Algebre Lineaire I

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Le language des Ensembles

Mon 14 Sep

1 Le language des Ensembles

Le terme “Algebre” est derive du mot arabe al-jabr tire du tire d’un ouvrage. Al-jabr signifie restoration.

Par exemple : $2x - 4 = 0$ Ce qu’on veut c’est trouver x. Il faut donc transformer cette egalite en effectuant des operations de part et d’autres de l egalite.

$$\begin{aligned} 2x &= 4 && | + 4 \\ x &= \frac{4}{2} = 2 && | : 2 \end{aligned}$$

Le but de l’ouvrage etait de resoudre des soucis administratifs, comment partager des champs etc.

Le but c’est d’introduire les espaces vectoriels a partir de 0.

Il y aura besoin d’introduire des groupes, anneaux, corps (anneaux particuliers), modules et des ensembles.

Il faut donc commencer avec les objets les plus simples, i.e. les groupes.
Ici, on introduit de maniere moins rigoureuse qu’avec les systemes algebriques.

1.1 Notations

— "Il existe" $\exists$, "Il existe un unique" $\exists!$

— "Quel que soit", "Pour tout", $\forall$

— "Implique", $\Rightarrow$

— "est equivalent" $\iff$, ou “ssi”

— "sans perte de generalite" “spdg”, “wlog”

— “on peut supposer” “ops, wma”

— “tel que” t.q. ou |

On ne va pas parler de logique mathematique dans ce cours, ni de definition rigoureuse des ensembles

1.2 Ensembles

Un ensemble est une collection d'elements "appartenant" a E

$$e \underbrace{\in}_{\text{"appartient à"}} E$$

1.2.1 Exemples

— $\emptyset$ ne contient aucun element

— $\mathbb{N} = \{0, 1, 2\}$

— $\mathbb{Z} = \{-2, -1, 0, 1, 2\}$

— $\mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\}$
— $\mathbb{R}$, nombres réels, nombres complexes.

1.3 Sous-Ensembles

Un sous-ensemble A d'un ensemble E est un ensemble t.q. tout element de A appartient a E. Formellement :

$$a \in A \Rightarrow a \in E$$
$$A \underbrace{\subset}_{\text{inclut dans } E} E$$

L'ensemble vide est un sous-ensemble de E pour tout ensemble E.

$$\emptyset \subset E \forall E$$

Deux ensembles E et F sont egaux si ils ont les mêmes élements, ssi E est inclus dans F et F est inclus dans E (regarder notations)

$$E \subset F \wedge F \subset E \Rightarrow E = F.$$

1.4 $\mathcal{P}(E)$ l'ensemble des sous-ensembles

C'est l'ensemble des $A \in E$, aussi appelé l'ensemble des parties de E.

Remarque : L'ensemble de TOUS les ensembles n'est pas un ensemble et c'est du au paradoxe de Russell (Logicien anglais) Si c'etait le cas, on considererait

$$Ncont = \{ \text{ L'ensemble des } E \text{ tq } E \text{ n'est pas contenu dans lui meme. } \}$$

Cet ensemble Ncont est-il contenu dans lui meme ou pas ?

1.4.1 Exercice

Ncont est il contenu dans lui meme ou pas ? ↯

1.5 Operations sur les ensembles

— $A, B \subset E$

$$A \cup B = \{e \in E \text{ tq } e \in A \text{ ou bien } e \in B\}$$

Réunion de A et B.

— $A \cap B = \{e \in E | e \in Ae \in B\}$

Difference : $A - B$ ou $A \setminus B$

$$= \{A \in A \wedge \notin B\}$$

Difference symmetrique :

$$A \Delta B = (A - B) \cup (B - A)$$

Si $A \cap B = \emptyset$ on dit que A et B sont disjoints. $A_1, \ldots, A_n \subset E$ $n \geq 1$

On peut noter une grande reunion ainsi :

$$\begin{aligned} A_1 \cup A_2 \cup \ldots \cup A_n &= A_1 \cup (A_2 \cup \ldots \cup A_n) \\ &= \{e \in E | \exists i \in \{1, \ldots, n\} \text{avec} e \in A_i\} \\ &= \bigcup_{i=1}^{n} A_i \end{aligned}$$

1.6 $\times$: Produit cartesien

Si A et B sont des ensembles

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

On peut bien sur iterer

$$A_1 \times \ldots \times A_n = \prod_{i=1}^{n} A_i = \{a_1, a_2, \ldots, a_n \text{ avec } a_i \in A_i\}$$

1.7 Applications entre ensembles

Soient X et Y deux ensembles.

Une application (fonction) f est la donnee pour chaque element $x \in X$ (L'espace de depart) d'un element $f(x) \in Y$ (l'espace d'arrivee)

$$f : X \to Y$$

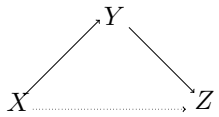

FIGURE 1 – Schema de la composition de 2 applications

1.7.1 Graphe

Se donner une application

$$f : X \to Y$$

equivaut a se donner un graphe G (graphe de f)

$$G \subset X \times Y = \{(x, y) | x \in X y \in Y\}$$

tq pour $x_0 \in X$ l'ensemble des elements du graphe G de la forme (x_0, y) possede exactement un element (x_0, y_0). $y_0 = f(x_0) =$ l'image de x_0 par l'application f.

On associe simplement au premier element un autre element.

1.8 Composition/Associativite

Soient

$$f : X \to Y$$

$$g : Y \to Z$$

$$g \circ f : X \longrightarrow Z | x \in X \longrightarrow f(x) \in Y \longrightarrow g(f(x)) \in Z$$

Cette application s'appelle la composee de f et g.

1.8.1 Associativite

$$f : X \longrightarrow Y$$

$$g : Y \longrightarrow Z$$

$$h : Z \longrightarrow W$$

Alors

$$(g \circ f) : X \longrightarrow Z \circ h : Z \longrightarrow W$$
$$\Rightarrow h \circ (g \circ f)$$

$$f : X \longrightarrow Y \circ h \circ g : Y \longrightarrow W$$

On a que

Theorème 1 (Composition de fonctions)

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

Preuve

$$\begin{aligned} h \circ (g \circ f) : x &\longrightarrow h((g \circ f)(x)) \\ &= h(g(f(x))) \in W \\ (h \circ g) \circ f : x &\longrightarrow (h \circ g)(f(x)) \\ h(g(f(x))) &\in W \end{aligned}$$

□

1.9 Image,Preimage

$$f : X \longrightarrow Y$$

A l'application f sont associes deux applications impliquant $\mathcal{P}(X), \mathcal{P}(Y)$.

— $Im(f) : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$
$A \subset X \longrightarrow Im(f)(A) = f(A)$
C'est ce qu'on appelle l'image de A par f

$$= \{f(a) \in Y | a \in A\} \subset Y \in \mathcal{P}(Y)$$

L'image de f $Im(f) := f(X) = \{f(x) \in Y | x \in X\}$

— Preimage de f : $Preim(f)$:

$$Preim(f) : \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$$
$$B \longrightarrow Preim(f)(B) = f^{-1}(B) \quad = \text{preimage de l'ensemble } B \text{ par } f.$$
$$f^{-1}(B) = \{x \in X | f(x) \in B\}$$

Exemples

$$f_1(\{1,2\}) = \{2,4\}$$

$$f_1^{-1}(\{1,2,3,4\}) = \{1,2,3,4\}$$

Lecture 2: Injectivite, Surjectivite et Bijectivite

Tue 15 Sep

Definition 1 (Injectivite)
Une application $f : X \mapsto Y$ est injective (injection) si $\forall y \in Y f^{-1}(\{y\})$ ne possede pas plus d'un element. On note

$$f : X \hookrightarrow Y$$

Remarque : Une condition equivalente d' injectivite :

$$\forall x \neq x' \in X \Rightarrow f(x) \neq f(x')$$

Definition 2 (Surjectivite)
Une application $f : X \mapsto Y$ est surjective (surjection) si $\forall y \in Y f^{-1}(\{y\})$ possede au moins un element.
On note

$$f : X \twoheadrightarrow Y$$

Soit $f^{-1}(\{y\}) \neq \emptyset$, il existe au moins $x \in X$ tq $f(x) = y$
De maniere equivalente

$$\text{surjectif} \iff Im(f) = f(X) = Y$$

Alors on a une application

$$\text{“}f'' : X \mapsto Y$$
$$x \mapsto f(x)$$

Cette application est toujours surjective.

Definition 3 (Bijectivite)
Une application $f : X \mapsto Y$ est bijective (bijection) si elle est injective et surjective, cad si $\forall y \in Y, f^{-1}(\{y\}$ (l'ensemble des antecedents de y par f) possede exactement un element. On note la bijectivite par

$$f : X \simeq Y$$

Si $f : X \simeq Y$, alors on peut identifier les els de X avec ceux de Y :

$$x \in X \leftrightarrow f(x) \in Y$$

Remarque : Si $f : X \hookrightarrow Y$
$Y' = f(X)$ l'application

$$f : X \twoheadrightarrow Y' = f(x)$$

et toujours surjective. et comme f est injective, on obtient une bijection $f : X \simeq Y' = f(X)$ entre X et $f(X)$.
X peut etre identifie a $f(X)$.

- $Id_X : \underbrace{X \mapsto X}_{x \mapsto x}$ est bijective
- $x \in \mathbb{R}_{\geq 0} \mapsto x^2 \in \mathbb{R}_{\geq 0}$ est inj et bijective.
- $\mathcal{P} \simeq \{0,1\}^X = \mathcal{F}(X, \{0,1\})$

Exercice
$C : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$
$(m,n) \simeq \frac{1}{2}((m+n)^2 + m + 3n)$
Montrer la bijectivite.

Dans ce qui suit, soient X et Y des ensembles finis possedant respectivement $|X|$ et $|Y|$ elements et $f : X \mapsto Y$ une application entre ces ensembles. On a les proprietes suivantes :

Proposition 2 (Injectivite et cardinalite)
Si $f : X \hookrightarrow Y$ est injective alors $|X| \leq |Y|$

Proposition 3 (Surjectivite et cardinalite)
Si $f :\twoheadrightarrow Y$ est surjective alors $|X| \geq |Y|$.

Proposition 4 (injectivite et condition)
Si $f : X \hookrightarrow Y$ et $|X| \geq |Y|$ alors $|Y| = |X|$ et f bijective.

Proposition 5 (Surjectivite et condition)
Si $f : X \twoheadrightarrow Y$ et $|X| \leq |Y|$ alors $|Y| = |X|$ et f bijective.

Propriete 6 (Bijectivite)
Si f bijective, on peut lui associer une application reciproque :

$$f^{-1} : Y \mapsto X$$
$$y \mapsto x$$

tel que $f^{-1}(\{y\}) = \{x\}$, x unique.

1.10 Relation de composition par les applications reciproques

— $f : X \simeq Y$ et $f^{-1} : Y \simeq X$

$$f^{-1} \circ f : X \mapsto Y \mapsto X = Id_X.$$

En effet, $\forall x \in X$ si on pose $y = f(x)$
on a $f^{-1}(y) = x = f^{-1}(f(x)) = x$
— $f \circ f^{-1} : Y \mapsto X \mapsto Y$
$f \circ f^{-1} = Id_Y$

— $(f^{-1})^{-1} = f$
— $f : X \simeq Y$ et $g : Y \simeq Z$
Alors $g \circ f : X \mapsto Z$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Lemme 7 (Composition d'applications surjectives et injectives)
1. *Si f et g sont injectives, $g \circ f$ est injective.*

2. *Si f et g sont surjectives, $g \circ f$ est surjective.*

3. *Si f et g sont bijectives, $g \circ f$ est bijective et*

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

Preuve
1. $g \circ f : X \mapsto Y \mapsto Z$
$x \mapsto g(f(x))$
$\forall z \in Z$ *on veut montrer que* $(g \circ f)^{-1}(\{z\})$ *a au plus un element*

$$(g \circ f)^{-1}(\{z\}) = \{x \in X | g(f(x)) = z\}$$
$$si\ g(f(x)) = z \Rightarrow f(x) \in g^{-1}(\{z\})$$

l'ensemble $\{x \in X | g(f(x)) = z\}$ est contenu dans $g^{-1}(\{z\})$ et donc possede au plus 1 element. Si cet ensemble est vide on a fini $(g \circ f)^{-1}(\{z\}) =$

$\emptyset$. *Si* $g^{-1}(\{z\}) \neq \emptyset$ *alors* $g^{-1}(\{z\}) = \{y\}$
et $x \in (g \circ f)^{-1}(\{z\})$ *verifie*

$$f(x) = y \Rightarrow x \in f^{-1}(\{y\})$$

Comme f^{-1} *est injective* $f^{-1}(\{y\})$ *possede au plus un element.*
Et donc $g^{-1}(f^{-1}(\{z\})$ *a au plus 1 element car* g *est surjective*

2. *Surjectivite : Exercice*

3. *Bijectivite : si* f *et* g *sont bijectives* $g \circ f$ *est bijective.*
   f *et* g *sont inj* $\Rightarrow g \circ f$ *inj.*
   f *et* g *sont surj* $\Rightarrow g \circ f$ *surj*
   Si f *et* g *sont bij* $\Rightarrow g \circ f$ *est injective et surjective*
   $\Rightarrow g \circ f$ *bijective.* □

Proposition 8 (Inverse d'une composition)
On veut montrer que $\forall z \in Z$

$$X := (g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z) \underbrace{=}_{?} f^{-1}(g^{-1}(z)) = x'$$

Preuve

$$\begin{aligned} g \circ f(x) &= g(f(x)) = z \\ g \circ f(f^{-1}(g^{-1}(z))) &= g(f(f^{-1}(g^{-1}(z)))) \\ &= g(f \circ f^{-1}(g^{-1}(z))) \end{aligned}$$

Or on sait que

$$f \circ f^{-1} = g \circ g^{-1} Id_Y$$

et donc

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

On a donc montre que

$$(g \circ f)(x) = z = (g \circ f)(x')$$ □

$\Rightarrow x$ *et* x' *on la meme image par* $g \circ f$ *et comme* $g \circ f$ *est injective* $x = x'$. *Donc* $\forall z \in Z (g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$.

L'ensemble des applications entre X et Y seran note

$$\mathcal{F}(X, Y) = HOM_{ENS}(X, Y) = Y^X$$

Definition 4 (Notations Injection)
L'ensemble des applications injectives sera note

$$INJ_{ENS}(X,Y)$$

Definition 5 (Notations Surjection)
L'ensemble des applications surjectives sera note

$$SURJ_{ENS}(X,Y)$$

Definition 6 (Notations Bijection)
L'ensemble des applications bijectives sera note

$$BIJ_{ENS}(X,Y) = Iso_{ENS}(X,Y)$$

Si il s'agit d'une bijections de X vers $Y = X$ alors

$$Hom_{ENS}(X,X) = END_{ENS}(X) = AUT_{ENS} = ISO_{ENS}(X)$$

On appelle cet ensemble aussi parfois l'ensemble des permutations de X.

