Mathématiques générales

4 décembre 2006

Table des matières

Onzième partie

Anneaux

1 Axiomes des anneaux

Définition (anneau) : Un anneau A est un ensemble muni de deux lois internes.
L'une additive, notée $+$, qui fait de A un groupe abélien.
L'autre multiplicative, notée $\times$ ou $\cdot$, qui vérifie :

A) $\forall x, y, z \in A,\ x(yz) = (xy)z$

N) $\exists e \in A,\ \forall x \in A,\ ex = xe = x$ De plus,

D$_d$) $\forall x, y, z \in A,\ (x + y)z = xz + yz$

D$_g$) $\forall x, y, z \in A,\ z(x + y) = xz + yz$
A est un anneau commutatif si

C) $\forall x, y \in A,\ xy = yx$
et dans ce cas, **D$_d$** est équivalent à **D$_g$**.

Conséquence :

1. La multiplication est distributive par rapport à la soustraction
2. L'élément nul est absorbant, i.e. $\forall a \in A,\ 0a = 0$
3. Si $A \neq \{0\}$, le neutre de la multiplication est différent de 0

Remarque : $A = \{0\}$ est un anneau.

Théorème de distributivité générale : Si $x_1, \ldots, x_n, y_1, \ldots, y_l$ sont des éléments de l'anneau A.

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{l} x_i y_j \right) = \left(\sum_{i=1}^{n} x_i \right) \left(\sum_{j=1}^{l} y_j \right)$$

Remarque : Soit $(A, +, \times)$ un anneau.
- $(A, +)$ est un groupe commutatif.
- $(A, \times)$ n'est pas un groupe si $A \neq \{0\}$.
- $(A\backslash\{0\}, \times)$ n'est, en général, pas un groupe et même pas forcément stable.

Définition (ensemble des éléments inversibles) : L'ensemble $\mathcal{U}_A$ des éléments inversibles de A :

$$\mathcal{U}_A = \{a \in A | \exists x \in A, \quad ax = xa = 1\}$$

est un groupe pour la loi $\times$.

2 Formule du binôme

Définition (commutatif) : Deux éléments a et b de A commutent si

$$ab = ba$$

On a alors :

$$(ab)^n = a^n b^n$$

Si a et b commutent, on a :

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

Formule du multinôme : Si $x_1, \ldots, x_r$ commutent, alors :

$$(x_1 + \cdots + x_r)^n = \sum_{\substack{(l_1,\ldots,l_r)\in\{0,\ldots,n\}^r \\ \sum l_i = n}} \frac{n!}{l_1! \cdots l_r!} x_1^{l_1} \cdots x_r^{l_r}$$

3 Sous-anneaux

Définition (sous-anneau) : Un sous-anneau B de l'anneau A est une partie de A contenant $\mathbf{1}_A$, qui est stable pour les lois $+$ et $\times$, et qui est un anneau pour les lois induites.

Théorème caractéristique : B est un sous-anneau de A si et seulement si :

1. $\mathbf{1}_A \in B$
2. Si $x, y \in B$, alors $x - y \in B$
3. Si $x, y \in B$, alors $xy \in B$

Propriété : Une intersection quelconque de sous-anneaux est un sous-anneau

Définition (sous-anneau engendré) : Soit A un anneau et B une partie de A. Notons

$$\mathcal{F} = \{C \text{ sous-anneau de } A | B \subset C\}$$

On appelle sous-anneau engendré par B :

$$[B] = \bigcap_{C \in \mathcal{F}} C$$

Remarque : Soit $x \in A$, alors le sous-anneau engendré par x est noté $[x]$.

4 Homomorphisme d'anneau

Définition (morphisme d'anneau) : Soient A et B deux anneaux. Un morphisme d'anneau de A vers B est une application f de A dans B telle que :

1. $f(\mathbf{1}_A) = \mathbf{1}_B$
2. $\forall x, y \in A, \quad f(x + y) = f(x) + f(y)$
3. $\forall x, y \in A, \quad f(xy) = f(x)f(y)$

Remarque :

- Si A' est un sous-anneau de A, alors $f(A')$ est un sous-anneau de B.
- Si B' est un sous-anneau de B, alors $f^{-1}(B')$ est un sous-anneau de A.
- Un morphisme d'anneau f définit un morphisme de groupe de $(A, +)$ dans $(B, +)$, et un autre de $(\mathcal{U}_A, \times)$ dans $(\mathcal{U}_B, \times)$.

5 Anneaux quotients, idéaux bilatères

Définition (idéal bilatère) : Un idéal bilatère I de l'anneau A est un sous-groupe de $(A, +)$ tel que :

$$\forall a \in A, \quad \forall x \in I, \qquad ax \in I \text{ et } xa \in I$$

Théorème : Les relations d'équivalences, compatibles avec la structure d'anneau de A, sont les relations de la forme :

$$x \mathcal{R} y \Leftrightarrow x - y \in I$$

Où I est un idéal bilatère de A.

