..., e_n$ sont linéairement indépendants.
3) On dit qu'une famille $B = (e_1, ..., e_n)$ de vecteurs de E est une base de E si elle est libre et génératrice de E.
4) On dit que E est de dimension finie si E admet une famille génératrice finie.

Théorème de la base incomplète. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et non réduit à $\{0\}$. Soient $\{\ell_1, ..., \ell_p\}$ une famille libre de E et $\{g_1, ..., g_q\}$ une famille génératrice de E.
Alors il existe un entier $n \geq p$ et une base $(e_1, ..., e_n)$ de E tels que :
1) pour tout $i \leq p$, on a : $e_i = \ell_i$;
2) pour tout $i > p$, on a : $e_i \in \{g_1, ..., g_q\}$.

Démontrons le théorème de la base incomplète ! Pour ce faire, nous allons commencer par démontrer une propriété intermédiaire.

Propriété. Si $\{\ell_1, ..., \ell_p\}$ est une famille libre de E (E étant un $\mathbb{K}$-espace vectoriel) et si u est un vecteur de E alors u est combinaison linéaire de $\ell_1, ..., \ell_p$ si et seulement si la famille $\{\ell_1, ..., \ell_p, u\}$ est liée.

Démonstration. Le sens direct repose sur la définition d'une famille liée.
Réciproquement, supposons que la famille $\{\ell_1, ..., \ell_p, u\}$ est liée alors il existe $\lambda_1, ..., \lambda_{p+1} \in \mathbb{K}$ tels que : $\lambda_1 \ell_1 + ... + \lambda_p \ell_p + \lambda_{p+1} u = 0$ et l'un de ces coefficients au moins n'est pas nul. Si $\lambda_{p+1} = 0$ alors on obtient une combinaison linéaire de $\ell_1, ..., \ell_p$ nulle où au moins l'un des λ_i, $1 \leq i \leq p$ est non nul donc ceci contredit la

liberté de la famille $\{\ell_1, ..., \ell_p\}$. Donc $\lambda_{p+1} \neq 0$ et alors on peut écrire : $u = -\dfrac{\lambda_1}{\lambda_{p+1}}\ell_1 - ... - \dfrac{\lambda_p}{\lambda_{p+1}}\ell_p$ ainsi, u est combinaison linéaire de $\ell_1, ..., \ell_p$.

Démonstration du théorème de la base incomplète. Distinguons deux cas.
1er cas : On suppose que dans ce cas, tous les vecteurs de $\{g_1, ..., g_q\}$ sont combinaison linéaire des vecteurs de la famille $\{\ell_1, ..., \ell_p\}$. Si u est un vecteur quelconque de E alors il est combinaison linéaire des vecteurs $g_1, ..., g_q$ donc des vecteurs $\ell_1, ..., \ell_p$. Autrement dit : la famille $\{\ell_1, ..., \ell_p\}$ est génératrice de E. Comme cette dernière famille est libre, c'est une base de E et donc $n = p$.

2ème cas : on suppose qu'il existe un vecteur g_j de la famille $\{g_1, ..., g_q\}$ qui n'est pas combinaison linéaire des vecteurs $\ell_1, ..., \ell_p$ donc par la propriété précédente, la famille $\{\ell_1, ..., \ell_p, g_j\}$ est libre. Soit alors n le plus grand entier, nécessairement compris entre $p + 1$ et $p + q$, tel qu'il existe une famille libre $\{e_1, ..., e_n\}$ vérifiant :
1) pour tout $i \leq p$, $e_i = \ell_i$.
2) pour tout $i > p$, $e_i \in \{g_1, ..., g_q\}$.
Montrons alors que $\{e_1, ..., e_n\}$ est une base de E. Il suffit de montrer que cette famille est génératrice puisque par construction elle est libre. Par définition de n, en ajoutant n'importe quel vecteur de $\{g_1, ..., g_q\}$ à $\{e_1, ..., e_n\}$, on obtient une famille liée. Autrement dit, tout vecteur de $\{g_1, ..., g_q\}$ est combinaison linéaire des vecteurs $e_1, ..., e_n$. Puisque tout vecteur de E est combinaison linéaire des vecteurs de la famille $\{g_1, ..., g_q\}$ alors tout vecteur de E est aussi combinaison linéaire des vecteurs de la famille $\{e_1, ..., e_n\}$ donc la famille $\{e_1, ..., e_n\}$ est génératrice de E.