2 Groupes

2.1 Le groupe Symmetrique

Voici un exemple d'un groupe, le groupe des bijections muni de la composition.
X ensemble

$$Bij(X,X) = Bij(X)$$

Clairement $\{Id_X\} \subset Bij(X) \Rightarrow Bij(X) \neq \emptyset$.
Supposons $f, g \in Bij(X)$, alors

$$f, g \mapsto g \circ f \in Bij(X)$$

On dispose donc de cette loi de composition :

$$\circ : \begin{array}{c} Bij(X) \times Bij(X) \longrightarrow Bij(X) \\ (g,f) \longrightarrow g \circ f \end{array}$$

$\circ$ est associative :
$f, g, h \in Bij(X)$, alors

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

Id_X est neutre : $\forall f \in Bij(X)$

$$f \circ Id_X = Id_X \circ f = f$$

Donc

$$x \in X (f \circ Id_X)(x) = f(Id_X(x)) = f(x)$$

Pour chaque element f on trouve une reciproque notee f^{-1} tel que

$$f^{-1} \circ f = Id_X = f \circ f^{-1}$$

Toutes ces proprietes font de

$$Bij(X) = Aut_{ENS}(X)$$

un groupe

Definition 7 (Groupe abstrait)
Un groupe $(G, \star, e_G, \cdot^{-1})$ est la donnee d'un quadruple forme

- *d'un ensemble G non-vide*
- *d'une application (appellee loi de composition interne) $\star$ tq*

$$\star : \begin{array}{l} G \times G \mapsto G \\ (g, g') \mapsto \star(g, g') =: g \star g' \end{array}$$

- *d'un element $e_G \in G$ (element neutre)*
- *de l'application d'inversion $\cdot^{-1}$*

$$\cdot^{-1} : \begin{array}{l} G \mapsto G \\ g \mapsto g^{-1} \end{array}$$

ayant les proprietes suivantes

- *Associativite : $\forall g, g', g'' \in G, (g \star g') \star g'' = g \star (g' \star g'')$.*
- *Neutralite e e_G : $\forall g \in G, g \star e_G = e_G \star g = g$.*
- *Inversibilite : $\forall g \in G, g^{-1} \star g = g \star g^{-1} = e_G$.*

Quelques exemples :

- $(Bij(X), \circ, Id_X, \cdot^{-1})$ est un groupe.
- $(\mathbb{Z}, +, 0, -\cdot)$ est un groupe.
- $(\mathbb{Q} \setminus \{0\}, \times, 1, \cdot^{-1})$ est un groupe.
- $(\{1, -1\}, \times, 1, \cdot^{-1})$ est un groupe.

Definition 8 (Groupes commutatifs)
Un groupe $(G, \star, e_G, .^{-1}$ est dit commutatif si $\star$ possede la propriete supplementaire de commutativite :

$$\forall g, g' \in G g \star g' = g' \star g$$

Exemple Les groupes $(\mathbb{Z}, +)$ ou $(\mathbb{Q} \setminus \{0\}, x)$ sont des groupes commutatifs.
Par contre si X possede au moins 3 elements $Bij(X)$ n'est pas commutatif.

Lecture 3: Groupes, Anneaux, Corps

Tue 22 Sep

$\exists \sigma, \tau \in Bij(x)$ tq. $\sigma \circ \tau \neq \tau \circ \sigma$

Definition 9 (Notation additive)
Si un groupe est commutatif on pourra utiliser une notation "additive" :

- *La loi sera notee $+$.*
- *L'element neutre sera note 0_G.*
- *L'inversion sera appele oppose et notee $-gg + (-g) = 0_G$.*

Proposition 9 (Lois de Groupe)

- *Involutivite de l'inversion : $\forall g, (g^{-1})^{-1} = g, g^{-1} \star g = e_G$.*
- *L'element neutre est unique, si $\exists e'_G$ tq $g \in G$ verifiant $g \star e'_G = g$, alors e'_G est l'element neutre.*
- *Unicite de l'inverse : si $g' \in G$ verifie $g \star g' = e_G$, alors $g' = g^{-1}$.*
- *On a $(g \star g')^{-1} = g'^{-1} \star g^{-1}$*

Preuve
La preuve de toutes les proprietes est donnee dans le support de cours.
On montre l'unicite de l'element neutre.
Si e'_G est telle que pour un certain $g \in G$, tq

$$g \star e'_G = g$$

Alors on $\star$ a gauche par $g^{-1} g^{-1} \star g \star e'_G = g^{-1} \star g$

$$= e_G \star e'_G = e_G = e'_G$$

Admettons que l'inverse est unique et montrons que si $g, g' \in G (g \star g')^{-1} = g'^{-1} \star g^{-1}$

On calcule

$$\begin{aligned}(g \star g') \star (g'^{-1} \star g^{-1}) &= g \star g' \star g'^{-1} \star g^{-1} \\ &= g \star e_G \star g^{-1} = g \star g^{-1}\end{aligned}$$

de meme :

$$(g'^{-1} \star g^{-1}) \star (g \star g') = e_G$$

Donc $g'^{-1} \star g^{-1}$ *a les meme proprietes d'inversion que* $(g \star g')$ *et par unicite c'est* $(g \star g')^{-1}$. □

Definition 10 (Notation exponentielle)
$(G, \cdot)$ *un groupe et* $g \in G$. *On peut :*

$$g \to g^{-1}\ g \cdot g, g \cdot g \cdot g, g \cdot g \cdot g \cdot g \dots$$

On peut faire ca n *fois* $n \geq 1$ *un entier, on notera :*

$$g \cdot g \cdot g \cdot g = g^n$$

si $n < 0$ *:*

$$g^n := (g^{-1})^n = \underbrace{g^{-1} \cdot g^{-1} \cdot \dots g^{-1}}_{|n| fois}$$

et $g^0 := e_G$

Exercice 10
Verifier que : $g^{m+n} = g^m \cdot g^n$

Definition 11 (exponentielle)

$$\exp_g : \begin{matrix}\mathbb{Z} \to G \\ n \to g^n\end{matrix}$$

On l'appelle l'exponentielle de n *en base* g.

$$\exp_g(m+n) = \exp_g(m) \cdot \exp_g(n)$$

Definition 12 (Notation multiple)
Si G *est commutatif et que le groupe est note additivement*

$$n \geq 1 \underbrace{g + \dots + g}_{n\ fois} = n \cdot g$$

Si $n < 0$

$$n \cdot g := \underbrace{(-g) + \dots + (-g)}_{|n|\ fois}$$

Donc on a la notation

$$\forall m, n \in \mathbb{Z} (m+n) \cdot g = m \cdot g + n \cdot g$$

3 Sous-Groupe

Definition 13 (Sous-groupe)
Soit $(G, \star, e_g, \cdot^{-1})$ un groupe. Un sous-groupe $H \subset G$ est un sous-ensemble de G tq

1. $e_G \in H$
2. *H est stable par la loi de composition*
$$\forall h, h' \in H, h \star h' \in H$$
3. *H est stable par l'inversion*
$$\forall h \in H, h^{-1} \in H$$

$(H, \star, e_g, \cdot^{-1})$ forme un groupe

Proposition 11 (Critere de Sous-groupe)
Pour montrer que $\emptyset \neq H \subset G$ est un sous groupe il suffite de verifier l'une ou l'autre de ces proprietes :

1. a. $\forall h, h' \in H, h \star h' \in H$
   b. $\forall h \in H, h^{-1} \in H$
2. $\forall h, h' \in H, h \star h'^{-1} \in H$.

Preuve
Montrons que H verifie le point 1 de la definition.
Comme $H \neq \emptyset$ il existe $h \in H$. Par hypothese $h \star h^{-1} \in H$.
On verifie la stabilite par inversion
Soit $h \in H$ et par hypothese $e_G \in H$ $e_G \star h^{-1} \in H$
On verifie la stabilite par produit
Soit $h, h' \in H$ alors $(h')^{-1} \in H$ et $h \star ((h')^{-1})^{-1} \in H$. Or
$$((h')^{-1})^{-1} = h' \Rightarrow h \star h' \in H$$ □

Exemple
$(G, \cdot) g \in G$ *et* $g^{\mathbb{Z}} = \exp_g(\mathbb{Z}) = \{g^n, n \in \mathbb{Z}\}$ *Forme un sous groupe.*

Preuve
Soit $h, h' \in H = g^{\mathbb{Z}}$ alors
$$h = g^m h' = g^{m'} m, m' \in \mathbb{Z}$$
Alors
$$h \cdot h' = g^m \cdot g^{m'} = g^{m+m'} \in g^{\mathbb{Z}}$$
Soit $h \in g^{\mathbb{Z}} h = g^m$ comme $h^{-1} = g^{-m}$ alors $h^{-1} \in g^{\mathbb{Z}}$ □

Exemple

1. *$\{e_G\} \subset G$ est un sous groupe de G on l'appelle le sous groupe trivial de G.*

2. *$G \subset G$ est un sous groupe*

3. *$(\mathbb{Z}, +) q \in \mathbb{Z}$*

4. *$q \cdot \mathbb{Z} = \{a, a = q \cdot k, k \in \mathbb{Z}\}$*

Preuve

On prouve la derniere propriete

— $0 \in q\mathbb{Z}$ *car* $0 = q \cdot 0$

— qk *et* $q \cdot k' \in q\mathbb{Z} \Rightarrow qk + qk' = q(k + k') \in q \cdot \mathbb{Z}$

— $qk \in q\mathbb{Z}$ □

Theorème 14 (Sous groupe de $\mathbb{Z}$)
Reciproqueme tout sousgroupe de $\mathbb{Z}$ est de la forme $q \cdot \mathbb{Z}$.

Preuve

Soit $H \subset \mathbb{Z}$ un sous groupe

— *si* $h = \{0\}, H = 0 \cdot \mathbb{Z}$.

— *si* $H \neq \{0\}$ *soit* $q \in H \neq 0$

Alors, sans perte de generalite, on peut supposer que $q > 0$ (si $q < 0$ on remplace q par $-q \in H$)

Sans perte de generalite on peut supposer que q est le plus petit el strictement positif contenu dans H

$$q = q_{min} = \min(h \in H, h > 0)$$

On va montrer que $H = q\mathbb{Z}$.
Soit $h \in H$ par division euclidienne il existe $k \in \mathbb{Z}$ et $r \in \{0, \ldots, q-1\}$ tq

$$h = qk + r$$
$$r = h - qk \in H$$ □

Donc $0 \geq r < q \Rightarrow r = 0$ par def de q.
Donc $h = q \cdot k \in q\mathbb{Z}$.

3.1 Groupe engendre par un ensemble

Proposition 15 (Intersection de sous-groupes)
Soit G un groupe et $H_1, H_2 \subset G$ deux sous groupes alors $H_1 \cap H_2$ est un sous groupe. Plus generalement l intersection de sous groupes est un sous-groupe.

Preuve
Cas $H_1 \cap H_2$. On veut montrer que c'est un sous groupe. On utilise la deuxieme version du critere de la proposition 11.

$$\forall h, h' \in H_1 \cap H_2 \Rightarrow ? h \star h'^{-1} \in H_1 \cap H_2$$

Comme $h, h' \in H_1 h \star h'^{-1} \in H_1$ et $h, h' \in H_2 h \star h'^{-1} \in H_2$
Donc $h \star h'^{-1} \in H_1 \cap H_2$
$\Rightarrow H_1 \cap H_2$ est un sous-groupe □

Definition 14 (Sous-groupe engendre)
G un groupe et $A \subset G$ un sous-ensemble de G.
Le sous-groupe engendre par A, note $< A > \subset G$ est par definition le plus petit sous groupe de G contenant A.
Soit

$$G_A = \{H \subset G, H \text{ est un sous groupe et } A \subset H\}$$

G_A est non-videcar il contient G.
Par la proposition precedente, on considere

$$\langle A \rangle := \bigcap_{H \in G_A} H$$

Par la proposition cette intersection est un sous groupe qui contient A et c'est le plus petit possible au sens ou si $H \subset G$ est un sous groupe contenant A alors

$$\langle A \rangle = \bigcap_{H \in G_A} H \subset H'$$

Exemple
Si $g \in G \langle \{g\} \rangle = g^{\mathbb{Z}} = \{g^n, n \in \mathbb{Z}\}$

Lecture 4: Groupes et Anneaux

Mon 28 Sep

Theorème 17
Soit $A \subset G$ un ensemble,si $A = \emptyset$ alors $\langle A \rangle = \{e_G\}$, sinon on pose

$$A^{-1} = \left\{g^{-1}, g \in A\right\} \subset G$$

l'image de A par l'inversion alors

$$\langle A \rangle = \left\{g_1 \star \ldots \star g_n, g_i \in A \cup A^{-1}\right\}$$

En d'autres termes, $\langle A \rangle$ est l'ensemble des elements de G qu'on peut former en multipliant ensemble des elements de A et de son invers A^{-1} de toutes les manieres possibles.

Preuve

Pour montrer que c'est $\langle A \rangle$, on procede par double inclusion.

$\supset$: soit $H \subset G$ un ssgpe tq

$$A \subset H \subset G$$

Alors commme H est stable par $\bullet^{-1}$

$$A^{-1} \subset H^{-1} = H$$

Donc, $A \cup A^{-1} \subset H$ comme H est stable par $\star$, si $g_1, \ldots, g_n \in A \cup A^{-1}$ Le produit $g_1 \star g_2 \star \ldots \star g_n \in H$

Donc $\left\{g_1 \star g_2 \star \ldots \star g_n, g_i \in A \cup A^{-1}\right\} \subset H$ et donc $\left\{g_1 \star g_2 \star \ldots \star g_n, g_i \in A \cup A^{-1}\right\} \subset \bigcap_{A \subset H} H \subset \langle A \rangle$

$\subset$: il suffit de mq $\{\ldots\}$ et un sous groupe de G. En effet, $\left\{g_1 \star \ldots \star g_n, n \geq 1, g_i \in A \cup A^{-1}\right\} \supset A$

Critere de ss-groupe :

a) Soit $g \in A \Rightarrow g^{-1} \in A^{-1}, g \star g^{-1} = e_G \in \{g_1 \star \ldots \star g_n, \ldots\}$

b)Soit $g = g_1 \star g_2 \star \star \ldots \star g_n$ etg$' = g'_1 \star g'_2 \star \star \ldots \star g'_n$

$$n, n' \geq 1, g_i, g'_j \in A \cup A^{-1}$$

Alors

$$g \star g' = g_1 \star \ldots \star g_n \star g'_1 \ldots g'_n \in \{\ldots\}$$

c) soit $g = g_1 \star \ldots \star g_n$comme ci-dessus

$$g^{-1} = g_n^{-1} \star g_{n-1}^{-1} \star \ldots \star g_1^{-1} \in \{\ldots\}$$

$\{\ldots\}$ est un sousgroupe de G contenant A donc il contient $\langle A \rangle$. □

3.2 Morphismes de Groupes

Definition 15 (Morphisme de Groupe)

Soient $(G, \star)$ et $(H, \bullet)$ deux groupes, un morphisme de groupes $\phi : G \to H$ est une application telle que

$$\forall g, g' \in G, \phi(g \star g') = \phi(g) \bullet \phi(g')$$

Theorème 18

Soit $\phi : G \to H$ un morphisme de groupes alors

1. $\phi(e_G) = e_H$
2. $\forall g \in G, \phi(g^{-1}) = \phi(g)^{-1}$

3. $\forall g, g' \in G, \phi(g \star g') = \phi(g) \bullet \phi(g')$

Preuve

Il suffit de demontrer 1 et 2, 3 est vrai par definition.

1)

Soit $g \in G, \phi(g) = \phi(g \star e_G) = \phi(g) \bullet \phi(e_G)$.

Donc $\phi(g) = \phi(g) \star \phi(e_G)$ *et donc*

$$h = h \bullet \phi(e_G)$$
$$h^{-1} \bullet h = h^{-1} \bullet h \bullet \phi(e_G)$$

2)

$$\phi(g) \bullet \phi(g)^{-1} = e_H$$
$$\phi(g) \bullet \phi(g^{-1}) = \phi(g \star g^{-1})$$
$$= \phi(e_G) = e_H$$

On conclut en utilisant l'unicite de l'inverse

$$\phi(g^{-1}) = \phi(g)^{-1}$$

□

Definition 16 (Notations)

- $Hom_{Gr}(G, H)$ *l'ensemble des morphismes de groupe entre* G *et* H.
- $End_{Gr}(G) = Hom_{Gr}(G, G)$ *les endomorphismes du groupe* G.
- $Isom_{Gr}(G, H)$ *l'ensemble des morphismes bijectifs*
- $Aut_{Gr}(G) = Isom_{Gr}(G, G)$ *l'ensembles des automorphismes du groupe* G.