Définition (anneau quotient) : Soit A un anneau et I un idéal bilatère de A.
L'ensemble quotient A/I peut être muni des lois :

$$\dot{x} + \dot{y} = \dot{\widehat{x + y}}$$

$$\dot{x}\dot{y} = \dot{\widehat{xy}}$$

$(A/I, +, \times)$ est alors un anneau appelé anneau quotient de A par l'idéal I.

Remarque : Attention à ne pas confondre sous-anneau et idéal.

Remarque : Si $\mathbf{1}_A \in I$, alors $I = A$.

Factorisation canonique : Soient A et B deux anneaux et f un morphisme de A dans B.
Ker f est un idéal bilatère de A.
$f = i \circ b \circ s$ avec :
$s : A \to A/\text{Ker } f$ la surjection canonique,
$b : A/\text{Ker } f \to \text{Im} f$ la bijection, et
$i : \text{Im} f \to B$ l'injection canonique.
i, s et b sont des morphismes d'anneaux.

6 Anneau intègre

Définition (diviseur de 0) : Soit A un anneau et $a \in A \backslash \{0\}$.

a est un diviseur de 0 à droite dans A si :

$$\exists b \in A\backslash\{0\}, \quad ba = 0$$

a est un diviseur de 0 à gauche dans A si :

$$\exists b \in A\backslash\{0\}, \quad ab = 0$$

Définition (anneau intègre) : Un anneau A est dit intègre s'il n'a pas de diviseur de 0,
ou encore :

$$\forall a, b \in A, \quad ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Définition (caractéristique d'un anneau) : Soit A un anneau et

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & A \\ & & n & \longmapsto & n\mathbf{1}_A \end{array}$$

un morphisme d'anneau.

1. Si Ker $\varphi = \{0\}$, alors on dit que l'anneau A est de caractéristique 0.
2. Sinon, $\exists a \in \mathbb{Z}$ tel que Ker $\varphi = a\mathbb{Z}$ et on dit alors que l'anneau est de caractéristique a.

7 Anneaux $\mathbb{Z}/n\mathbb{Z}$

Proposition : On a équivalence entre :

1. n est premier
2. $\mathbb{Z}/n\mathbb{Z}$ est intègre
3. $\mathbb{Z}/n\mathbb{Z}$ est un corps (voir plus loin)

Corollaire (petit théorème de Fermat) : Si $p \in \mathbb{Z}$ est premier, alors

$$\forall x \in \mathbb{Z}, \quad x^p \equiv x \ (p)$$

Douzième partie

Divisibilité dans un anneau

Dans tout ce chapitre, on travail dans un anneau commutatif A.

1 Le treillis des idéaux de A

Proposition Soit A un anneau commutatif. Une partie I de A est un idéal si et seulement si $I \neq \emptyset$et

$$\forall x, y \in I, \quad \forall \alpha, \beta \in A, \qquad \alpha x + \beta y \in I$$

Définition (idéal engendré) Soit S une partie de A. L'idéal engendre par S est le plus petit idéal de A contenant S. C'est l'intersection de tous les idéaux contenants S.

L'idéal engendré par S est l'ensemble des combinaisons linéaires finies d'éléments de S à coefficients dans A, i.e. l'ensemble des éléments de la forme :

$$\lambda_1 x_1 + \cdots + \lambda_n x_n, \quad \text{avec} : n \in \mathbb{N}^*,\ x_1, \ldots, x_n \in S \text{ et } \lambda_1, \ldots, \lambda_n \in A$$

On note cet idéal (S)

Si S est fini : $S = \{x_1, \ldots, x_r\}$
L'idéal engendré par S est l'ensemble des éléments de A de la forme :

$$\sum_{i=1}^{r} \lambda_i x_i, \text{ avec } \lambda_1, \ldots, \lambda_r \in A$$

Si S est réduit à un élément : $S = \{a\}$
L'idéal engendré par a est noté (a) et est appelé idéal principal. L'éléments a est un générateur de l'idéal (a).

Définition (treillis des idéaux) : Notons $\mathcal{I}$ l'ensemble des idéaux de A. C'est un treillis pour l'inclusion :
Si $I, J \in \mathcal{I}$, alors la paire (I, J) admet une borne inférieure :

$$I \cap J = \{x \in A | x \in I \text{ et } x \in J\}$$

et une borne supérieure :

$$I + J = \{i + j \ : \ i \in I \text{ et } j \in J\}$$

Théorème : Soit A un anneau commutatif et L un ensemble quelconque d'indices. Dans l'ensemble $\mathcal{I}$ des idéaux de A ordonné par l'inclusion, toute famille $\{I_l\}_{l\in L}$ admet

- une borne supérieure : $\sum_{l\in L} I_l$.
- une borne inférieure : $\bigcap_{i\in L} I_l$

2 Divisibilité et idéaux

Soit A un anneau commutatif.