Corollaire. Tout espace vectoriel de dimension finie et non réduit à $\{0\}$ admet au moins une base.

Démonstration. Soit E un $\mathbb{K}$-espace vectoriel non réduit à $\{0\}$ et de dimension finie.
Comme $E \neq \{0\}$, il existe au moins un vecteur $\ell \in E$ tel que $\ell \neq 0$. Donc la famille $\{\ell\}$ est libre. De plus, E est de dimension finie donc il a une famille génératrice : $\{g_1, ..., g_q\}$ finie. L'existence d'une base de E est alors une conséquence du théorème de la base incomplète.

Remarque. Le théorème de la base incomplète affirme que l'on peut obtenir une base en ajoutant des éléments d'une famille génératrice à une famille libre. La base obtenue aura donc au moins autant d'éléments que la famille libre considérée. De cette remarque, découle la propriété ci-dessous :

Propriété (admise). Soit E un $\mathbb{K}$-espace vectoriel non réduit à $\{0\}$ et de dimension finie.
Soient $(e_1, ..., e_n)$ une base de E et $\{\ell_1, ..., \ell_p\}$ une famille libre de E. Alors $p \leq n$.

Théorème. Toutes les bases d'un $\mathbb{K}$-espace vectoriel de dimension finie et non réduit à $\{0\}$ ont le même nombre d'éléments.

Démonstration. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et non réduit à $\{0\}$.
Soient $B_1 = (e_1, ..., e_n)$ et $B_2 = (f_1, ..., f_p)$ deux bases de E. Montrons que $n = p$.
Puisqu'en particulier B_1 est une famille libre et B_2 est une base de E, on a : $n \leq p$ mais B_1 est une base de E et B_2 est une famille libre donc $p \leq n$. Ainsi, $n = p$.

Définition. Etant donné E : un $\mathbb{K}$-espace vectoriel de dimension finie, non réduit à $\{0\}$, le nombre d'éléments de chacune des bases de E est appelé : dimension de E. On note dim E la dimension de l'espace vectoriel E.
On a aussi : $\dim(\{0\}) = 0$.

Propriété. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$. Soit F un s.e.v de E.
Alors $\dim F \leq n$ et $\dim F = n$ si et seulement si $F = E$.

Preuve. Pour montrer que $\dim F \leq n$, supposons par l'absurde que $\dim F > n$. Alors, il existe $n + 1$ vecteurs libres appartenant à F. Comme F est un s.e.v de E, il existe alors $n + 1$ vecteurs linéairement indépendants dans E, ce qui contredit le fait que $\dim E = n$. Donc $\dim F \leq n$.
Si $F = E$ alors il est évident que $\dim F = \dim E = n$. Supposons maintenant que $\dim F = n$. Alors F admet

une base composée de n élements : $(f_1, ..., f_n)$. Comme F est un s.e.v de E, les vecteurs $f_1, ..., f_n$ appartiennent à E. Ainsi, E admet n vecteurs linéairement indépendants. De plus, comme $\dim E = n$, toutes les bases de E ont n éléments. Puisque la famille $\{f_1, ..., f_n\}$ est libre, on peut la compléter en une base de E qui doit avoir n éléments. La famille $\{f_1, ..., f_n\}$ ayant n éléments, on en déduit que c'est une base de E. Ainsi, toute base de F est une base de E donc $F = E$.

Exercice 6.
Soient $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ et $e_3 = (0, 0, 1)$ trois vecteurs de $\mathbb{R}^3$.
Montrer que les vecteurs e_1, e_2 et e_3 forment une base de $\mathbb{R}^3$.
Cette base est appelée : base canonique de $\mathbb{R}^3$.

Solution de l'exercice 6. Montrons que la famille $\{e_1, e_2, e_3\}$ est génératrice de $\mathbb{R}^3$ puis libre.
Soit $u = (x, y, z) \in \mathbb{R}^3$. On écrit : $u = xe_1 + ye_2 + ze_3$ donc tout vecteur de $\mathbb{R}^3$ s'écrit comme combinaison linéaire des vecteurs e_1, e_2 et e_3, ce qui prouve que la famille $\{e_1, e_2, e_3\}$ est génératrice de $\mathbb{R}^3$. Montrons maintenant que cette famille est libre : soit $\lambda e_1 + \mu e_2 + \gamma e_3 = (0, 0, 0)$, λ, μ, $\gamma \in \mathbb{R}$. On a immédiatement : $\lambda = \mu = \gamma = 0$ donc la famille $\{e_1, e_2, e_3\}$ est libre.
La famille $\{e_1, e_2, e_3\}$ est libre et génératrice de $\mathbb{R}^3$ donc c'est une base de $\mathbb{R}^3$.