Exemple

—

$$e_H : \begin{cases} G \to H \\ g \to e_h \end{cases}$$

— *Soit* $g \in G$

$$\exp_G : \begin{cases} \mathbb{Z} \to G \\ n \to g^n \end{cases}$$

Si G *est commutatif note additivement*

$$\bullet.g : \begin{cases} \mathbb{Z} \to G \\ n \to n.g \end{cases}$$

Conjugaison dans un groupe : $(G, .)$

$$h \in G$$

$$Ad_h : \begin{cases} G \to G \\ g \to h.g.h^{-1} \end{cases}$$

Preuve

On veut montrer que $\forall g, g' \in G$

$$Ad_h(g.g') = Ad_h(g).Ad_h(g')$$

$$\begin{aligned} Ad_h(g).Ad_h(g') &= (h.g.h^{-1}).(h.g.h^{-1}) \\ &= h.g.h^{-1}.h.g'.h^{-1} \\ &= h.g.e_G.g'.h^{-1} \qquad\qquad = h.g.g'.h^{-1} = Ad_h(g.g') \end{aligned}$$

Terminologie :

$$Ad_h(g) = h.g.h^{-1}$$ □

Le conjugue de g *par* g*.*

Remarque

$Ad_h : G \to G$ *est bijectif.* Ad_h *admet une application reciproque qui est* Ad_h^{-1}

Preuve

$Ad_{h^{-1}} \circ Ad_h ? = Id_G$

$Ad_h \circ Ad_{h^{-1}} ? = Id_G$

Il suffit de montrer le premier.

$$\begin{aligned} Ad_{h^{-1}} \circ Ad_h(g) &= h^{-1}.(h.g.h^{-1}).h \\ &= h^{-1}.h.g.h^{-1}.h \\ = g = Id_G(g) \end{aligned}$$

car $(h^{-1})^{-1} = h$ □

$\forall h \in G$,

$$Ad_h \in Aut_{Gr}(G)$$

Proposition 21

Soient $(G, \star), (H, *), (K, \bullet))$ *des groupes et* $\phi : G \to H$ *et* $\psi : H \to K$ *des morphismes de groupes alors la composee* $\psi \circ \phi : G \to K$ *est un morphisme de groupes*

Preuve
On veut montrer que

$$\psi \circ \phi(g \star g') = ?\psi \circ \phi(g) \bullet \psi \circ (g')$$

on a :

$$\begin{aligned} \psi \circ \phi(g \star g') &= \psi(\phi(g \star g')) \\ &= \psi(\phi(g) * \phi(g')) \\ &= \psi(\phi(g)) \bullet \psi(\phi(g')) \end{aligned}$$ □

Proposition 22
Soit $\phi : G \to H$ un morphisme de groupe bijectif alors l'application reciproque ϕ^{-1} est un morphisme bijectif.

Preuve
Soit $\phi : G \to H$ un morphisme de groupe bijectif (en tant qu'application), on veut montrer que $\phi^{-1} : H \to G$ verifie

$$\phi^{-1}(h \star h') = ?\phi^{-1}(h) * \phi^{-1}(h'), \forall h, h' \in H$$

On calcule

$$\begin{aligned} \phi(\phi^{-1}(h) * \phi^{-1}(h')) &= \phi(\phi^{-1}(h)) \star \phi(\phi^{-1}(h')) \\ &= h \star h' \\ \Rightarrow \phi^{-1}(h) * \phi^{-1}(h') & \end{aligned}$$ □

est un antecedent de $h \star h'$ mais le seul antecedent de $h \star h'$ c'est $\phi^{-1}(h \star h')$
$\Rightarrow \phi^{-1}(h) * \phi^{-1}(h') = \phi^{-1}(h \star h')$

Definition 17 (Groupes Isomorphes)
Soient G et H deux groupes si

$$Isom_{gr}(G, H) \neq \emptyset$$

On dit que G et H sont isomorphes (comme groupes)

$$G \simeq_{Gr} H$$

et si $Isom_{gr}(G.H) \neq \emptyset$ alors $Isom_{Gr}(H, G) \neq 0, H \simeq_{Gr} G$

La relation "etre isomorphe" dans la categorie des groupes est une relation d'equivalence :

— $G \simeq_{Gr} G$ ($Isom_{Gr(G,G) \ni Id_G}$)
— Si $G \simeq_{Gr} H \Rightarrow H \simeq_{Gr} G$

— Si $G \simeq_{Gr} H$ et $H \simeq_{Gr} K \Rightarrow G \simeq_{Gr} K$

Exemple
Le groupe des automorphismes d'un groupe

$$Aut_{Gr}(G) = Isom_{Gr}(G,G) \subset Bij(G)$$

Theorème 24
$Aut_{Gr}(G)$ est un sous-groupe de $\left(Bij(G), \circ, Id_G, \bullet^{-1}\right)$

Preuve
Si ϕ et $\psi \in Isom_{Gr}(G,G)$, alors $\psi \circ \phi$ est un morphisme et $\psi \circ \phi$ est bijectif $\Rightarrow \in Isom_{Gr}(G,G)$
Si $\phi \in Isom_{Gr}(G,G) \cup Bij(G,G)$ alors ϕ^{-1} est un morphisme donc

$$Isom_{Gr}(G,G) = Aut_{Gr}(G)$$ □

Lecture 5: Noyau et Image

Tue 29 Sep

4 Noyau et Image

Proposition 25
Soit $\phi \in Hom_{Gr}(G,H)$ un morphisme de groupes.

— *Soit $K \subset G$ un sous groupe alors $\phi(K) \subset H$ est un sous-groupe. En particulier l'imaged de ϕ,*

$$Im(\phi) = \phi(G)$$

— *Soit $L \subset H$ un sous-groupe de H, alors l'image inverse*

$$\phi^{-1}(L) = \{g \in G, \phi(g) \in L\} \subset G$$

est un sous-groupe de G. En particulier, $\phi^{-1}(\{e_H\})$ est un sous-groupe

Preuve
Soit $K \subset G$ un sous-groupe.
Soit

$$h, h' \in \phi(K)$$

On veut montrer que $h \star h'^{-1} \in \phi(K)$.
Il existe $k, k' \in K$ tel que $\phi(k) = h, \phi(k') = h'$

$$\begin{aligned} h \star h'^{-1} &= \phi(k) \star \phi(k')^{-1} \\ &= \phi(k) \star \phi(k'^{-1}) \end{aligned}$$

$$= \phi(k * k'^{-1}),\ k * k'^{-1} \in K$$

car K sous-groupe.

$$h \star h'^{-1} \in \phi(K)$$

Soit $L \subset H$ un sous-groupe, on veut montrer que

$$\phi^{-1}(L) \subset G$$

est un sous-groupe Soient $g, g' \in \phi^{-1}(L)$, alors $\phi(g) = h \in L, \phi(g') = h' \in L$

$$g \star g'^{-1} \in \phi^{-1}(L)?$$

on a

$$\begin{aligned}\phi(g \star g'^{-1}) &= \phi(g) * \phi(g')^{-1} \\ &= h * h'^{-1} \in L \text{ car } L \text{ sous-groupe}\end{aligned}$$ □

Definition 18
Le sous-groupe $\phi^{-1}(\{e_H\})$ s'appelle le noyau de ϕ et est note

$$\ker(\phi) = \phi^{-1}(\{e_H\}) = \{g \in G, \phi(g) = e_H\}$$

L'importance du noyau vient du fait qu'il permet de tester facilement si un morphisme est injectif.

Theorème 26 (Critere d'injectivite)
Soit $\phi \in Hom_{Gr}(G, H)$ un morphisme de groupes alors les proprietes suivantes sont equivalentes

- *ϕ est injectif*
- $\ker(\phi) = \{e_G\}$

Preuve
$1 \to 2$
si ϕ est injectif, l'image reciproque de $\{e_H\}$ possede au plus un seul element. Mais comme ϕ est un morphisme $\phi(E_G) = e_H \Rightarrow \phi^{-1}(\{e_H\}) = \{e_G\}$
$2 \to 1$
On se donneun $h \in H$ et on veut montrer que $\phi^{-1}(\{h\}) = \{g \in G, \phi(g) = h\}$ n'a pas plus d'un element.
Si $\phi^{-1}(\{h\}) = \emptyset$ OK
Si $\phi^{-1}(\{h\}) \neq \emptyset$, soient $g, g' \in \phi^{-1}(\{h\})$ on veut montrer que $g =? g'$.
Par definition, $\phi(g) = \phi(g') = h$

$$\phi(g) * \phi(g')^{-1} = e_H$$

$$= \phi(g * g'^{-1}) \text{ car } \phi \text{ morphisme}$$

Donc, $g * g'^{-1} \in \ker(\phi) = \{e_G\}$,

$$\Rightarrow g * g'^{-1} = e_G \Rightarrow g = g' \qquad \square$$

Exemple
Ordre d'un element
Soit $g \in G$ *groupe*

$$\exp_g : \mathbb{Z} \to Gn \in (\mathbb{Z}, +) \to g^n \in G$$

est un morphisme de groupes.

$$\ker(\exp_g) \subset \mathbb{Z}q \cdot \mathbb{Z}, q \in \mathbb{Z}$$

Si $q = 0$, $\ker(\exp_q) = \{0\}$

$$\Rightarrow \mathbb{Z} \to G$$
$$n \to g^n \text{ est injective}$$

$\mathbb{Z}$ *est isomorphe a* $g^{\mathbb{Z}}(\mathbb{Z} \simeq g^{\mathbb{Z}})$

$$G \supset g^{\mathbb{Z}} \simeq \mathbb{Z}$$

donc g *est d'ordre infini.*
Si $q > 0$, *alors*

$$g^{\mathbb{Z}} = \left\{g^0 = e_G, g, g^2, \ldots, g^{q-1}\right\}$$

est un sous-groupe de cardinal q *(a demontrer en exercice) et donc* G *contient un sous-groupe d'ordre* q

$$q := \text{ ordre de } g \ = ord(g)$$

q *est le plus petit entier* > 0 *tel que*

$$g^q = e_G$$

Exemple (Conjugaison)
$G \ni h$

$$Ad_h : g \to h.g.h^{-1}$$

On a montrer que $Ad_h \in Aut_{Gr}(G)$

On considere l'application

$$h \in G \to Ad_h \in Aut_{Gr}(G)$$

Cette application est un morphisme de groupes :
On doit verifier que : $\forall h, h' \in G$

$$Ad_{h.h'} = Ad_h \circ Ad_{h'}$$

On veut montrer que pour tout $g \in G$

$$Ad_{h.h'} = Ad_h(Ad_{h'}(g))$$

$$\begin{aligned} h.h'.g.(h.h')^{-1} &= h.h'.g.h'^{-1}.h^{-1} \\ &= h.(h'.g.h'^{-1}).h^{-1} \\ &= Ad_h(Ad_{h'}(g)) \\ \ker(Ad) &= \{h \in G | Ad_h = Id_G\} \\ &= \{h \in G | \forall g \in G Ad_h(g) = g\} \\ &= \left\{h \in G | \forall g \in G, h.g.h^{-1} = g\right\} \\ h.g.h^{-1} = g &\iff h.g = g.h \end{aligned}$$

On dit que h commute avec g.

$\ker(Ad) =$ { l'ensemble des h dans G qui commutent avec tous les elements de de G }
$=$ Centre de G
$= Z(G) = Z_G$

Z_G est un groupe commutatif de G

Exemple (Translation)
Soit $h \in G$ la translation a gauche par h

$$t_h : \begin{cases} G \to G \\ g \to h.g \end{cases}$$

Attention t_h n'est pas un morphisme de groupes, car l'element neutre ne va pas sur lui meme (sauf si $h = e_G, t_h = t_{e_G} = Id_G$)
Par contre t_h est bijective de reciproque $t_{h^{-1}}$

$t_\bullet : h \in G \to t_h \in Bij(G)$ *est un morphisme de groupe injectif, l'image s'appelle le groupe des translations (a gauche) de G.*
Donc $G \simeq t_G \subset Bij(G)$
Tout groupe G abstrait peut s'identifier (est isomorphe) a un sous-groupe d'un groupe de bijections d'un ensemble.

5 Anneaux

Definition 19 (Anneaux)
Un anneau $(A, +, ., 1_A)$ est la donee, d'un groupe commutatif $(A, +)$ (note additivement)d'element neutre note 0_A, d'une loi de composition interne (dite de multiplication)

$$\bullet.\bullet \begin{cases} A \times A \to A \\ (a, b) \to a.b \end{cases}$$

et d'un element unite $1_A \in A$ ayant les proprietes suivantes

1. *Associativite de la mutliplication*

$$\forall a, b, c \in A, (a.b).c = a.(b.c) = a.b.c$$

2. *Distributivite*

$$\forall a, b, c \in A (a + b).c = a.c + b.c, c.(a + b) = c.a + c.b$$

3. *Neutralite de l'unite*

$$\forall a \in A, a.1_A = 1_A.a = a$$

Un anneau est dit commutatif si de plus la multiplication est commutative

$$\forall a, b \in A, a.b = b.a$$

Lemme 30
Pour tout $a, b \in A$, on a

$$0_A.a = a.0_A = 0_A$$

On dit que l'element neutre de l'addition 0_A est absorbant. Pour l'oppose, on a

$$(-a).b = -(a.b) = a.(-b)$$

Preuve
$\forall a \in A$

$$\begin{aligned} a = a.1_A &= a.(1_A + 0_A) \\ &= a.1_A + a.0_A \\ 0_A &= a.0_A \end{aligned}$$

□

Exemple

— *L'anneau nul :* $\{0\}$

— $\mathbb{Z}, (\mathbb{Q}, +, \bullet), (\mathbb{R}, +, \bullet)$
— $\mathcal{F}(X, \mathbb{R})$ *des fonctions d'un ensemble* X *a valeurs dans* $\mathbb{R}$.

$$+ : f + g : x \in X \to f(x) + g(x) = (f + g)(x)$$

$$0_{\mathcal{F}(X,\mathbb{R})} : x \to 0 \in \mathbb{R}$$

$$1_{\mathcal{F}(X,\mathbb{R}):x\to 1\in\mathbb{R}}$$

$(\mathcal{F}(X, A), +, \bullet)$ *est un anneau (commutatif si* A *commutatif) generalisation du cas des fonctions reelles*
— $\mathbb{R}[x] = \left\{P(x) = a_0 + a_1 x + \ldots + a_d x^d, a_0, a_1, \ldots, a_d \in \mathbb{R}, d \geq 0\right\}$
— $A[x] = \left\{P(x) = a_0 + a_1 x + \ldots + a_d x^d, a_0, \ldots a_d \in Ad \geq 0\right\}$
Anneau des polynomes a coefficients dans A.
— $(M, +)$ *un groupe commutatif*

$$End(M) = End_{Gr}(M) = Hom_{Gr}(M, M)$$

$$+ : \psi, \phi \in End(M)$$
$$\phi + \psi : m \to \phi(m) + \psi(m)$$

Soient $\phi, \psi \in End(M)$

$$\phi \circ \psi \in End(M)$$
$$0_{End(M)} : m \in M \to 0_M \in M$$
$$1_{End(M)} : Id_M : m \in M \to m \in M$$

$(End(M), +, \circ, 0_M, Id_M)$ *est un anneau*

Lecture 6: Anneaux 2

Mon 05 Oct

Preuve

Soit $\phi, \psi \in End_{Gr}(M)$, *on veut montrer que*

$$\phi + \psi \in End_{Gr}(M)$$

Pour vérifier celà, on utilise le critère de morphisme : $\forall m, m' \in M$, *alors*

$$(\phi + \psi)(m + m') = (\phi + \psi)(m) + (\phi + \psi)(m')$$

$$\begin{aligned}(\phi + \psi)(m + m') &= \phi(m + m') + \psi(m + m') \\ &= \phi(m) + \psi(m') + \psi(m) + \psi(m') \\ &+ \text{ est commutative} \\ &= \phi(m) + \psi(m') + \phi(m') + \psi(m') \\ &= (\phi + \psi)(m) + (\phi + \psi)(m')\end{aligned}$$

Soit $\phi, \psi, \psi' \in End_{Gr}(M)$ on veut montrer que

$$\phi \circ (\psi + \psi') = \phi \circ \psi + \phi \circ \psi'$$

On veut montrer que $\forall m \in M$

$$\phi \circ (\psi + \psi')(m) = (\phi \circ \psi + \phi \circ \psi')(m)$$

$$\begin{aligned} \phi((\psi + \psi')(m)) &= \phi(\psi(m) + \psi'(m)) \\ &= \phi(\psi(m)) + \phi(\psi'(m)) \\ &= (\phi \circ \psi + \phi \circ \psi')(m) \end{aligned}$$

Reste à faire : associativité de $+$
0_M est l'élément neutre de $+$
Id_M est l'unité pour $\circ$ □

5.1 Elément inversible

Definition 20 (Element Inversible)
Un element $a \in A$ est inversible si il existe $b \in A$ tel que

$$a.b = b.a = 1_A.$$

On dit alors que b est un inverse de a (pour la multiplication).