Définition (divisibilité) : Soit $a, b \in A$. On dit que a divise b dans A, et on note $a|b$, s'il existe $q \in A$ tel que $b = qa$.

Définition (associativité) : Soit $a, b \in A$. On dit que a et b sont associés s'il existe $u \in \mathcal{U}_A$ tel que $a = bu$.

Remarque :

- La divisibilité est un pré-ordre.
- L'associativité est une relation d'équivalence car $\mathcal{U}_A$ est un groupe.
- a et b sont associés si et seulement si ils engendrent le même idéal, i.e. : $(a) = (b)$.
- La divisibilité est une relation d'ordre sur les classes d'éléments associés, ou encore sur les idéaux.
- Sur les idéaux, cet ordre correspond à l'inclusion inverse, i.e.

$$a|b \Leftrightarrow (a) \supset (b)$$

Définition (irréductible) : Notons $\mathcal{P}$ l'ensemble des idéaux principaux de A. Un élément a de $A\backslash\{0\}$ est dit irréductible si :

1. $(a) \neq A$
2. L'idéal (a) est maximal dans $\mathcal{P}\backslash A$

pgcd et ppcm Soit $\{a_l\}_{l\in L}$ une famille quelconque d'éléments de A.

Définition (pgcd) : La famille $\{a_l\}_{l\in L}$ admet un pgcd dans A si et seulement si la famille d'idéaux $\{(a_l)\}_{l\in L}$ admet une borne supérieure dans $\mathcal{P}$, notée (d). L'élément d est un pgcd des a_l, $l \in L$.

Définition (ppcm) : La famille $\{a_l\}_{l\in L}$ admet un ppcm dans A si et seulement si la famille d'idéaux $\{(a_l)\}_{l\in L}$ admet une borne inférieure dans $\mathcal{P}$, notée (m). L'élément m est un ppcm des a_l, $l \in L$.

Définition (anneau principal) : Un anneau commutatif intègre tel que tout idéal est principal est appelé anneau principal.

3 Anneaux euclidiens

Définition (anneau euclidien) Un anneaux intègre A est dit euclidien si il est muni d'une application ω de $A\backslash\{0\}$ dans $\mathbb{N}$ telle que :

1. $b|a \Rightarrow \omega(b) \leq \omega(a)$
2. $\forall(a,b) \in A\times(A\backslash\{0\}), \exists q,r \in A, \quad a = bq+r$ avec $r = 0$ ou $\omega(r) < \omega(b)$

Théorème : Dans un anneau euclidien, tout idéal est principal.

Définition (premier) : Un élément $p \in A$ est dit premier, irréductible ou extrémal si p n'est pas inversible et si ses seuls diviseurs sont ses associés et les inversibles.

Remarque : Si p est premier et $p|ab$, alors $p|a$ ou $p|b$.

On a équivalence entre :

1. p est premier
2. $A/(p)$ est intègre
3. $A/(p)$ est un corps

Théorème Soit A un anneau euclidien. Tout élément de $A\backslash\{0\}$ se décompose de manière essentiellement unique en produit de facteurs premiers.

Treizième partie

Corps

1 Définitions

Définition (corps) : Un corps est un anneau non réduit à $\{0\}$ tel que tout élément non nul est inversible, ou encore c'est un anneau K tel que $(K\backslash\{0\}, \times)$ est un groupe.

Un corps est dit commutatif si la multiplication est commutative.

Proposition : Tout anneau intègre fini est un corps.

Variante : Toute $\mathbb{K}$ algèbre intègre de dimension finie est un corps.

2 Sous-corps

Définition (sous-corps) : Soit K un corps. L est un sous-corps de K si c'est un sous-anneau de K et si ce sous-anneau est un corps.

Théorème caractéristique : L est un sous-corps de K si et seulement si :

1. $1_K \in L$
2. $\forall x, y \in L, \quad x - y \in L$
3. $\forall x, y \in L, \quad xy \in L$
4. $\forall x \in L\backslash\{0\}, \quad x^{-1} \in L$

3 Morphismes

Définition (morphisme de corps) : Soient K et L deux corps. Un morphisme de corps de K dans L est une application f de K dans L telle que :

1. $f(1_k) = 1_L$
2. $\forall x, y \in K, \quad f(x + y) = f(x) + f(y)$
3. $\forall x, y \in K, \quad f(xy) = f(x)x(y)$

Remarque : Les morphismes de corps sont toujours injectifs.