Exercice 7.
Soit $F = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\}$ un s.e.v de $\mathbb{R}^3$. Déterminer une base de F puis la dimension de F.

Solution de l'exercice 7. On écrit : $F = \{(x, y, z) \in \mathbb{R}^3 : x = -y - z, y = y, z = z\} = \{(-y - z, y, z), y, z \in \mathbb{R}\} = \{(-y, y, 0) + (-z, 0, z), y, z \in \mathbb{R}\} = Vect\{(-1, 1, 0), (-1, 0, 1)\}$. Cette écriture nous permet de déduire que la famille $\{(-1, 1, 0), (-1, 0, 1)\}$ est génératrice de F. On remarque de plus que cette famille est libre. Ainsi, c'est une base de F. Comme elle comporte 2 éléments, on en déduit que F est de dimension 2 (il s'agit alors d'un plan vectoriel).

Théorème du rang (en dimension finie, admis). Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies et $f : E \longrightarrow F$ une application linéaire. Alors :

$$rgf + \dim \operatorname{Ker} f = \dim E$$

où rgf désigne le rang de f, i.e : la dimension de l'image de f.

Exercices supplémentaires.

Exercice 8.
Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies (supérieures ou égales à 1) et $f : E \longrightarrow F$ une application linéaire. Montrer que l'image d'une base de E est une famille génératrice de $\operatorname{Im} f$.

Solution de l'exercice 8.
Notons $n = \dim E$. Soit $B_E = (e_1, ..., e_n)$ une base de E. Montrons que : $\{f(e_1), ..., f(e_n\}$ est une famille génératrice de $\operatorname{Im} f$. Soit $y \in \operatorname{Im} f$ alors $\exists x \in E$ tel que : $y = f(x)$. Comme $x \in E$ et que B_E est une base de E, il existe un unique n-uplet de scalaires : $(\lambda_1, ..., \lambda_n) \in \mathbb{K}^n$ tel que : $x = \lambda_1 e_1 + ... + \lambda_n e_n = \sum_{i=1}^{n} \lambda_i e_i$. On a alors : $y = f(x) = \lambda_1 f(e_1) + ... + \lambda_n f(e_n)$ (par linéarité de f) i.e : $y = f(x) = \sum_{i=1}^{n} \lambda_i f(e_i)$. Ainsi, tout $y \in \operatorname{Im} f$ s'écrit comme combinaison linéaire des vecteurs : $f(e_1)$, $f(e_2)$, ..., $f(e_n)$ donc la famille $\{f(e_1), ..., f(e_n\}$ est une famille génératrice de $\operatorname{Im} f$.

Exercice 9. Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies respectives n et p (n, $p \geq 1$) et $f : E \longrightarrow F$ une application linéaire.
1) Dans cette question uniquement, on suppose que $n > p$. L'application linéaire f peut-elle être injective ?
2) Dans cette question uniquement, on suppose que $n < p$. L'application linéaire f peut-elle être surjective ?
3) On suppose enfin que $n = p$. L'application linéaire f peut-elle être bijective ?

<u>*Solution de l'exercice* 9.</u>
1) L'image de f est un s.e.v de F donc $\dim(\operatorname{Im} f) \leq \dim F \Rightarrow \dim(\operatorname{Im} f) \leq p$. Appliquons le théorème du rang : $\dim E = \dim(\operatorname{Im} f) + \dim(\operatorname{Ker} f) \Rightarrow \dim(\operatorname{Ker} f) \geq n - p > 0$ donc en particulier : $\dim(\operatorname{Ker} f) \neq 0$. Ainsi, $\operatorname{Ker} f \neq \{0\}$ donc f ne peut pas être injective.
2) Raisonnons par l'absurde. Supposons alors qu'il existe une telle application linéaire f surjective. Alors, on a d'après le théorème du rang : $n = p + \dim(\operatorname{Ker} f) \Rightarrow \dim(\operatorname{Ker} f) = n - p < 0$, c'est absurde ! Ainsi, il n'existe pas d'application linéaire surjective de E dans F lorsque $\dim E < \dim F$.
3) Oui, f peut être bijective si $n = p$. Par exemple : l'application linéaire $f : \mathbb{R}_1[X] \longrightarrow \mathbb{R}^2$ telle que : pour tout polynôme $P \in \mathbb{R}_1[X]$, $f(P) = (P(0), P(1))$ (on rappelle que $\mathbb{R}_1[X]$ est l'ensemble des polynômes à coefficients réels de degré inférieur ou égal à 1). On a : $\dim(\mathbb{R}_1[X]) = \dim(\mathbb{R}^2) = 2$ et f est bijective ! (Il suffit de montrer qu'elle est injective par exemple et on aura la surjectivité avec le théorème du rang !).