Remarque
Si l'inverse existe, l'inverse est unique, et on le note a^{-1}.

Notation :
On note $A^\times$ l'ensemble des éléments inversibles de A.

Proposition 33
Soit $A^\times$ l'ensemble des éléments inversibles, alors

$$(A^\times, ., 1_A, \bullet^{-1})$$

forme un groupe : le groupe des éléments inversibles de A.

Exemple

- $\mathbb{Z}^\times = \{\pm 1\}, \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- $\mathcal{F}(X, \mathbb{R})^X = \{f : X \to \mathbb{R}^\times \subset \mathbb{R} | f(x) \neq 0_{\mathbb{R}}$ *pour tout* $x \in X\}$
- $\mathbb{R}[x]^\times = \{a_0 | a_0 \in \mathbb{R}^\times\}$
- $End_{Gr}(M)^\times = Aut_{Gr}(M) = Isom_{Gr}(M, M)$

5.2 Sous-Anneau

Definition 21 (Sous-Anneau)

Soit $(A,+,.)$ un anneau. Un sous-anneau $B \subset A$ est un sous-groupe de $(A,+)$ qui est

- *soit le sous-groupe trivial $\{0_A\}$,*
- *soit qui contient l' unité 1_A et qui est stable par . :*

$$\forall b, b' \in B b.b' \in B$$

Ains $(B,+,.)$ est un anneau.

Lemme 35 (Critère de sous-anneau)

Soit $(A,+,.)$ un anneau et $B \subset A$ un sous-ensemble non-vide alors B est un sous-anneau ssi $B = \{0_B\}$ ou bien $1_A \in B$ et

$$\forall b, b', b'' \in B, b.b' - b'' \in B$$

Preuve

Si $B = \{0_A\}$ c'est un sous-anneau.
Sinon $1_A \in B$ si on prend $b \in B$ alors

$$0_A = 1_A.b - b \in B$$

Alors

$$\forall b, b' \in B$$
$$b - b' = 1_A.b - b' \in B$$

Donc $(B,+)$ est un sous-groupe.
Soient $b, b' \in B$ alors

$$b.b' - 0_A \in B \qquad \square$$

$= b.b'$.

Exemple

- $\{0_A\} \subset A \subset A$
- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- *A un anneau*

$$A.Id_A := \{a.Id_A : b \to a.b\} \subset End_{Gr}(A).$$

est un sous-anneau

5.3 Morphismes d'anneaux

Definition 22 (Morphisme d'anneaux)

Soient $(A,+,.)$, et $(B,+,.)$ des anneaux. Un morphisme d'anneaux $\phi : A \mapsto B$ est un morphisme de groupes commutatif $\phi : (A,+) \mapsto (B,)$ tel que

$$\phi(1_A) = 1_B \text{ ou bien } \phi(1_A) = 0_B$$

$$\forall a, a' \in A, \phi(a.a') = \phi(a).\phi(a')$$

Remarque
Si $\phi(1_A) = 0_B$ *alors* $\phi = 0_B$
Alors $\forall a \in A$

$$\begin{aligned}\phi(a) &= \phi(a.1_A) \\ &= \phi(a)\phi(1_A) = 0_B\end{aligned}$$

Notation : On note les morphismes d'anneaux de A vers B

$Hom_{Ann}(A,B), End_{Ann}(A) = Hom_{Annn}(A,A), Isom_{Ann}(A,B), Aut_{Ann}(A) = Isom_{Ann}(A,A)$

Exemple (Le morphisme canonique)
Le morphisme cannonique :

$Can_A : (\mathbb{Z}, +, .) \to (A, +, .)$

$$n \to n.1_A = 1_A + 1_A + \ldots + 1_A \text{ } n \textit{ fois si } n \geq 0 \textit{ et } -n \textit{ fois si } n < 0$$

est un morphisme d'anneaux.
On doit vérifier que Can_A *est un morphisme entre les groups additifs.*
On doit montrer que $\forall m, n \in \mathbb{Z}$

$$(m \times n).1_A = m.(n.1_A)$$

si m *et* $n \geq 0$

$$\begin{aligned}(m \times n).1_A &= \underbrace{1_A + \ldots + 1_A}_{m \times n \textit{ fois}} \\ &= \underbrace{1_A + \ldots + 1_A}_{n \textit{ fois}} + \underbrace{1_A + \ldots + 1_A}_{n \textit{ fois}} \text{ } m \textit{ fois} \\ &= m.(n.1_A)\end{aligned}$$

5.4 Noyau/Image

Proposition 39 (Noyau d'un morphisme d'anneau)
Soient $\phi \in Hom_{Ann}(A,B)$ *un morphisme alors* $\phi(A) \subset B$ *est un sous-anneau. Par ailleurs le sous-groupe* $\ker(\phi)$ *est stable par multiplication par* A *:*

$$\forall a \in A, k \in \ker(\phi) a.k \in \ker(\phi)$$

Preuve
Soit $k \in \ker \phi, a \in A$

$$a.k \in \ker \phi ?$$

$$\phi(a.k) = \phi(a).\phi(k) = \phi(a).0_B = 0_B \qquad \square$$

Theorème 40
$\phi(A) \subset B$ est un sous-anneau de B.

Preuve
Si $\phi(1_A) = 0_B \Rightarrow \phi = \underline{0}_B$ et donc $\phi(A) = \{0_B\} \subset B$
Sinon $\phi(1_A) = 1_B$. $B' = \phi(A)$ alors $1_B \in B', \phi(A)$ est un sous-groupe de $(B, +)$
Soit $b, b' \in B' = \phi(A)$.

$$b = \phi(a), b' = \phi(a')a, a' \in A$$

Alors

$$b.b' = \phi(a).\phi(a') = \phi(a.a') \text{ car } \phi \text{ est un morphisme d'anneaux} \qquad \square$$

5.5 Modules sur un Anneau

Definition 23 (Modules sur un Anneau)
Soit A un anneau, un A-module (à gauche) est un groupe commutatif $(M, +)$ muni d' une loi de multiplication externe

$$\bullet * \bullet : A \times M \mapsto M$$
$$(a, m) \mapsto a * m$$

(appelée multiplication par les scalaires)ayant lles propriétés suivantes
- *Associativité : $\forall a, a' \in A, m \in M$,*

$$(a.a') * m = a.(a' * m).$$

- *Distributivité : $\forall a, a' \in A, m, m' \in M$,*

$$(a + a') * m = a * m + a' * m, a * (m + m') = a * m + a * m'.$$

- *Neutralité de 1_A : $\forall m \in M$,*

$$1_A.m = m$$

Exemple
- *$\{0_A\} \subset A$ est un A-module*
- *A est un A-module*
- *$(M, +)$ = groupe commutatif est canoniquement un $\mathbb{Z}$-module*

$$\mathbb{Z} \times M \to M$$
$$(n, \overrightarrow{m}) \to n * \overrightarrow{m} = \underbrace{\overrightarrow{m} + \overrightarrow{m} + \ldots}_{n \text{ fois}}$$

Lecture 7: Anneaux Et Modules

Tue 06 Oct

$$A^d = \{(a_1, \ldots, a_d) a_1, \ldots, a_d \in A\}$$

C'est un A-module : le A-module libre de rang d. Soit

$$\begin{aligned} \overrightarrow{x} &= (a_1, \ldots, a_d) \\ \overrightarrow{x'} &= (a'_1, \ldots, a'_d) \\ &\in A^d \\ \overrightarrow{x} + \overrightarrow{x'} &(a_1 + a'_1, \ldots) \end{aligned}$$

Soit

$$a \in A, \overrightarrow{x} \in A^d$$
$$a.\overrightarrow{x} := (a.a_1, \ldots, \ldots, a.a_d)$$

On vérifie (en utilisant l'associativité de $(A, +, .)$ et la distributivité dans A) que A^d est un A-module.

$$1_A.\overrightarrow{x} = \overrightarrow{x}$$

Exemple

— $\phi : A \to B, \ker \phi$ *est un A module pour la multiplication dans A.*

$$\bullet.\bullet : A \times \ker \phi \to \ker \phi$$
$$(a, k) \to a.k$$

— $\mathcal{F}(X, A)$ *fonctions de X (un ensemble quelconque) à valeurs dans A, on a vu que $\mathcal{F}(X, A)$ un groupe commutatif*

$$A \times \mathcal{F}(X, A) \to \mathcal{F}(X, A)$$
$$(a, f) \to a.f : x \to a.f(x)$$

Plus généralement, si M est un A-module $\mathcal{F}(X, M)$ est un A-module.

$$a \in Af : X \to M$$
$$a * f : x \to a * f(x) \in M$$

Remarque

Si X possède d éléments

$$\mathcal{F}(X, A) = A^{\times} \simeq A^d$$

Definition 24 (A-Algebre)

Une A-algebre est un anneau $(B, +, .)$ possedant une structure de A-module qui verifie la propriete d'associativité suivante :

$$\forall a \in A, b, b' \in B a * (b.b') = (a * b).b'$$

$\mathbb{R}[x]$ est une $\mathbb{R}$-algèbre.

5.6 Sous-Module

Definition 25 (Sous-Module)
Un sous-module $N \subset M$ d' un A-module M est un sous-groupe de M qui est stable pour la mutliplication par les scalaires

$$\forall a \in A, n \in B, a * n \in N$$

Definition 26 (Ideal)
Un ideal de A est un sous-ensemble $I \subset A$ qui est un sous-module du module A. De manière équivalente, un idéal de A est un sous-groupe $I \subset A$ qui est stable par multiplication par les éléments de A :

$$\forall a \in a, b \in I, a.b \in I$$

Remarque
Tout idéal $I \subset A$ est un noyau d' un morphisme d'anneau.

Lemme 45 (Critère de Sous-Module)
Soit $N \subset M$ un sous-ensemble dûn A-module M alors N est un sous-module de M ssi

$$\forall a \in A, n, n' \in N, a * n + n' \in N.$$

Preuve
Si on prend $a = -1_A$, on a que

$$\begin{aligned} \forall n, n' \in N - 1_A * n + n' &\in N \\ -n + n' &\in N \end{aligned}$$

Donc N vérifie le critère de sous-groupe, donc est un sous-groupe de $(M, +)$. Comme N est un sous-groupe $0_M \in N$, et $\forall a \in A \forall n \in N$

$$a * n = a * n + 0_M \in N$$

N vérifie les 2 propriétés requises pour être un sous-module. □

Exemple
$\{0_M\} \subset M$ *est clairement stable par multiplication*

- $d \leq d', A[x]_{\leq d} \leq A[x]_{\leq d'} \leq A[x]$
- $\Delta A = \{(a, \ldots, a) = a.(1, \ldots, 1)\} \subset A^d$ ΔA *est un sous-module de A^d.*
- *Plus généralement,*

$$\overrightarrow{x} = (a_1, \ldots, a_d), A.\overrightarrow{x} = \{a.\overrightarrow{x} = (a.a_1, \ldots, a.a_n | a \in A\}$$

est un sous-module de A^d.

Preuve
Soient $a \in A, \overrightarrow{v}, \overrightarrow{v'} \in A.\overrightarrow{x}$

$$\overrightarrow{v} = a'.(a_1, \ldots, a_d) = a'.\overrightarrow{x}$$
$$\overrightarrow{v'} = a''(a_1, \ldots, a_d) = a''.\overrightarrow{x}$$

Critère de sous-module :

$$a.\overrightarrow{v} + \overrightarrow{v'} = a.a'.\overrightarrow{x} + a''.\overrightarrow{x} = (a.a' + a'').\overrightarrow{x} \in A.\overrightarrow{x} \qquad \square$$

5.7 Module engendré par un ensemble

Proposition 47
Soit M *un* A*-module et* M_1, M_2 *des sous-modules alors*

$$M_1 \cap M_2 \subset M$$

est un sous-module et plus généralement soit $(M_i)_{i \in I}$ *une collection de sous-modules alors*

$$\bigcap_{i \in I} M_i \subset M$$

est un sous-module.

Definition 27
Soit $X \subset M$ *un sous-ensemble d' un* A*-module, le module engendré par* X *est le plus petit sous-mdoule de* M *contenatn* X *(l'intersection de tous les sous-modules contenant* X*)*

$$\langle X \rangle := \bigcap_{X \subset N \subset M} N.$$

Theorème 48
Soit $X \subset M$ *un ensemble alors* $\langle X \rangle$ *est soit le module nul* $\{0_M\}$ *si* X *est vide, soit l'ensemble des combinaisons linéaires d'éléments de* X *à coefficients dans* A *:*

$$\langle X \rangle = CL_A(X) := \left\{ \sum_{i=1}^{n} a_i * x_i, , n \geq 1, a_1, \ldots, a_n \in A, x_1, \ldots, x_n \in X \right\}.$$

Pour tout $n \geq 1$*.*

Preuve
$CL_A(X)$ *on va montrer que* $CL_A(X)$ *est un sous-module contenant* X

$$\Rightarrow \langle X \rangle \subset CL_A(X)$$

ensuite on va montrer que si $X \subset N \subset M$ est un sous-module contenant X alors

$$N \supset CL_A(X)$$
$$\Rightarrow CL_A(X) \subset \langle X \rangle$$

On utilise le critère de sous-module :
Soit $a \in A, u, v \in CL_A(X)$

$$a * u + v \in CL_A(X)$$

Or

$$u = a_1 x_1 + \ldots + a_n x_n, a_i \in A, x_i \in X$$
$$v = a'_1 x'_1 + \ldots + a'_m x'_m a'_j \in A, x'_j \in X$$
$$a * u + v = a.a_1 * x_1 + \ldots + a.a_n * x_n + a'_1 * x'_1 + \ldots + a'_m * x'_m \in CL_A(X)$$

$$X \subset CL_A(X)$$

car

$$x = 1_A.x = \text{ combinaison linéaire de longueur 1}$$ □

Soit $X \subset N \subset M$ un sous-module et soit $n \geq 1, a_1, \ldots, a_n \in A$

$$x_1, \ldots x_n \in X$$

Alors comme N est stable par $*$ et que $x_1, \ldots, x_n \in X \subset N$

$$\Rightarrow a_1 * x_1 + \ldots + a_n * x_n \in N$$

Lecture 8: Modules et Corps

Mon 12 Oct

5.8 Morphismes de Modules

Definition 28 (Morhpismes de Module)
Soit A un anneau et M, N des A-modules, un morphisme de A-modules entre M et N est un morphisme de groupes

$$\phi : M \to N$$

qui est compatible avec les lois de multiplication externes $*_M$ et $*_N$:

$$\forall a \in A, m \in M, \phi(a *_M m) = a *_N \phi(m)$$

On dit aussi que ϕ est une application A-linéaire.