4 Corps des fractions d'un anneau intègre

Définition (corps des fractions) : Soit A un anneau commutatif intègre et L un corps contenant A. On définit le corps des fractions $(\mathcal{F}, +, \times)$ de A par :

1. $\mathcal{F} = A \times (A \backslash \{0\})/\mathcal{R}$ où $\mathcal{R}$ est une relation d'équivalence sur $A \times (A \backslash \{0\})$ définie par :
$$(a, b)\mathcal{R}(a', b') \Leftrightarrow ab' = a'b$$
Notons $\theta(x, y) = \dot{\widehat{x, y}}$
2. La loi + est définie par :
$$\theta(a, b) + \theta(c, d) = \theta(ad + cb, bd)$$
3. La loi $\times$ est définie par :
$$\theta(a, b)\theta(c, d) = \theta(ac, bd)$$

On vérifie que $\mathcal{F}$ est bien un corps en plongeant A dans $\mathcal{F}$ par l'application :

$$\begin{array}{rccc} \varphi & : & A & \longrightarrow & \mathcal{F} \\ & & a & \longmapsto & \theta(a, 1) \end{array}$$

Quatorzième partie

Espaces vectoriels généraux

Soit $\mathbb{K}$ un corps commutatif.

1 Définition

Définition (espace vectoriel) : Un espace vectoriel sur $\mathbb{K}$ est un ensemble E muni de deux lois :

- Une loi interne additive, notée $+$, telle que $(E, +)$ est un groupe abélien.
- Une loi multiplicative externe de $\mathbb{K} \times E$ dans E, notée $\cdot$, qui vérifie :
  1. $\forall \lambda \in \mathbb{K}, \forall x, y \in E, \quad \lambda(x + y) = \lambda x + \lambda y$
  2. $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, \quad (\lambda + \mu)x = \lambda x + \mu x$
  3. $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, \quad \lambda(\mu x) = (\lambda\mu)x$
  4. $\forall x \in E, \quad 1_{\mathbb{K}} x = x$

Définition (vecteur) : Les éléments de E s'appellent les vecteurs

Définition (scalaires) : Les éléments de $\mathbb{K}$ s'appellent les scalaires

2 Combinaisons linéaires. Sous-espaces vectoriels.

2.1 Combinaisons linéaires

Définition (combinaison linéaire) : Soit E un $\mathbb{K}$ espace vectoriel. On dit que $x \in E$ est combinaison linéaire de $(x_1, \ldots, x_n)$ s'il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ tels que $x = \alpha_1 x_1 + \cdots + \lambda_n x_n$

Soit $(x_i)_{i \in I}$ une famille quelconque de vecteurs de E. Un vecteur x est combinaison linéaire des $(x_i)_{i \in I}$ si il existe une famille $(\alpha_i)_{i \in I}$ d'éléments de $\mathbb{K}$ **tous nuls sauf un nombre fini** telle que $x = \sum_{i \in I} \alpha_i x_i$.

2.2 Sous-espaces vectoriels

Définition (sous-espace vectoriel) : Une partie F d'un espace vectoriel E est un sous-espace vectoriel si elle est stable pour $+$ et $\cdot$ et si F est un espace vectoriel pour les lois induites.

Théorème caractéristique : F est un sous-espace vectoriel de E si et seulement si :

- $F \neq \emptyset$
- $\forall x, y \in F, \quad x + y \in F$
- $\forall \alpha \in \mathbb{K}, \forall x \in F, \quad \alpha x \in F$

ou si et seulement si :

- $F \neq \emptyset$
- $\forall \alpha, \beta \in \mathbb{K}, \forall x, y \in F, \quad \alpha x + \beta y \in F$

2.3 Sous-espace vectoriel engendré

Propriété : Si $(F_i)_{i \in I}$ est une famille quelconque de sous-espaces vectoriels de E, alors $\bigcap_{i \in I} F_i$ est encore un sous-espace vectoriel de E.

Définition (sous-espace vectoriel engendré) Si A est une partie de E, alors l'intersection de tous les sous-espaces vectoriels de E contenant A est le plus petit sous-espace vectoriel de E contenant A. On l'appelle sous-espace vectoriel de E engendré par A et on le note $[A]$

Proposition : Le sous-espace vectoriel engendré par une partie A est l'ensemble des vecteurs de E qui sont combinaisons linéaires d'éléments de A.

$$[A] = \left\{ \sum_{i=1}^{n} \alpha_i x_i \ : \ n \in \mathbb{N}^*, \quad x_1, \ldots, x_n \in A, \quad \alpha_1, \ldots, \alpha_n \in \mathbb{K} \right\}$$

3 Sommes de sous-espaces vectoriels

Remarque : La réunion de deux sous-espaces vectoriels F et G est un sous-espace vectoriel si et seulement si $F \subset G$ ou $G \subset F$.