<u>Exercice 10.</u> Soient E, F et G trois $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications linéaires. Démontrer que $g \circ f = 0 \Leftrightarrow \operatorname{Im} f \subset \operatorname{Ker} g$.

<u>*Solution de l'exercice* 10.</u> Montrons d'abord le sens direct : supposons alors que $g \circ f = 0$.
Soit $y \in \operatorname{Im} f$ alors il existe $x \in E$ tel que $y = f(x)$. En appliquant g à cette égalité, on obtient : $g(y) = g(f(x)) = (g \circ f)(x) = 0$ (puisque $g \circ f = 0$). Ainsi, $y \in \operatorname{Ker} g$. D'où, $\operatorname{Im} f \subset \operatorname{Ker} g$.
Réciproquement, supposons que $\operatorname{Im} f \subset \operatorname{Ker} g$ et montrons que $g \circ f = 0$.
$\forall\, x \in E$, $(g \circ f)(x) = g(f(x))$. Comme $x \in E$, $f(x) \in \operatorname{Im} f$ mais alors $f(x) \in \operatorname{Ker} g$ car $\operatorname{Im} f \subset \operatorname{Ker} g$. Ainsi, $\forall\, x \in E$, $g(f(x)) = 0$. Par conséquent, $g \circ f = 0$.

<u>Exercice 11.</u> Soient E un $\mathbb{K}$-espace vectoriel et f un endomorphisme de E.
Montrer que $\operatorname{Ker}(f) = \operatorname{Ker}(f^2) \Leftrightarrow \operatorname{Im} f \cap \operatorname{Ker} f = \{0\}$.

<u>*Solution de l'exercice* 11.</u> Sens direct : supposons que $\operatorname{Ker}(f) = \operatorname{Ker}(f^2)$.
Soit $y \in \operatorname{Im} f \cap \operatorname{Ker} f \Rightarrow y \in \operatorname{Im} f$ et $y \in \operatorname{Ker} f$. Comme $y \in \operatorname{Im} f$, il existe $x \in E$ tel que : $y = f(x)$. Comme $y \in \operatorname{Ker} f$, $f(y) = 0$. Ainsi, on en déduit que $f(y) = f^2(x) = 0$. Donc $x \in \operatorname{Ker}(f^2)$. Or, $\operatorname{Ker}(f) = \operatorname{Ker}(f^2)$ donc $x \in \operatorname{Ker} f$ ainsi, $f(x) = 0$. Par conséquent, $y = 0$ et $\operatorname{Im} f \cap \operatorname{Ker} f = \{0\}$.
Réciproquement, supposons que $\operatorname{Im} f \cap \operatorname{Ker} f = \{0\}$. Montrons que $\operatorname{Ker}(f) = \operatorname{Ker}(f^2)$.
Pour la première inclusion, soit $x \in \operatorname{Ker}(f)$ alors $f(x) = 0 \Rightarrow f(f(x)) = f(0) = 0 \Rightarrow f^2(x) = 0$. Donc $x \in \operatorname{Ker}(f^2)$. Ainsi, $\operatorname{Ker}(f) \subset \operatorname{Ker}(f^2)$ (remarque : cette première inclusion est toujours vraie, pour n'importe quelle application linéaire !).
Pour la seconde inclusion, soit $y \in \operatorname{Ker}(f^2)$ alors $f^2(y) = 0 \Rightarrow f(f(y)) = 0$ donc $f(y) \in \operatorname{Ker} f$. De plus, $f(y) \in \operatorname{Im} f$ donc $f(y) \in \operatorname{Im} f \cap \operatorname{Ker} f$ mais $\operatorname{Im} f \cap \operatorname{Ker} f = \{0\}$ donc $f(y) = 0$ ainsi, $y \in \operatorname{Ker} f$. Par conséquent, $\operatorname{Ker}(f^2) \subset \operatorname{Ker} f$. Finalement, on a bien : $\operatorname{Ker}(f) = \operatorname{Ker}(f^2)$.