Remarque
$\forall a, a' \in A, m, m' \in M$

$$\phi(a *_M m + a' *_M m') = \phi(a * m) + \phi(a' * m') = a *_N \phi(M) + a' *_N \phi(m')$$

Lemme 50 (Critere de l'application lineaire)
Soit $\phi : M \to N$ une application entre deux modules alors ϕ est un morphisme si et seulement si

$$\forall a \in A, m, m' \in M, \phi(a *_M m + m') = a *_N \phi(m) + \phi(m')$$

Preuve
$\Rightarrow$ *a été fait ci-dessus.*
$\Leftarrow$ *:*
Si on prend $a = -1_A$, on obtien

$$\forall m, m' \quad \phi(-m + m') = -\phi(m) + \phi(m')$$

en prenant $m = m'$ on obtient $\phi(0) = 0$, et en prenant $a = 1$, on a

$$\phi(m + m') = \phi(m) + \phi(m')$$

$\Rightarrow$ *ϕ est un morphisme de groupes additifs.*
Si on prend $m' = 0_M$

$$\begin{aligned}\phi(a * m + 0_M) &= \phi(a * m) \\ &= a * \phi(m) + \phi(0_M) = a * \phi(m)\end{aligned}$$

Proposition 51
Soit $\phi : M \to N$ un morphisme de A-module et $M' \subset M$ et $N' \subset N$ des sous-modules, alors

$$\phi(M') \subset Net\phi^{-1}(N') \subset M$$

sont des sous-modules de M et N respectivement. En particulier

$$\ker \phi = \phi^{-1}\{0_N\} \subset M \text{ et } Im\phi(M) \subset N$$

Preuve
Comme ϕ est un morphisme de groupes $\phi(M') \subset N$ est un sous-groupe de N et $\phi^{-1}(N') \subset M$ est un sous-groupe de M Reste a vérifier la stabilité par $*$.

On veut montrer que si $m' \in \phi^{-1}(N')$ alors

$$\forall a \in A \quad a *_M m' \in \phi^{-1}(N')$$

$$m' \in \phi^{-1}(N') \Rightarrow \phi(m') \in N'$$

Comme N' est un sous-module

$$a *_N \phi(m') \in N'$$

msid comme ϕ est linéaire

$$a *_N \phi(m') = \phi(a *_M m') \Rightarrow a * m' \in \phi^{-1}(N')$$

— *Si $M' \subset M$ est un sous-module alors $\phi(M')$ est un sous-module.*
— *On sait que $\phi(M') \subset N$ est un sous-groupe*
Reste a verifier que $\phi(M')$ est stable par $*$ dans A.
Soit $n' \in \phi(M')$ alors $n' = \phi(m'), m' \in M'$ Soit $a \in A$, $a *_N n' = a * N\phi(m') = \phi(a *_M m')$
Comme M' est un sous-module

$$a *_M m' \in M' \text{ et donc}$$
$$a *_N n' = \phi(a *_M m') \in \phi(M') \qquad \square$$

Remarque
Le critère d'injectivité s'applique ϕ un morphisme de A-modules est injectif ssi $\ker \phi = \{0_m\}$ C'est vrai parce que c'est vrai quand on voit ϕ comme un morphisme de groupes.

5.9 Structures Algebriques des espaces de morphismes

Definition 29
On note

$$Hom_{A-mod}(M,N), Isom_{A-mod}(M,N)$$
$$End_{A-mod}(M), = Hom_{A-Mod}(M,M)$$
$$Aut_{A-mod}(M) = GL_{A-mod}(M) = Isom_{A-mod}(M,M)$$

les ensembles de morphismes, morphismes bijectifs, d'endomorphismes et d'automorphismes des A-modules M et N

Proposition 53
Soient $\phi : L \to M$ et $\psi M \to N$ des morphisms de A-modules alors $\psi \circ \phi : L \to N$ un morphisme.

Preuve
Soit $\phi : L \to M$, $\psi : M \to N$ des applications lineaires alors

$$\psi \circ \phi \text{ est linéaire}$$

On sait que $\psi \circ \phi$ est un morphisme de groupes.
Reste a voir que $\forall a \in A, l \in L$

$$\psi \circ \phi(a *_L l) = a *_N \psi \circ \phi(l)$$

$$\psi \circ \phi(a * l) = \psi(\phi(a * l)) = \psi(a *_M \phi(l)) = a *_N \psi \circ \phi(l) \qquad \square$$

Proposition 54
Soient M et N des A-modules alors $Hom_{A-mod}(M, N)$ a une structure naturelle de groupe commutatif.
Si de plus A est commutatif alors $Hom_{A-mod}(M, N)$ a une structure de A-module

Preuve
Si ϕ et $\psi \in Hom_{A-mod}(M, N)$, alors

$$\phi + \psi : m \to \phi(m) + \psi(m)$$

on sait que $\phi + \psi$ est un morphisme de groupes et on montre que c'est meme un morphisme de modules.

$$(\phi + \psi)(a * m) = \phi(a * m) + \psi(a * m) = a * \phi(m) + a * \phi(m) = a * (\phi(m) + \psi(m))$$

Donc $\phi + \psi \in Hom_{A-mod}(M, N)$, donc la proposition est prouvee. $\square$

Theorème 55
Soit M un A-module. L'ensemble $End_{A-mod}(M)$des endomorphismes de M est un sous-anneau de $(End, +, \circ)$ dont le groupe des unites est $Aut_{A-mod}(M)$;
de plus, si A est commutatif, $End_{A-mod}(M)$ possede une structure naturelle de A-module qui en fait une A-algebre.
$End_{A-mod}(M)$ est appellee l'algebre des endomorphismes du A-module M

Preuve
On utilise le critère du sous-anneau.
On sait que $\phi \circ \psi + \Phi \in End_{Gr}(M)$, et on doit vérifier que c'est compatible avec la loi de multiplication externe $*$

$$\begin{aligned}(\phi \circ \psi + \Phi)(a * m) =& ? a * (\phi \circ \psi + \Phi)(m)\\ (\phi \circ \psi + \Phi)(a * m) &= \phi \circ \psi(a * m) + \Phi(a * m)\\ &= a * \phi \circ \psi(m) + a * \Phi(m)\\ &= a * (\phi \circ \psi(m) + \Phi(m))\end{aligned} \qquad \square$$

6 Corps

Definition 30 (Corps)
Un corps K est un anneau commutatif possédant au moins deux éléments $0_k \neq 1_k$ et tel que tout element non-nul est inversible :

$$K^\times = K \setminus \{0_K\}$$

Exemple

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *sont des corps.*
- $\mathbb{Z}$ *n'est pas un corps, car* $\mathbb{Z}^\times = \{\pm 1\}$
- $\mathbb{R}(x)$ *Le corps des fractions rationelles à coefficients dans* $\mathbb{R}$

$$= \left\{ f(x) = \frac{P(x)}{Q(x)}, P(x), Q(x) \in \mathbb{R}[x], Q \neq 0 \right\}$$

si $f(x) = \frac{P(x)}{Q(x)} \neq 0, f(x)^{-1} = \frac{Q(x)}{P(x)}$

Proposition 57
Soit K un corps, B un anneau et $\phi \in Hom_{Ann}(K, B)$ un morphisme. Alors, si ϕ n'est pas nul ($\phi \neq 0_B$) ϕ est injectif.

$$\phi : K \hookrightarrow B$$

Preuve
Soit $\phi : K \to B$ un morphisme d'anneaux, supposons $\phi \neq 0_B$.
Il existe $k \in K$ tel que $\phi(k) \neq 0_B$, alors $k \neq 0_k$ (sinon $\phi(k) = 0_B$)
Comme K est un corps, k est inversible et il existe k^{-1} tel que $k.k^{-1} = 1_K$.
Montrons que ϕ est injectif :
c'est à dire que

$$\ker \phi = \{0_K\}.$$

Supposons que non, alors soit $k \in \ker \phi$, tel que

$$\phi(k) = 0_B \text{ et } k \neq 0_K$$

Comme k est inversible

$$\phi(1_K) = \phi(k.k^{-1}) = \phi(k).\phi(k^{-1}) = 0_B$$

Donc si $\ker \phi \neq \{0_K\}$, *alors* $\phi(1_K) = 0_B$, *mais alors* $\forall \lambda \in K$

$$\phi(\lambda) = \phi(\lambda.1_K) = \phi(\lambda)\phi(1_K) = 0_B$$ □

Donc $\phi = 0_B$ ce qu'on a exclu. ↯

6.1 Corps des fractions

Lemme 58
Soit $\{0\} \neq A \subset K$ *un sous anneau non-nul commutatif d' un corps* K*, alors*

$$\forall a, b \in A, a.b = 0 \iff a = 0 \text{ ou } b = 0$$

Definition 31
Un anneau commutatif tq si $a.b = 0 \Rightarrow a = 0$ *ou* $b = 0$ *est appelé integre.*

Un corps est toujours intègre.

Preuve
Soit $a, b \in A \subset K$*, tel que* $a.b = 0_A = 0_K$*, supposons que* $a \neq 0_K$*, alors* a *admet un inverse dans* K*, il existe* $a^{-1} \in K$ *tel que* $a^{-1}.a = 1_K$*.*

$$a.b = 0_K \Rightarrow a^{-1}.a.b = a^{-1}.0_K \Rightarrow b = 0_K$$ □

Lecture 9: Corps

Tue 13 Oct

Proposition 59
Soit A *un anneau integre, alirs il existe un corps* K *et un morphisme d'anneau injectif*

$$\iota : A \hookrightarrow K$$

de sorte qu'on peut considerer A *comme un sous-anneau de* K *en identifiant* A *à* $\iota(A) \subset K$ *et tel que* K *a la propriete de minimalite suivante : pout tout corps* K' *et tout morphisme injectif*

$$\iota' : A \hookrightarrow K'$$

de sorte que A *peut etre identifie a un sous-crops de* K'*, il existe un morphisme (necessairement injectif)*

$$\iota' : K \hookrightarrow K'$$

prologeant le morphisme ι' *(ainsi* A *et* K *peuvent etre vus comme des sous-anneaux de* K'*)*

Definition 32
On appelle ce corps K *le corps des fractions de* A*.*

Exemple
- $Frac(\mathbb{Z}) = \mathbb{Q}$
- $Frac(\mathbb{R}[X]) = \mathbb{R}(X)$ *(défini comme avant)*

Preuve
Construison K*.*

A est intègre.
On considère l'ensemble produit

$$A \times A \setminus \{0\} = \{(a,b) | a,b \in A, b \neq 0_A\}$$

On définit sur cet ensemble une relation.
$(a,b) \sim (a',b')$ *si et seulement si* $a.b' = a'.b$, *la relation* $\sim$ *est une relation d'équivalence.*

- *Symmetrique : Si* $a.b' = a'.b \iff a'.b = a.b' \iff (a',b') \sim (a,b)$
- *Reflexive :* $(a,b) \sim (a,b) \iff a.b = a.b$
- *Transitive :* $(a,b) \sim (a',b')$ *et* $(a',b') \sim (a'',b'')$.
  On a $a.b' = a'.b$ *et* $a'.b'' = a''.b'$.

$$\begin{aligned} &\implies ab'b'' = a'b'b'' \\ &\implies a.b''.b' = a.b''.b' \\ \implies a.b''b' = a'b''b = a''b'b &= a''bb' \\ \implies (ab'' - a''b).b' &= 0_A \end{aligned}$$

Comme A est intègre,

$$ab'' - a''b = 0_A \text{ ou bien } b' = 0_A$$

Donc

$$ab'' - a''b = 0_A$$

Donc $(a,b) \sim (a'',b'')$

Soit $K = A \times A \setminus \{0\} / \sim$ *l'ensemble des classe d'équivalences.*
On note $\frac{a}{b}$ *la classe de l'élément* (a,b).
On va munir K d'une addition et d'une multiplication d'un 0_K, *d'une* 1_K *ainsi que*

$$\iota : A \hookrightarrow K$$

Il faut maintenant vérifier toutes les propriétés d'un corps.

$$+ : \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

$b.b' \neq 0_A$ *vrai car* $b, b' \neq 0$ *et A integre.*

On doit vérifier que cette définition ne dépend que des classes d'équivalence $\frac{a}{b}$ *et* $\frac{a'}{b'}$.
Si $(a'',b'') \sim (a',b')$ *on veut voir que* $\frac{a}{b} + \frac{a'}{b'} = \frac{a}{b} + \frac{a''}{b''}$. *On doit vérifier que*

$$\underbrace{(ab' + a'b)}_{abb'b'' + a'b^2b''} .bb'' = \underbrace{(ab'' + a''b)}_{abb'b'' + a''b^2b'} .bb'$$

On sait que $a'b'' = a''b'$.

$$\Rightarrow a'b^2b'' = a''b^2b'$$

On fait pareil pour définir la multiplication $\times$

$$\frac{a}{b} \times \frac{a'}{b'} = \frac{a.a'}{b.b'}$$

et on doit vérifier que si $\frac{a''}{b''} = \frac{a'}{b'}$ *alors* $\frac{a}{b} \times \frac{a'}{b'} = \frac{a}{b} \times \frac{a''}{b''}$ *sachant que* $a'b'' = a''b'$.
On vérifie que $+, \times$ *sont commutatives, associatives, distributives.*
On définit $0_k = \frac{0}{1_A}$ *et* $1_K = \frac{1_A}{1_A}$
Enfin, dire que $\frac{a}{b} \neq 0_K \iff a$ *et* $b \neq 0_A$ *et alors si* $\frac{a}{b} \neq 0_K$ $\frac{b}{a} \times \frac{a}{b} = \frac{1_A}{1_A} = 1_K$.
On a un morphisme injectif

$$\iota : A \hookrightarrow K$$

donné par

$$\iota(a) = \frac{a}{1_A}$$

On vérifie que c'est un morphisme d'anneau et, si $\iota(a) = 0_K = \frac{0_A}{1_A} \iff \frac{a}{1_A} = \frac{0_A}{1_A} \iff a = 0_A$, *donc*

$$\ker \iota = \{0_A\}$$

donc ι *est injectif.* □

6.2 Caractéristique des Corps

K un corps,

$$Can_K : \mathbb{Z} \to A$$
$$n \to n.1_K = n_k$$
$$\ker(Can_K) = p\mathbb{Z}, p \geq 0$$

Definition 33 (Caractéristique)
L'entier p *s'appelle la caractéristique du corps* K *et se note*

$$car(K)$$

Si $p = 0$: $\ker Can_K = \{0_\mathbb{Z}\}$, donc Can_K est injectif et donc $\mathbb{Z}$ peut être vu comme sous-anneau de K.

$$n \in \mathbb{Z} \to n_K \in K$$

Si $n \neq 0, n_K \neq 0$ et $\frac{1}{n_K}$ existe et pour tout $a, b \in \mathbb{Z}, b \neq 0$, on définit

$$(\frac{a}{b})_K = a_K / b_K \in K$$

On dispose d'un morphisme injectif

$$Can_K : \mathbb{Q} \hookrightarrow K$$
$$\frac{a}{b} \to \frac{a_K}{b_K}$$

Si $Car(K) = 0$, le corps $\mathbb{Q}$ est un sous-corps de K.

Lemme 61
Si $car(K) > 0$, alors $car(K) = p$ est un nombre premier.

Preuve
Si $p = 1$, $\ker Can_K = \mathbb{Z}$

$$\Rightarrow Can_K(1) = 1_K = 0_K \lightning$$

Donc $p \geq 2$.
Soit une factorisation

$$p = q_1 \cdot q_2$$

non-triviale ($q_1, q_2 \geq 2$)

$$0_K = Can_K(p) = Can_K(q_1 \cdot q_2) = Can_K(q_1) \cdot Can_K(q_2)$$

Comme K est intègre, $Can_K(q_1) = 0_K$

$$q_1 \in \ker Can_K = p\mathbb{Z}$$
$$q_1 = pk, k \in \mathbb{Z} \setminus \{0\}$$

Donc $q_1 \geq p$ mais comme $q_2 \geq 2$

$$q_2 \leq \frac{p}{2} < p$$

Donc p est premier. □

Definition 34

$$\mathbb{F}_p = Can_K(\mathbb{Z}) = \mathbb{Z}.1_K$$

Lemme 62
L'anneau $\mathbb{F}_p$ est un corps fini de cardinal p.