Définition (somme de sous-espaces vectoriels) : Si F et G sont deux sous-espaces vectoriels de E, on définit leur somme $F + G$ par :

$$F + G = \{x + y \ : \ x \in F, \ y \in G\}$$

Proposition : $F+G$ est le plus petit sous-espace vectoriel de E contenant F et G.

4 Espaces vectoriels quotients

Toutes les relations d'équivalences $\mathcal{R}$ compatibles avec la structure d'espace vectoriel sur E sont de la forme :

$$\forall x, y \in E, \quad x\mathcal{R}y \Leftrightarrow x - y \in F$$

avec F un sous-espace vectoriel de E.

Définition (espace vectoriel quotient) : L'ensemble quotient E/F muni des lois $+$ et $\cdot$ définies par :

$$\dot{x} + \dot{y} = \dot{\widehat{x+y}}$$

$$\dot{x}\dot{y} = \dot{\widehat{xy}}$$

est un espace vectoriel appelé espace vectoriel quotient.

5 Applications linéaires

Définition (application linéaire) : Soient E et F deux $\mathbb{K}$ espaces vectoriels.
Un application u de E dans F est dite linéaire si :
- $\forall x, y \in E, \quad u(x+y) = u(x) + u(y)$
- $\forall \alpha \in \mathbb{K}, \forall x \in E, \quad u(\alpha x) = \alpha u(x)$

ou si et seulement si $\forall \alpha, \beta \in \mathbb{K}, \forall x, y \in E, \quad u(\alpha x + \beta y) = \alpha u(x) + \beta u(y)$

Définition (endomorphisme) : Un endomorphisme est une application linéaire de E dans E.

Définition (isomorphisme) : Un isomorphisme est une application linéaire bijective.

Définition (automorphisme) : Un automorphisme est un endomorphisme bijectif.

Notation : On note $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E dans F, $\mathcal{E}$ l'ensemble des endomorphismes de E et $\mathcal{GL}(E)$ le groupe des automorphismes linéaires de E.

Proposition : Si $u \in \mathcal{L}(E,F)$ et $v \in \mathcal{L}(F,G)$, alors $v \circ u \in \mathcal{L}(E,G)$

Proposition : Si $u \in \mathcal{L}(E,F)$ est un isomorphisme, alors u^{-1} est encore linéaire.

Proposition : Soit $u \in \mathcal{L}(E,F)$

1. Si A est un sous-espace vectoriel de E, alors $u(A)$ est un sous-espace vectoriel de F.
2. Si B est un sous-espace vectoriel de F, alors $u^{-1}(B)$ est un sous-espace vectoriel de E.

Proposition : Soit $u \in \mathcal{L}(E,F)$

- u est surjective si et seulement si $\text{Im}u = F$
- u est injective si et seulement si $\text{Ker } u = \{0\}$

Factorisation canonique : Soient E et F deux espaces vectoriels et u une application linéaire de E dans F.
$u = i \circ b \circ s$ avec :
$s : E \to E/\text{Ker } u$ la surjection canonique,
$b : E/\text{Ker } u \to \text{Im}u$ la bijection, et
$i : \text{Im}u \to F$ l'injection canonique.
i, s et b sont des applications linéaires.

6 Somme directe

Définition (somme directe) : Soit E un espace vectoriel et F_1,F_2 deux sous espaces vectoriels de E.
F_1 et F_2 sont en somme directe si :

$$\forall x \in F_1 + F_2, \quad \exists!(x_1, x_2) \in F_1 \times F_2, \qquad x = x_1 + x_2$$

On note alors $F_1 \oplus F_2$ leur somme.

Proposition : F_1 et F_2 sont et somme directe si et seulement si $F_1 \cap F_2 = \{0\}$.

7 Sous-espaces supplémentaires

Définition (sous-espaces vectoriels supplémentaires) : Soit E un espace vectoriel et F_1,F_2 deux sous espaces vectoriels de E.
F_1 et F_2 sont deux sous-espaces vectoriels supplémentaires si $E = F_1 \oplus F_2$

Remarque :
- supplémentaire ne veut pas dire complémentaire
- Il n'y a pas unicité du supplémentaire

Théorème : Soit E un espace vectoriel, F_1,F_2 deux sous espaces vectoriels de E et s_1 de E dans E/F_1 la surjection canonique. Alors

$$E = F_1 \oplus F_2 \Leftrightarrow s_1|_{F_2} : F_2 \to E/F_1 \text{ est un isomorphisme}$$

En particulier, tout supplémentaire de F_1 est isomorphe à E/F_1.