Preuve
Si $n \in \mathbb{Z}$ et $k \in \mathbb{Z}$

$$(n + pk)_K = n_K + p_k.k_K = n_k$$

Donc, si $r \in \{0, \ldots, p\}$ le reste de la division euclidienne de n par p

$$\mathbb{Z}.1_K = \{0_K, 1_K, \ldots, (p-1)_K\}$$

$\mathcal{F}_p$ est de cardinal p.
Il faut montrer que si $0 < i \neq j \leq p - 1$

$$i_K \neq j_K$$

mais

$$i_K - j_K = (i-j)_K$$

et comme $0 \leq i, j \leq p-1$, $0 \neq |i-j| < p$ *Donc* $i-j$ *ne peut pas etre un multiple de* p, *donc* $i - j \notin \ker Can_K$ *Donc*

$$(i-j)_K = i_K - j_K \neq 0_K$$ □

Lemme 63
Un anneau commutatif integre et fini est un corps

Preuve
exercice □

$\mathbb{F}$ est integre car c'est un sous-anneau du corps K et il est fini de cardinal p.

Definition 35
Le corps $\mathbb{Q} \subset K$ *si* $car(K) = 0$ *ou bien* $\mathbb{F}_p \subset K$ *(si* $car(K) = p > 0$*) s'appelle le sous-corps premier de* K.

Remarque
Le corps

$$\mathbb{F}_p \simeq (\mathbb{Z}/p\mathbb{Z}, +, \times)$$

l'anneau des classes de congruences module p

6.3 Arithmétique des corps de caractéristique $p > 0$

Proposition 65
Soit K *un corps de caractéristique* $p > 0$, *alors l'application*

$$\begin{aligned} \bullet^p : K &\to K \\ x &\to x^p \end{aligned}$$

est un morphisme d'anneaux non-nul (donc nécessairement injectif).

Definition 36
Soit K *un corps de caractersitique* p, *le morphisme d'anneau precedent s'appelle le morphisme de Frobenius (ou simplement le Frobenius)de* K *se note*

$$frob_p : x \to x^p$$

Preuve
$\forall x, y \in K$

$$\begin{aligned} (x.y)^p &= x.y.x.y.x.y.x.y \dots \\ &= x^p y^p \end{aligned}$$

$\forall x, y \in K$

$$(x+y)^p = x^p + y^p$$

Comme K est commutatif, on a la formule du binome de Newton

$$\begin{aligned}(x+y)^p &= \sum_{k=0}^{p} \binom{k}{p} x^k y^{p-k} \\ &= x^p + y^p + \sum_{k=1}^{p-1} \binom{k}{p} x^k y^{p-k}\end{aligned}$$

Lemme 66
Si $1 \leq k \leq p-1$, alors

$$p | \binom{p}{k}$$

Or

$$\binom{p}{k} x^k y^{p-k} = \binom{p}{k} x^k y^{p-k} = 0_K \cdot x^k y^{p-k}$$

□

Lecture 10: EV

Mon 19 Oct

7 Espaces Vectoriels

Definition 37 (Espace Vectoriel)
Soit K un corps, in K-espace vectoriel V est simplement un K-module.
Les éléments de V sont appelés vecteurs de V.

Exemple
$\mathbb{Q}^d, \mathbb{R}^d, \mathbb{C}^d, d \geq 1$
Espaces de fonctions

$$\mathcal{F}(X; \mathbb{R}) \simeq \mathbb{R}^X$$

Plus généralement, si V est un K-ev

$$\mathcal{F}(X; V) = V^X \text{ est un } K\text{-ev}$$

Definition 38 (Produit)
Si V et W sont des K-ev

$$V \times W = \{(v, w), v \in V, w \in W\}$$

Definition 39
Soit V un K-espace vectoriel, un sous-espace vectoriel (SEV) de V est un sous-K module $W \subset V$

Proposition 68 (Critere de SEV)
Un sous-ensemble $U \subset V$ d'un K-ev est un sev si

$$\forall \lambda \in K, \overrightarrow{v}, \overrightarrow{v'} \in U \Rightarrow \lambda \overrightarrow{v} + \overrightarrow{v'} \in U$$

Exemple
- $\{0_V\} \subset V$
- $e \in V \quad K.e = \{\lambda.e \quad \lambda \in K\} \subset V$ *est un SEV.*

Definition 40
Soient V et W deux K-espaces vectoriels, un morphisme $\phi : V \to W$ de K-modules est appelé une application K-linéaire.

Proposition 70 (Critere d'application linéaire)
Une application entre espaces vectoriels $\phi : V \to W$ est linéaire ssi

$$\forall \lambda \in K, \overrightarrow{v}, \overrightarrow{v'} \in V, \phi(\lambda.\overrightarrow{v} + \overrightarrow{v'}) = \lambda\phi(\overrightarrow{v}) + \phi(\overrightarrow{v'})$$

Preuve
C'est un cas particulier du critere de morphisme de modules. □

Proposition 71
Le noyau et l'image d' une application linéaire est un sev

Preuve
C'est un cas particulier du critere de morphisme de modules. □

Proposition 72
ϕ une application linéaire. ϕ injective ssi

$$\ker \phi = \{0\}$$

Definition 41 (Notations)
On notera

$$Hom_{K-ev}(V, W), Isom_{K-ev}(V, W), Aut_{K-ev}(V) = GL(V)$$

Les ensembles des applications bijectives.

Definition 42
Une forme linéaire sur V est une application linéaire a valeurs dans K

$$l : V \mapsto K.$$

On note l'ensemble des formes linéaires

$$V^* := End_{K-ev}(V, K)$$

C'est le dual.

Proposition 73
Soit $l : V \mapsto K$, si $l \neq 0_K$, alors l est surjective

$$l(V) = K.$$

Preuve
Comme $l \neq 0_K$, il existe

$$v \in V \text{ tel que } l(v) = x \neq 0_K$$

Soit $y \in K$, on cherche v' tel que $l(v') = y$.
Comme $x \neq 0_K$, x est inversible d'inverse x^{-1} soit $v' = y.x^{-1}.v$, on a

$$l(v') = l(y.x^{-1}.v) = y.x^{-1}.l(v) = y.x^{-1}.x = y \qquad \square$$

7.1 Familles génératrices

Definition 43
Soit $\mathcal{F} \subset V$ un sous-ensemble, on note

$$\langle \mathcal{F} \rangle = Vect(\mathcal{F}) = CL_K(\mathcal{F})$$

le sous-espace vectoriel engendre par $\mathcal{F}$.

Definition 44
Soient $X, Y \subset V$ des sev d' un espace vectoriels. Leur somme $X + Y \subset V$ est

$$X + Y = \langle X \cup Y \rangle \subset V$$

est le sev engendré par les vecteurs de X et de Y.

Lemme 74
On a

$$X + Y = \{x + y, x \in X, y \in Y\}$$

Preuve
Il suffit de montrer que $\{x + y, x \in X, y \in Y\}$ est un sev.
En effet, si c'est le cas, il contient X, Y, il contient donc $X \cup Y$ et donc il contient $\langle X \cup Y \rangle = X + Y$.
De plus, comme $\langle X \cup Y \rangle$ contient tout élément $x \in X$ et tout élément $y \in Y$, il contient $x + y$ (car c'est un sev)

$$\Rightarrow \langle X \cup Y \rangle = \{x + y \quad x \in X, y \in Y\}$$

Soit $\lambda \in K, x + y$ et $x' + y' \in \{u + v \quad u \in X, v \in Y\}$.

$$\lambda(x + y) + (x' + y') = \lambda x + \lambda y + x' + y'$$
$$= (\lambda x + x') + (\lambda y + y') \in \{u + v, u \in X, v \in Y\} \qquad \square$$

Definition 45 (Notations)
Si $X \cap Y$, on dit que X et Y sont en somme directe et on ecrit

$$X \oplus Y \subset V$$

pour leur somme.Si

$$X \oplus Y = V$$

on dit que V est somme directe de X et Y.

Proposition 75
Soit X et Y en somme directe. Soit $W = X \oplus Y$, alors $w \in W$ s'écrit comme combinaison linéaire unique de $x \in X$ et $y \in Y$

Preuve
Supposons $w = x + y = x' + y'$, alors

$$\begin{aligned} &\Rightarrow x + y = x' + y' \\ &\Rightarrow X \ni x - x' = y' - y \in Y \end{aligned}$$

Donc $x - x' = y' - y = 0$ □

Definition 46 (Famille génératrice)
Soit V un K-ev. Un sous-ensemble $\mathcal{F} \in V$ est une famille génératrice si

$$Vect(\mathcal{F}) = V$$

ie. tout élément $v \in V$ peut s'écrire sous la forme d' une combinaison linéaire

$$v = \sum_{i=1}^{n} x_i e_i$$

Definition 47 (Espace vectoriel fini)
Un K-espace vectoriel non-nul est dit de dimension finie si il est de type fini comme K-module : si il exist un ensemble $\mathcal{F}$ fini tel que

$$V = Vect(\mathcal{F})$$

La dimension de V est définie comme le minimum du cardinal de toutes les familles génératrices finies de V

$$\dim_K(V) = \min_{\mathcal{F}\ génératrice} |\mathcal{F}|$$

Par convention, la dimension de l'espace vectoriel nul $\{0_V\}$ est

$$\dim_K(\{0_K\}) = 0$$

On peut prendre la famille vide comme famille génératrice

Theorème 76
Tout K-espace vectoriel de dimension finie est linre,c'est a dire isomorphe a K^d pour un certain $d \geq 0$

Remarque
$d = \dim_K(V)$

Remarque
On verra à la fin ce qui arrive aux espaces vectoriels qui ne sont pas de dimension finie.

Lecture 11: Espaces Vectoriels 2

Tue 20 Oct

Soit V un K-ev de dimension finie et $G = \{e_1, \cdots, e_n\}$ une famille de vecteurs.

$$CL_G : K^d \to V$$
$$(x_1, \cdots, x_d) \to x_1.e_1 + x_2e_2 + \cdots + x_de_d$$

CL_G est linéaire, suit du critere de combinaison linéaire.
Dire que G est génératrice $\iff$ CL_G est surjective, donc que $CL_G(K^d) = V$.

7.2 Famille Libre

Definition 48 (Famille Libre)
Soit $\mathcal{F} = \{e_1, \ldots, e_d\} \subset V$ et définissons

$$CL_{\mathcal{F}} : K^d \mapsto V$$

une application pas forcément surjective.
Si cette application est injective, alors la famille $\mathcal{F}$ est libre.

Comme $CL_{\mathcal{F}}$ est linéaire, $CL_{\mathcal{F}}$ est injective si et seulement si

$$\ker CL_{\mathcal{F}} = \{0_V\}$$

Donc $\overrightarrow{x} = (x_1, \ldots, x_n)$ ssi

$$\sum_i x_i e_i = 0$$

Definition 49
Un sous-ensemble fini $\mathcal{F} = \{e_1, \ldots, e_d\} \subset V$ d'un espace vectoriel forme une famille libre de V si et seulement si pour tous $x_1, \ldots, x_d \in K$

$$\sum_i x_i e_i = 0_V \implies x_1 = \cdots = x_d = 0$$

Une famille $\mathcal{F}$ qui n'est pas libre est dite liée.

Proposition 79
Une famille à d éléments $\mathcal{F} = \{e_1, \cdots, e_d\} \subset V$ est liée si et seulement si il existe $i \in \{1, \cdots, d\}$ tel que e_i peut s'exprimer comme combinaison linéaire des autres éléments de $\mathcal{F}$

$$e_i \in CL(\mathcal{F} \setminus \{e_i\}) = CL\,(e_j, j \neq i)$$

Preuve
Supposons $\mathcal{F}$ est liée, il existe $(x_1, \cdots, x_d) \neq 0_V$ tel que

$$x_1 e_1 + \cdots + x_d e_d = 0_V$$

un des $x_i \neq 0_K$ on peut suposer sans perte de géneralité que $x_d \neq 0$, donc

$$-x_d e_d = x_1 e_1 + \cdots + x_{d-1} e_{d-1}$$

Or $x_d \neq 0$ donc innversible, on obtient donc

$$x(x_d)^{-1} \in K \setminus \{0\}$$

Donc

$$e_d = \frac{x_1}{-x_d} e_1 + \cdots + \frac{x_{d-1}}{-x_d} e_d$$

Si $e_d \in CL\,(\{e_1, \cdots, e_{d-1}\})$, avec avec

$$e_d = y_1 e_1 + \cdots + y_{d-1} e_{d-1}, y_i \in K$$

Donc

$$0_V = y_1 e_1 + \cdots + y_{d-1} e_{d-1} - e_d \neq 0$$

□

Theorème 80
Soit V un espace vectoriel non-nul de dimension d et $\mathcal{F} = \{v_1, \cdots, v_f\} \subset V$ une famille finie et libre, alors $f \leq d$

Preuve
Par récurrence sur d.
Supposons que l'espace est engendré par un élément K.

$$d = 1 \quad V = K.e, \quad e \neq 0$$

Montrons que $\mathcal{F} = \{v_1, \cdots, v_f\} \subset V = K.e$ avec $v_i = x_i.e \quad f \geq 2$ Comme $v_1 \neq v_2, x_1.e = v_1, x_2.e = v_2$, alors x_1 ou $x_2 \neq 0_k$.
Supposons $x_1 \neq 0$, alors $v_2 = x_2.e = \frac{x_2}{x_1}.x_1.e$
Alors $\mathcal{F}$ est liée car v_2 est cl de v_1.
Dimesions $\dim V = d \geq 2$ et on suppose le résultat démontré en dimension

$\leq d-1$.
Soit $\mathcal{F} = \{v_1, \cdots, v_f\} \subset V$ *avec* $f \geq d+1$, *on veut montrer que* $\mathcal{F}$ *est liée.*
Soit $G = \{e_1, \cdots, e_d\}$ *une famille génératrice de* V *pour* $i = 1, \cdots, f$

$$v_i = x_{i,1}e_1 + \cdots + x_{i,d}e_d$$

avec $x_{i,j}j \leq d$ *dans* K.
Comme $f > d \geq 1$, *il existe* $x_{i,j} \neq 0_K$.
Quitte à permuter les e_j *et les* v_i *on peut supposer que*

$$x_{f,d} \neq 0_K$$

On pose : $i \leq f$

$$v'_i := v_i - \left(\frac{x_{i,d}}{x_{f,d}}.v_f\right)$$

Si $i = f \quad v'_f = v_f - \frac{x_{f,d}}{x_{f,d}}v_f = 0_V$.
Posons

$$v'_i = x'_{i,1}e_1 + \cdots + x'_{i,d-1}e_{d-1} + (x_{i,d} - \frac{x_{i,d}}{x_{f,d}}x_{f,d})e_d$$

On a construit $f-1$ *vecteurs* $\mathcal{F}' = \left\{v'_1, v'_2, \cdots, v'_{f-1}\right\}$ *qui sont contenus dans l'espace vectoriel*

$$V' = CL(\{e_1, \cdots, e_{d-1}\}) \subset V$$

Or

$$\dim V' \geq d-1 \text{ comme } f-1 > d-1$$

la famille $\mathcal{F}'$ *est liée par hypothèse de récurrence.*
Donc l'un des v'_i *est CL des autres* $v'_{i'} i' \neq i$, *On peut supposer que c'est* v'_1

$$v'_1 = y_2v'_2 + \cdots + y_{f-1}v'_{f-1}$$

Or

$$v'_1 = v_1 - \frac{x_{1,d}}{x_{f,d}}v_f = y_2(v_2 - ()v_f) + \cdots + y_{d-1}(v_{d-1} - ().v_f)$$

Donc

$$v_1 = y_2(v_2 - ()v_f) + \cdots + y_{d-1}(v_{d-1} - ()v_f) + \frac{x_{1d}}{x_{f,d}}v_f$$ □

Donc v_1 *est cl de* $v_2, \cdots, v_f$, *donc* $\mathcal{F}$ *est liée.*

Corollaire 81
$\dim K^d = d$

Preuve
On sait que pour K^d, *la base canonique*

$$B_d^0 = \left\{e_1^0, \cdots, e_d^0\right\}$$

est génératrice, donc $\dim K^d \leq d$.
Est libre : $d \leq \dim K^d$ □

7.3 Bases

Definition 50

Soit V un espace vectoriel de dimnesion finie. Une famille $\mathcal{B} = \{e_1, \cdots, e_d\}$ est une base de V si l'une des contions equivalentes suivantes est vérifiée :

1. *$\mathcal{B}$ est génératrice et libre*
2. *L'application combinaison linéaire de $\mathcal{B}$*

$$CL_{\mathcal{B}} : K^d \to V$$

   est un isomorphisme.