8 Prolongement d'applications linéaires

Remarque : Soient E et G deux espaces vectoriels et F un sous-espace vectoriel de E. Soit $u \in \mathcal{L}(F, G)$.
Pour prolonger u dans E, la bonne idée et de prendre H, un sous-espace vectoriel de E tel que $E = F \oplus H$.
Alors $\forall x \in E$, $x = x_F + x_H$ avec $x_F \in F$ et $x_H \in H$ uniques et

$$\begin{array}{rccc} \bar{u} & : & E & \longrightarrow & G \\ & & x & \longmapsto & u(x_F) + v(x_H) \end{array}$$

avec $v \in \mathcal{L}(H, G)$.

Théorème : Soit $u \in \mathcal{L}(E, F)$.
Tout supplémentaire de Ker u dans E est isomorphe à Imu.

9 Somme directe de plusieurs sous-espaces vectoriels

Définition (somme directe) : Soit E un espace vectoriel et $F_1, \ldots, F_p$ des sous-espaces vectoriels de E.
On dit que $F_1, \ldots, F_p$ sont en somme directe si :

$$\forall x \in F_1 + \cdots + F_p, \quad \exists!(x_1, \ldots, x_p) \in F_1 \times \cdots \times F_p, \qquad x = x_1 + \cdots + x_p$$

Proposition : Soit E un espace vectoriel et $F_1, \ldots, F_p$ des sous-espaces vectoriels de E.
$F_1, \ldots, F_p$ sont en somme directe si et seulement si :

$$\forall (x_1, \ldots, x_p) \in F_1 \times \cdots \times F_p, \quad x_1 + \cdots + x_p = 0 \Leftrightarrow x_1 = \cdots = x_p = 0$$

Quinzième partie

Existence de bases

Rappel : Une famille $(x_i)_{i\in I}$ de vecteurs de E indexée part I (ensemble quelconque) est une application

$$\begin{array}{ccc} I & \longrightarrow & E \\ i & \longmapsto & x_i \end{array}$$

Remarque : Attention : Une famille n'est pas un ensemble!!!

1 Familles libres, génératrices, bases

Définition (famille libre) Une famille $(x_1, \ldots, x_n)$ de vecteurs de E est dite libre si :

$$\forall (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n, \quad \lambda_1 x_1 + \cdots + \lambda_n x_n = 0 \Rightarrow \lambda_1 = \cdots = \lambda_n = 0$$

Conséquence Si y est combinaisons linéaire de $x_1, \ldots, x_n$, alors les coefficients sont uniques.

Définition (famille libre) La famille $(x_i)_{i\in I}$ de vecteurs de E est dite libre si toute sous-famille finie est libre, i.e. :

$$\begin{gathered} \forall n \in \mathbb{N}^*, \quad \forall i_1, \ldots, i_n \in I \text{ distincts}, \quad \forall \lambda_{i_1}, \ldots, \lambda_{i_n} \in \mathbb{K}, \\ \lambda_{i_1} x_{i_1} + \cdots + \lambda_{i_n} x_{i_n} = 0 \Rightarrow \lambda_{i_1} = \cdots = \lambda_{i_n} = 0 \end{gathered}$$

Conséquence Si y est combinaison linéaire de la famille $(x_i)_{i\in I}$,

$$y = \sum_{i\in I} \alpha_i x_i$$

avec $(\alpha_i)_{i\in I} \in \mathbb{K}^{(I)}$ (tous nuls sauf un nombre fini), alors les coefficients $(\alpha_i)_{i\in I}$ sont uniques.

Remarque : Toute sous-famille d'une famille libre est libre.

Définition (famille liée) Une famille $(x_i)_{i\in I}$ est dite liée si elle n'est pas libre.

Remarque Toute sur-famille d'une famille liée est liée.

Définition (famille génératrice) Une famille $(x_i)_{i\in I}$ est génératrice si elle engendre E, i.e. :

$$\forall x \in E, \quad \exists (\lambda_i) \in \mathbb{K}^{(I)}, \qquad x = \sum_{i\in I} \lambda_i x_i$$

Remarque : cette propriété de dépend que de $\{x_i \ : \ i \in I\}$ et pas de l'indexation de la famille.
Toute sur-famille d'une famille génératrice est génératrice.

Définition (base) Un famille $(x_i)_{i\in I}$ est une base de E si elle est libre et génératrice, i.e.

$$\forall x \in E, \quad \exists ! (\lambda_i)_{i\in I} \in \mathbb{K}^{(I)}, \qquad x = \sum_{i\in I} \lambda_i x_i$$

Si E a une base finie $(e_1, \ldots, e_n)$, alors l'application

$$\begin{array}{rccc} u & : & \mathbb{K}^n & \longrightarrow & E \\ & & (\lambda_1, \ldots, \lambda_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} \lambda_i e_i \end{array}$$

est un isomorphisme d'espace vectoriel.

Si E a une base infinie $(e_i)_{i\in I}$, alors l'application

$$\begin{array}{rccc} u & : & \mathbb{K}^{(I)} & \longrightarrow & E \\ & & (\lambda_i)_{i\in I} & \longmapsto & \displaystyle\sum_{i=1}^{n} \lambda_i e_i \end{array}$$

est un isomorphisme d'espace vectoriel.

Théorème : On a équivalence entre :

1. $\mathcal{B}$ est une base
2. $\mathcal{B}$ est une famille libre maximale
3. $\mathcal{B}$ est une famille génératrice minimale

Procédé de construction d'application linéaire Soit E un espace vectoriel admettant une base $(e_i)_{i\in I}$. Soit F un autre espace vectoriel et $(y_i)_{i\in I}$ une famille de vecteurs de F.
Alors il existe une unique application linéaire u de E dans F telle que :

$$\forall i \in I, \quad u(e_i) = y_i$$

Propriété Soit $u \in \mathcal{L}(E, F)$
- u est injective si et seulement si l'image de toute famille libre est libre
- u est surjective si et seulement si l'image de toute famille génératrice est génératrice

2 Axiome du choix

Définition (fonction de choix) Soit X un ensemble. Une fonction de choix f est une application de $\mathcal{P}(X)$ dans X telle que

$$\forall E \in \mathcal{P}(X), \quad f(E) \in E$$

C'est une fonction qui "choisi" un élément dans chaque partie de X.

Axiome du choix Pour tout ensemble, il existe une fonction de choix.

Variantes :

Théorème de maximalité de Hausdroff : Tout ensemble non vide partiellement ordonné contient un sous-ensemble maximal totalement ordonné.

Lemme de Zorn : Un ensemble partiellement ordonné possède un éléments maximal si tout sous-ensemble totalement ordonné admet une borne supérieure.

3 Existence de bases

Théorème (Complétion d'une partie libre en une base) : Soit E un $\mathbb{K}$-espace vectoriel, L une partie libre de E et S une partie génératrice de E telle que $L \subset S$.
Il existe alors une base $\mathcal{B}$ de E telle que

$$L \subset \mathcal{B} \subset S$$

Corollaire (existence de bases) : Soit E un $\mathbb{K}$-espace vectoriel.

- Si L une partie libre de E, alors L est contenue dans une base $\mathcal{B}$
- si S est une partie génératrice de E, alors S contient une base $\mathcal{B}$.
- Tout $\mathbb{K}$-espace vectoriel admet une base.

Théorème de la base incomplète : Soit E un $\mathbb{K}$-espace vectoriel, L une partie libre de E et S une partie génératrice de E.
Alors il existe $S' \subset S$ tel que $L \cup S'$ soit une base.

Théorème (Existence de sous-espaces vectoriels supplémentaires) : Soit E un $\mathbb{K}$-espace vectoriel, F et G des sous-espaces vectoriels de E tels que $F \cap G = \{0\}$.
Alors il existe H, un sous-espace vectoriel de E tel que :

$$E = F \oplus H \text{ et } G \subset H$$

Seizième partie

Espaces vectoriels de dimension finie

1 Définition, dimension

Définition (espace vectoriel de dimension finie) On dit qu'un espace vectoriel sur $\mathbb{K}$ est de dimension finie s'il admet une partie génératrice finie.

Dans le cas contraire, il est dit de dimension infini.

Théorème de la dimension : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Si L est une partie libre de E et S une partie génératrice de E, alors

$$\text{card } L \leq \text{card } S$$

Remarque Ce théorème reste encore vrai en dimension infinie si on quotiente par la relation d'équivalence :

$$X \approx Y \Leftrightarrow X \text{ est en bijection avec } Y$$

Corollaire Si E est de dimension finie, toute ses bases ont le même cardinal.

Définition (dimension) Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Le cardinal commun de toutes ses bases s'appelle la dimension de E et se note $\dim E$ ou $\dim_{\mathbb{K}} E$

Corollaire : Deux $\mathbb{K}$-espaces vectoriels de dimension finie sont isomorphes si et seulement si ils ont la même dimension.

Proposition Si $\dim E = n$, les bases de E sont les familles libres à n éléments.

Corollaire E est de dimension infinie si et seulement si il existe une famille libre infinie.

2 Calcul de dimension

Proposition Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.
- Si F est un sous-espace vectoriel de E, alors

$$\dim F \leq \dim E$$

- Si de plus $\dim F = \dim E$, alors $E = F$.

Proposition Soit E un espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors :

$$\dim(E/F) = \dim E - \dim F$$

Proposition : Soient E et F deux espaces vectoriels de dimension finie. Alors $E \times F$ est aussi de dimension finie et

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

Proposition Si E est un $\mathbb{K}$-espace vectoriel de dimension finie et F, G deux sous-espaces vectoriels de E, alors :

$$\dim(F + G) + \dim(F \cap G) = \dim F + \dim G$$

Corollaire Si E est un $\mathbb{K}$-espace vectoriel de dimension finie et F, G deux sous-espaces vectoriels de E, alors :

$$\dim(F + G) \leq \dim F + \dim G$$

Il y a égalité si et seulement si F et G sont en somme directe

Corollaire Soient $F_1, \ldots, F_p$ des sous-espaces vectoriels de E, alors

$$\dim(F_1 + \cdots + F_p) \leq \dim F_1 + \cdots + \dim F_p$$

Il y a égalité si et seulement si $F_1, \ldots, F_p$ sont en somme directe.