3. *Pour tout $v \in V$ il existe un unique uplet $(x_1, \cdots, x_d) \in K^d$ tel que v s'écrit sous la forme*

$$v = x_1 e_1 + \cdots + x_d e_d$$

Remarque

$$|\mathcal{B}| = \dim V$$

Une base à travers l'isomorphisme $CL_{\mathcal{B}}$ permet d'identifier un espace vectoriel abstrait V avec un espace vectoriel concret K^d.

Theorème 83

Soit V un K-espace vectoriel de dimension $d = \dim V \geq 1$ alors V possède une base $\mathcal{B}$ et on a donc un isomorphisme de K-ev

$$V \simeq K^d$$

Plus précisément

1. *Soit $\mathcal{K} \subset V$ une famille génératrice alors $\mathcal{K}$ contient une base de V. Si de plus $|\mathcal{K}| = d$, alors $\mathcal{K}$ est une base.*
2. *Si $\mathcal{L} \subset V$ est lire alors $\mathcal{L}$ est contenue dans une base de V. Si $|\mathcal{L}| = d$, alors $\mathcal{L}$ est une base.*

Preuve

Soit G une famille génératrice

$$|G| = d' \geq d = \dim V$$

Soit $B \subset G$ une famille génératrice de G de taille minimale parmi les familles génératrices contenues dans G.
$\mathcal{B}$ est libre (et est donc une base)

$$G = \{e_1, \cdots e_n\}$$

Supposons que $\mathcal{B}$ est liée, alors il existe $e_{|B|}$ qui est cl de $\{e_1, \cdots e_{|B|-1}\}$
Mais alors

$$V = CL(\mathcal{B}) = CL(\{e_1, \cdots, e_{|B|}\})$$

mais comme $e_{|B|}$ est cl de $\{e_1, \cdots e_{|B|-1}\}$

$$CL(\{e_1, \cdots, e_{|B|-1}\}) \supset \{e_1, \cdots, e_{|B|-1}, e_{|B|}\} \qquad \square$$

Ca contredit la minimalité de $\mathcal{B}$. Donc $\mathcal{B}$ est libre et c'est une base.

Lecture 12: Espaces Vectoriels 3

Mon 26 Oct

Continuation de la preuve de 83

Preuve
Soit $\alpha \subset V$ libre. Soit $\mathcal{B} \subset V$ une base.
Alors $\alpha \cup \mathcal{B}$ est génératrice et contient α.
Soit $\mathcal{B}'$ une famille génératrice contenant α et contenue dans $\alpha \cup \mathcal{B}$, de taille minimale.
On va montrer que $\mathcal{B}'$ est libre et que ce sera une base contenant α (et même contenue dans $\alpha \cup \mathcal{B}$)
Si $\alpha = \mathcal{B}'$, on a fini : $|\alpha| = |\mathcal{B}'|$ et α est une base.
Quitte à renuméroter $\mathcal{B}'$ on peut supposer que

$$\mathcal{B}' = \left\{ \underbrace{e_1, \ldots, e_{|\alpha|}}_{\in \alpha}, e_{|\alpha|+1}, \ldots \right\}$$

Soient $x_1, \ldots, x'_d \in K$ tel que

$$x_1 e_1 + x_2 e_2 + \ldots + x_{|\alpha|} e_{|\alpha|} + e_d x_d = 0_V$$

Si tous les $x_{|\alpha|+i} = 0$ pour $i \geq 1$, alors on a

$$0_V = x_1 e_1 + \ldots + e_{|\alpha|} x_{|\alpha|}$$

Mais comme α est libre $\Rightarrow$

$$x_1 = \ldots = x_{|\alpha|} = 0_K$$

Si il existe $x_{|\alpha|+i} i \geq 1$ qui est non nul, alors

$$e_{|\alpha|+1} = \frac{x_1}{-x_{|\alpha|+i}} e_1 + \ldots + \frac{x_{|\alpha|}}{x_{|\alpha|+i}} e_{|\alpha|} + \ldots$$

Ce qui implique que V est engendré par $\{e_1, \ldots, e_{|\alpha|}\} \setminus e_{|\alpha|+i}$ Ce qui contredit la minimalité de la famille génératrice $\mathcal{B}'$ parce que

$$\mathcal{B}' - \{e_{|\alpha|+i}\} \qquad \square$$

est génératrice et contient α

Theorème 84 (Dimension de SEV)
Soit V un espace vectoriel de dimension finie, et $W \subset V$ un sous-espace vectoriel alors

1. *W est de dimension finie et $\dim W \leq \dim V$*
2. *Si $\mathcal{B}_W$ est une base de W, alors il existe une base $\mathcal{B}_V$ de contenant $\mathcal{B}_W$*
3. *Si $\dim W = \dim V$, alors $W = V$*

Preuve
Si $W = \{0_V\}$, on a fini
Sinon, si $W \neq \{0_V\}$, alors W contient une famille non-vide α qui est libre.
Soit $\alpha \subset W$ libre et de cardinal maximal (parmi les familles libres) On va montrer que α est génératrice de W (et α sera une base de W) .
Si α n'est pas génératrice, il existe $e \in W \setminus \langle \alpha \rangle$.
Ce qui implique que e n'est pas combinaison linéaire des éléments de $\alpha \Rightarrow \alpha \cup \{e\}$ est libre, et elle est contenue dans W, ce qui contredit la maximalité de $|\alpha|$.
Donc W est de dimension finie, $\dim W = |\alpha| \leq \dim V$
Si $|\alpha| = \dim V$, α est libre dans V et de taille $\dim V$.
Donc α est une base de V, et donc $W = V$ □

7.4 Espaces vectoriels de dimension infinie

Exemple

— $\mathcal{F}(\mathbb{R}, \mathbb{R}) = \mathbb{R}^{\mathbb{R}}$ *n'est pas de dimension finie*
— $\mathcal{C}(\mathbb{R}, \mathbb{R})$ *fonctions continues*
— $\mathbb{R}[x]$ *fonctions polynomiales sur $\mathbb{R}$ n'ont pas de dimension finie*

Definition 51
Soit V un K-ev. Un sous-ensemble $G \subset V$ est une famille génératrice si

$$Vect(G) = V$$

ie. tout élément $v \in V$ peut s'écrire sous la forme d'une combinaison linéaire finie d'éléments de G il existe $e_1, \dots e_D \in G$, $x_1, \dots x_d \in K$ tq

$$v = x_1 e_1 + \ldots + x_d e_d$$

Definition 52
Soit V un $K-$ ev, un sous-ensemble $\mathcal{L} \subset V$ est une famille libre si tout sous-ensemble fini $\mathcal{L}' \subset \mathcal{L}$ est libre : $\forall d \geq 1$ et tout $\{e_1, \dots, e_d\} \subset \mathcal{L}$, on a

$$x_1 e_1 + \ldots + x_d e_d = 0_V \iff x_1 = \ldots = x_d = 0_k$$

Definition 53
Une base $\mathcal{B} \subset V$ est une famille libre et génératrice : tout élément de v est représentable comme combinaison linéaire finie d'éléments de $\mathcal{B}$

Theorème 86
Dans une théorie des ensembles contenant l'axiome du choix, tout espace vectoriel possède une base et toutes les bases de V ont le même cardinal : pour toutes bases $\mathcal{B}, \mathcal{B}'$, il exists une bijection

$$\mathcal{B} \simeq \mathcal{B}'$$

La dimension de V est de cardinal d'une base

$$\dim V = |\mathcal{B}|$$

Lemme 87 (Lemme de Zorn)
Soit E un ensemble ordonné tel que tout sous-ensemble $A \subset E$ totalement ordonné possède un majorant alors E possède un élément maximal.

Proposition 88
Soit $\phi : V \to W$ une application linéaire avec V de dimension finie. Soit $G = \{e_1, \ldots, e_g\} \subset V$ une famille génératrice, alors

$$\phi(G) = \{\phi(e_1), \ldots, \phi(e_g)\} \subset W$$

est une famille génératrice de $Im(\phi)$ et on a

$$\dim Im\phi \leq \dim V$$

Definition 54
Soit $\phi : V \to W$ une application linéaire. Le rang de ϕ est la dimension de $Im\phi$:

$$rg(\phi) = \dim Im\phi$$

Preuve
Soit $G = \{e_1, \ldots, e_g\} \subset V$ génératrice et soit

$$\phi(G) = \{\phi(e_1), \ldots, \phi(e_g)\} \subset W$$

Soit $w \in Im\phi$ on veut montrer que w est $CL(\phi(G))$.
Comme $w \in Im\phi$, $w = \phi(v), v \in V$ et comme G est génératrice de V

$$v = x_1 e_1 + \ldots + x_g e_G, \quad x_i \in K$$

Donc

$$w = \phi(v) = x_1\phi(e_1) + \ldots + x_g\phi(e_g)$$

Soit $G = B$ une base, alors

$$|B| = \dim V$$

et

$$\dim Im\phi(V) \leq |phi(B)| \leq |B| \qquad \square$$

Corollaire 89
Une application linéaire envoyant une base sur une base est un isomorphisme

Preuve
$\phi : V \to W$
B une base de ϕ *et on suppose que*

$$\phi(B) = \{\phi(e_1), \ldots, \phi(e_d)\} = \text{ Base de } W$$

Alors $\phi : V \simeq W$.
ϕ *est surjective car* $\phi(B)$ *engendre l'image de* ϕ *et comme* $\phi(B)$ *est ube base de* W

$$\langle \phi(B) \rangle = Im\phi = W$$

ϕ *est injective : Soit* $v \in \ker \phi$

$$v = x_1 e_1 + \ldots + x_d e_d$$

$\phi(v) = 0 = x_1\phi(e_1) + \ldots + x_d\phi(e_d)$
Mais car $\{\phi(e_1), \ldots, \phi(e_d)\}$ *est libre dans* W.
Donc $x_1 = \ldots = x_d = 0 \Rightarrow v = 0$ $\square$

Theorème 90 (Le théorème noyau-image)
Soit $\phi : V \mapsto W$ *une application linéaire avec* V *de dimension finie. On a*

$$\dim V = \dim \ker \phi + \dim Im\phi$$

Preuve
Soit $\{e_1, \ldots, e_k\}$ *une base de* $\ker \phi$ *(* $k \leq \dim V$*)*
Soit $\{f_1, \ldots, f_r\}$ *une base de* $Im\phi$ *(* $r \leq \dim V$*) , alors*

$$f_1 = \phi(e'_1), \ldots, f_r = \phi(e'_r) \text{ avec } e'_j \in V$$

On va montrer que

$$\{e_1, \ldots, e_k, e'_1, \ldots, e'_r\} \subset V$$

c'est une base de V. *Alors*

$$\dim V = |\{...\}| = k + r$$

Montrons que la famille est libre :
Soit $x_1, \ldots, x_k, x'_1, \ldots, x'_r \in K$ *tel que*

$$x_1 e_1 + \ldots + x'_r e'_r = 0_V$$

On a

$$\begin{aligned}\phi(0_V) = \phi(x_1e_1 + \ldots + x'_re'_r) = 0_W \\ = x_1\phi(e_1) + \ldots x'_re'_r \\ = x'_1f_1 + \ldots + x'_rf_r \Rightarrow x'_1 = \ldots x'_r = 0\end{aligned}$$

Il reste

$$0_V = x_1e_1 + \ldots + x_ke_k$$

Donc $\{e_1, \ldots, e_k\}$ *est linre* $\Rightarrow \quad x_1 = \ldots = x_k = 0_K$
Montrons que $\{e_1, \ldots, e_k, e'_1, \ldots, e'_r\}$ *est génératrice.*
Soit $v \in V$ *on veut montrer que* v *est cl de la famille.*

$$\begin{aligned}\phi(v) = \underbrace{w}_{\in Im\phi} = x'_1f_1 + \ldots x'_rf_r \\ = x'_1\phi(e'_1) + \ldots + x'_r\phi(e'_r) \\ = \phi(x'_1e'_1 + \ldots + x'_re'_r)\end{aligned}$$

Donc $\phi(v) = \phi(v')$, *or*

$$v - v' \in \ker\phi \text{ car } \phi(v - v') = \phi(v) - \phi(v') = 0_W$$

Donc

$$\begin{aligned}v - v' = x_1e_1 + \ldots + x_ke_k \\ \text{donc} \\ = x_1e_1 + \ldots + x_ke_k + x'_1e'_1 + \ldots + x'_re'_r\end{aligned}$$

□

Lecture 13: Applications lineaires

Tue 27 Oct

Corollaire 91
Soit $\phi : V \to W$ *une application lineaire entre espaces de dimension finie*
- *Si* ϕ *est injective et* $\dim W = \dim V$, *alors* ϕ *est bijective*
- *Si* ϕ *est surjective et* $\dim W = \dim V$, *alors* ϕ *est bijective*

Preuve
Si ϕ *est injective, alors* $\ker\phi = \{0_V\}$, *et donc*

$$\dim V = \dim\ker\phi + \dim Im\phi = \dim Im\phi = \dim W$$

De même, si ϕ *surjective, alors*

$$Im\phi = W \text{ et donc } \dim Im\phi = \dim W$$

Donc on a

$$\dim W = \dim V = \dim\ker\phi + \dim W$$

□

Donc $\dim\ker\phi = 0$ *et donc* ϕ *est innjective* $\Rightarrow$ *bijective.*

Corollaire 92
Deux espaces vectoriels de dimension finie sont isomorphes si et seulement si ils ont meme dimension

Preuve
Soit V et W de même dimension $=d$.
En choisissant B une base de V et B' de W
On a les isomorphismes

$$CL_B : K^d \simeq V \text{ et } CL_{B'} \simeq W$$

Donc V et W sont isomorphes.
Si $V \simeq W$, alors $\ker\phi = \{0_V\}$ et $Im\phi = W$, on a alors

$$\dim V = \dim\ker\phi + \dim Im\phi = 0 + \dim W \qquad \square$$

7.5 Formes linéaires

$$l : V \to K$$

On rappelle que si $l \neq \underline{0}_k$, alors l est surjective $l(V) = K$.

$$\dim V = \dim\ker l + \dim K = \dim\ker l + 1$$

Donc, si $l : V \to L, l \neq \underline{0}_K$, alors $\dim\ker l = \dim V - 1$, alors $\ker l$ est un hyperplan vectoriel de V.