3 Rang d'un système de vecteurs

Définition (rang) Soit E un espace vectoriel et $S = (x_1, \ldots, x_p)$ p vecteurs de E.
Le rang de S est la dimension du sous-espace vectoriel qu'il engendre.

Proposition Si $\dim E = n$ et $\text{card } S = p$, alors :
- rang $S \leq \min\{n, p\}$
- rang $S = n \Leftrightarrow S$ est génératrice
- rang $S = p \Leftrightarrow S$ est libre
- rang $S = n = p \Leftrightarrow S$ est une base

Remarque Le rang est inchangé par :
- permutation des vecteurs,
- multiplication d'un vecteur par un scalaire non nul,
- ajout à un vecteur d'une combinaison linéaire des autres.

Définition (rang) Soit E et F deux espaces vectoriels et $u \in \mathcal{L}(E, F)$
Le rang de u est la dimension de Imu.

Théorème du rang : Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie et $u \in \mathcal{L}(E, F)$. Alors :

$$\dim E = \dim \text{Ker } u + \text{rang } u$$

Théorème Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie tels que $\dim E = \dim F$ et soit $u \in \mathcal{L}(E, F)$. On a équivalence entre :

1. u est bijective
2. u est injective
3. u est surjective

4 Matrices

Définition (matrice) Soit $\mathbb{K}$ un corps commutatif, I et J des ensembles finis. Une matrice de type I, J est une application de $I \times J$ dans $\mathbb{K}$

Si $I = \{1, \ldots, n\}$ et $J = \{1, \ldots, p\}$, on note d'ensemble des matrices de type I, J (à n lignes et p colonnes) :

$$\mathcal{M}_{n,p}(\mathbb{K}) \text{ ou } \mathcal{M}_{\mathbb{K}}(n, p)$$

Définition (matrice d'un morphisme) Soient E et F deux espaces vectoriels de dimension fini sur $\mathbb{K}$ et $u \in \mathcal{L}(E, F)$.
Soient $\mathcal{B}_E = (e_j)_{j \in J}$ une base de E et $\mathcal{B}_F = (f_i)_{i \in I}$ une base de F.
Pour tout $j \in J$, $u(e_j) \in F$ se décompose sur $\mathcal{B}_F$:

$$u(e_j) = \sum_{i \in I} \alpha_{ij} f_i$$

La matrice $(\alpha_{ij})_{\substack{i \in I \\ j \in J}}$ de type I, J est la matrice de u dans les bases $\mathcal{B}_E$ et $\mathcal{B}_F$.
On la note

$$\mathcal{M}(u, \mathcal{B}_E, \mathcal{B}_F) \text{ ou } \mathcal{M}_{(\mathcal{B}_E, \mathcal{B}_F)}(u)$$

Théorème : Soient $\mathcal{B}_E$ et $\mathcal{B}_F$ des bases fixées de E et F, espaces vectoriels de dimension finie.
L'application

$$\begin{array}{ccc} \mathcal{L}(E, F) & \longrightarrow & \mathcal{M}_{I,J}(\mathbb{K}) \\ u & \longmapsto & \mathcal{M}(u, \mathcal{B}_E, \mathcal{B}_F) \end{array}$$

est un isomorphisme d'espace vectoriel.

Remarque : Si

$$E \xrightarrow{u} F \xrightarrow{v} G$$

alors

$$\mathcal{M}(v \circ u, \mathcal{B}_E, \mathcal{B}_G) = \mathcal{M}(v, \mathcal{B}_F, \mathcal{B}_G)\mathcal{M}(u, \mathcal{B}_E, \mathcal{B}_F)$$

Changement de base

Définition (matrice de passage) Soit E un espace vectoriel et $\mathcal{B}_E$, $\mathcal{B}'_E$ deux bases de E.
La matrice de passage de $\mathcal{B}_E$ à $\mathcal{B}'_E$ est la matrice donnant les coordonnées des vecteurs de $\mathcal{B}'_E$ dans $\mathcal{B}_E$.

Soit $x \in E$, si on note X les coordonnées de x dans $\mathcal{B}_E$, X' les coordonnées de x dans $\mathcal{B}'_E$ et P la matrice de passage de $\mathcal{B}_E$ à $\mathcal{B}'_E$, alors :

$$X = P \cdot X'$$

Index