7.6 Espaces d'applications linéaires

Soient V, W de dim $< \infty$, alors

$$Hom_{K-ev}(V, W) \text{ a une structure de } K - ev$$

donné par

$$(\phi + \psi)(v) = \phi(v) + \psi(v)$$

et que

$$\lambda \in K \quad (\lambda.\phi)(v) = \lambda(\phi(v))$$

Theorème 93
Si V et W sont de dimension finie, alors $Hom_K(V, W)$ est de dimension fini

$$\dim(Hom_K(V, W)) = \dim V.\dim W$$

Preuve
On va montrer que

$$Hom(V,W) \simeq W^{\dim V}$$

Soit $B = \{e_1, \ldots, e_d\}$ *une base de* V

$$eval_B : Hom(V,W) \to W^{\dim V}$$
$$\phi \to (\phi(e_1), \phi(e_2), \ldots, \phi(e_d))$$

On va montrer que $eval_B$ *est un isomorphisme d'espaces vectoriels.*
$eval_B$ *est linéaire :*

$$eval_B(\lambda\phi + \psi) = (\lambda\phi(e_1) + \psi(e_1), \ldots, \lambda\phi(e_d) + \psi(e_d)) = \lambda eval_B(\phi) + eval_B(\psi)$$

Montrons que $eval_B$ *est injective, si*

$$eval_B(\phi) = (0_W, \ldots, 0_W)$$

Implique

$$\forall v \in V \quad v = x_1e_1 + \ldots + x_de_d$$

Donc

$$\phi(v) = x_1\phi(e_1) + \ldots + x_d\phi(e_d) = 0_W$$

Donc ϕ *injectif.*
Soit $(w_1, \ldots, w_d) \in W^{\dim V}$ *et soit* ϕ *l'application définie pour tout* $v \in V$ *par*

$$\phi(v) = x_1w_1 + \ldots + x_dw_d$$

si $v = x_1e_1 + \ldots + x_de_d$.
C'est bien défini car B *est une base de* V *et la combinaison linéaire qui représente* V *est unique.*
Alors ϕ *est linéaire et*

$$\phi(e_i) = w_i \quad i = 1 \ldots d$$

Donc $eval_B$ *est surjective et donc bijective* □

Remarque

$$eval_B : Hom(V,W) \simeq W^{\dim V}$$

dépend du choix de B.

Remarque
Si on choisit B' *une base de* W,

$$W \simeq K^{d'}$$

et donc on obtient un isomorphisme

$$Hom_K(V,W) = (K^{d'})^d$$

7.7 Formes linéaires et dualité

Definition 55

On note l'espace des formes linéaires $l : V \to K$

$$V^* = Hom(V, K)$$

et on l'appelle le dual de V
Comme $\dim K = 1$*, on a*

$$\dim(V^*) = \dim Hom(V, K) = \dim V$$

En particulier un espace vectoriel V *et son dual sont isomorphes. Plus précisément, soit*

$$B = \{e_1, \ldots, e_d\}$$

une base de V*, on a alors un isomorphisme*

$$eval_B : l \to (l(e_1), \ldots, l(e_d)) \in K^d$$

Definition 56

Soit B *une base de* V*, la base duale de* B*,* $B^* \subset V^*$ *est l'image réciproque de la base canonique* $B_d^0 = \left\{e_i^0, i \leq d\right\} \subset K^d$ *par l'application* $eval_B$*. On pose*

$$e_i^* = eval_B^{-1}(e_i^0)$$

De sorte que

$$B^* = \{e_i^*, i \leq d\}$$

et c'est une base (car image d'une base par un isomorphisme) .

Proposition 96

Soit $B = \{e_1, \ldots, , e_d\} \subset V$ *et* $B^* = \{e_1^*, \ldots e_d^* \subset V^*\}$ *la base duale. On a*

$$\forall i, j \leq d, \quad e_i^*(e_j) = \delta_{ij}$$

Preuve

Calculons $e_1^* = eval_B^{-1}((1, 0, 0 \ldots))$
Donc

$$eval_B(e_1^* = (1, 0, 0 \ldots)) = (e_1^*(e_1), \ldots)$$ □

idem pour e_i^**.*

Remarque

L'application $eval_B$ *donne*

$$V^* \simeq K^d \simeq V$$

Donc l'isomorphisme composé $V^* \simeq V$ *est celui qui envoie* e_i *sur* e_i^**.*
Cet isomorphisme dépend du choix de B*(pas canonique) .*

Definition 57 (Application linéaire duale)
Soit $\phi : V \to W$ à partie de ϕ, on construit (canoniquement) une application

$$\phi^* : W^* \to V^* \text{ (application linéaire duale de } \phi)$$

Soit $l' \in W^* \to \phi^*(l')$ donné par

$$\phi^*(l')(v) = l'(\phi(v)) = ' \circ \phi$$

ϕ^* est linéaire et

$$\bullet^* : \phi \in Hom(V,W) \to \phi^* \in Hom(W^*, V^*)$$

est linéaire.

7.8 Représentation paramétrique d'unn sev cartesienne

$W \subset V$, Soit $\{e_1, \ldots, e_{d'}\}$ une base de W, alors tout vecteur de W s'écrit

$$w = x_1 e_1 + \ldots + x_{d'} e_{d'}$$

Alors

$$W = \{w = x_1 e_1 + \ldots\}$$

On a alors une représentation paramétrique de tout vecteur

$$w \in W, \quad w = x_1 e_1 + \ldots + x_{d'} e_{d'}$$

de paramètre $x_1, \ldots, x_{d'}$.
Note : Il n'est pas nécessaire que $\{e_1, \ldots e_{d'}\}$ soit une base, il suffit que ce soit une famille génératricre de W.

Représentation cartésienne

Proposition 98
Soit $W \subset V$ un sev. Il existe $d_V - d_W$ formes linéaires

$$\mathcal{L}_W^* = \{l_1, \ldots, l_{d_v - d_W}\} \subset V^*$$

linéairement indépendantes (ie tq $\mathcal{L}_W^*$ soit libre) telles que

$$W = \{v \in V, l_1(v) = \ldots = l_{d_v - d_w}(v) = 0\}$$

De maniere equivalente, $W = \ker \phi_{\mathcal{L}_W^*}$ avec

$$\phi_{\mathcal{L}_W^*} : v \in V \to (l_1(v), \ldots, l_{d_v - d_W}(v)) \in K^{d_v - d_w}$$

Preuve
Soit $W \subset V$ et soit $\{e_1, \ldots, e_{d'}\}$ une base de W.
Il existe $e_{d'+1}, \ldots, e_d \in V$ tel que

$$\{e_1, \ldots e_d\}$$

forme une base de V.
W est l'ensemble des vecteurs V dont les coordonnées suivant les vecteurs $e_{d'+1}, \ldots e_d$ sont nulles.

$$v = x_1 e_1 + \ldots x_{d'} e_{d'} + \ldots + x_d e_d$$

Donc

$$W = \left\{ v \in V | e^*_{d'++1}(v) = \ldots = e^*_d(v) = 0_K \right\} \qquad \square$$

7.9 Une base de $Hom_k(V, W)$

Soit $B = \{e_1, \ldots, e_d\} \subset V$ et $B*$ la base duale

$$B' = \{f_1, \ldots, f_{d'}\} \, | i \leq d' = \dim W \quad j \leq d = \dim V$$

Alors

$$e_{ij} : V \to W$$
$$v \to e^*_j(v).f_i$$

On dispose de $d.d'$ applications e_{ij}

Lemme 99
L'application $e_{ij} : V \to W$ est linéaire, de rang 1, d'image $K.f_i$ et de noyau

$$\ker e_{ij} = \langle () \, B - \{e_j\})$$

L'hyperplan vectoriel engendré par les vecteurs de la base B moins le vecteur e_j

Preuve
e_{ij} est linéaire car

$$e^*_j : V \to K$$

est linéaire.
Vérification simple avec critère.

On a

$$Im(e_{ij}) = Im(e^*_j).f_i = K.f_i$$

de dimension 1.

$$\ker e_{ij} = \left\{ v \in V \text{ tel que } e^*_j(v).f_i = 0_W \right\}$$

mais comme $f_i \neq 0_W$ (car f_i fait partie d'une base).

$$e_j^*(v).f_i = 0_w$$

si et seulement si

$$e_j^* = 0_K$$

Donc

$$\ker e_{ij} = \left\{v \in V \text{ tel que } e_j^*(v) = 0_K\right\}$$ □

Theorème 100
La famille d'applications linéaires

$$B_{B,B'} = \{e_{ij}, i \leq d', j \leq d\} \subset Hom(V,W)$$

forme une base de $Hom(V,W)$

Preuve
$B_{B,B'}$ est de taille $d.d' = \dim Hom(V,W)$ pour montrer que c'est une base, il suffit de montrer que $B_{B,B'}$ est libre.
Soient $m_{ij}, i \leq d', j \leq d$ des scalaires tel que

$$\sum_{i=1}^{d'} \sum_{j}^{d} m_{ij} e_{ij} = \underline{0}_W$$

On veut montrer que $m_{ij} = 0_K$.

$$\begin{aligned}
&\left(\sum_{i,j} m_{ij} e_{ij}\right)(e_k) \\
&= \sum_i \sum_j m_{ij} e_{ij}(e_k) \\
&= \sum_i \sum_j m_{ij} e_j^*(e_k).f_i \\
&= \sum_{i=1}^{d'} m_{ik} f_i = 0
\end{aligned}$$ □

Donc $m_{ik} = 0$ car les f_i forment une famille libre.

Proposition 101
Soit $\phi : V \to W$ une application linéaire et (m_{ij}) les coordonnées dans la base $B_{B,B'}$. Alors pour $k = 1, \ldots, d$ les

$$m_{i,k}$$

sont les coordonnées de $\phi(e_k)$ dans la base B'

Preuve
On a

$$\begin{aligned} e_{ij}(e_k) &= \sum_{i\leq d'}\sum_{j\leq d} m_{ij}e_j^*(e_k).f_i \\ &= \sum_{i\leq d'} m_{ik}.f_i \end{aligned}$$

Proposition 102
Avec les notations précédentes, si $v = \sum_{j=1}^{d} x_j e_j$, on a

$$\phi(v) = \sum_{i=1}^{d'} y_i f_i \text{ avec } y_i = \sum_{j\leq d} m_{ij}x_j$$

Preuve

$$\phi(v) = \phi(\sum_{k=1}^{d} x_k e_k) = \sum_{k=1}^{d} x_k\phi(e_k) = \sum_{k=1}^{d} x_k\phi(e_k) = \sum_{k=1}^{d} x_k \sum_{k\leq d'} m_{ik}f_k = \sum_{i\leq d'}\left(\sum_{k=1}^{d} m_{ik}x_k\right) f_i$$

et par définition

$$\sum_{i\leq d'} y_i f_i$$

□

Lecture 14: Applications Lineaires, Matrices

Mon 02 Nov

7.10 Composition d'applications linéaires

$$\phi : U \to V, \psi : V \to W \text{ et } \psi\circ\phi : U \to W$$

Soit

$$B = \{e_k, k \leq d\}, B' = \{f_j, j \leq d'\}, B'' = \{g_i, i \leq d''\}$$

et finalement

$$B_{B,B'} = \{e_k^*.f_j\}, B_{B',B''} = \left\{f_j^*.g_i\right\}, B_{B,B''} = \{e_k^*.g_i\}$$

Theorème 103
Soient $(n_{jk})_{j\leq d',k\leq d}$ les coordonn ;es de ϕ dans la base $B_{B,B'}$ et $(m_{ij})_{i\leq d'',j\leq d'}$ les coordonnees de ϕ dans la base $B_{B',B''}$. Alors les coordonnees $(l_{ik})_{i\leq d'',k\leq d}$de

$\psi \circ \phi$ dans la base $B_{B,B''}$ sont donnees par

$$l_{ik} = \sum_{j=1}^{d'} m_{ij}.n_{jk}$$

Preuve

$$\phi = \sum_{j \leq d'} \sum_{k \leq d} n_{jk} e_k^*.f_j$$

et

$$\psi = \sum_{j \leq d'} \sum_{i \leq d''} m_{ij} f_j^*.g_i$$

On veut calculer

$$\psi \circ \phi(e_k) = \sum_{i \leq d''} l_{ik} g_i$$

On voit que

$$\begin{aligned}
\phi(e_k) = \sum_{j \leq d'} \sum_{k' \leq d} n_{jk'} e_{k'}^*(e_k) f_j &= \sum_{j \leq d'} n_{jk} f_j \\
&= \psi(\phi(e_k)) = \psi(\sum_{j \leq d'} n_{jk} f_j) \\
&= \sum_{j \leq d'} n_{jk} \psi(f_j) \\
&= \sum_{j \leq d'} n_{jk} \sum_{i \leq d''} m_{ij} g_i \\
&= \sum_{i \leq d''} \left(\sum_{j \leq d'} n_{jk} m_{ij} \right) g_i \\
&= \sum_{i \leq d''} \left(\sum_{j \leq d'} m_{ij} n_j \right) g_i
\end{aligned}$$

8 Matrices

On a donc défini l'application linéaire

$$CL_{B_{B,B'}} : (m_{ij})_{i \leq d', j \leq d} \in K^{d'd} \mapsto \phi = \sum_{i \leq d'} \sum_{j \leq d} m_{ij} e_{ij} \in \hom(V, W)$$

Definition 58
Les systeme de coordonnées à 2 indices $i \leq d'$ et $j \leq d$ s' appellent des matrices. On le note

$$M_{d' \times d}(K) = \{(m_{ij})_{i \leq d', j \leq d}, m_{ij} \in K\}$$

Un element de $M_{d'\times d}(K)$ est appelé matrice de dimensions $d'\times d$ ou matrice $d'\times d$. On les notes sous forme de tableaux.

Definition 59
Soient $B\subset V$, $B'\subset W$ des bases comme ci-dessous et $B_{B,B'}\subset \hom(V,W)$ la base de $\hom(V,W)$ associee. L'application reciproque $Cl^{-1}_{B_{B,B'}}$ sera également notee

$$Mat_{B',B}:\hom(V,W)\to M_{d'\times d}(K)$$

Explicitement, si on a la décomposition $\phi == \sum_{i\leq d'}\sum_{j\leq d} m_{ij}e_{ij}$, alors on a

$$Mat_{B',B}(\phi)=(m_{ij}(\phi))_{i\leq d',j\leq d}=\begin{pmatrix} m_{11} & m_{12} & \dots m_{1d}\\ \vdots & \dots & \dots\\ m_{d'1} & m_{d'2} & \dots m_{d'd}\end{pmatrix}$$

L'espace $M_{d'\times d}(K)=(K^{d'})^d$ est un K-ev : on définit la somme de 2 matrices en sommant les coefficients :

$$(m_{ij})+(n_{ij})=(m_{ij}+n_{ij})_{\leq d',j\leq d}$$

On définit de la même manière la multiplication par les scalaires.

8.1 Produit de Matrices

On a introduit les matrices à partir d'applications linéaires.
On se souvient que le produit de deux matrices m_{ij} et n_{jk} est défini par

$$l_{ik}=\sum m_{ij}n_{jk}$$

Definition 60 (Multiplication Matricielle)
Soient $d,d',d''\geq 1$ et $M\in M_{d''\times d'}(K), N\in M_{d'\times d}(K)$, on définit le produit des matrices M et N comme étant la matrice

$$L=M.N=M\times N$$

avec

$$L=(l_{ik})_{i\leq d'',k\leq d}=(\sum_{j=1}^{d'} m_{ij}n_{jk})_{i\leq d'',k\leq d}\in M_{d''\times d}(K)$$

Theorème 104
Le produit de matrices ainsi défini a les propriétés suivantes

1. *Distributive à gauche : pour $\lambda\in K$, $M,M'\in M_{d''\times d'}(K)$*

$$(\lambda.M+M').N=\lambda.M.N+M'.N.$$

2.

3. *distributive à droite pour* $\lambda \in K,\ M, M' \in M_{d'' \times d'}(K)$

$$N.(\lambda.M + M') = \lambda.N.M + N.M'.$$

4. *Neutralité de l'identité : Pour* $M \in M_{d'' \times d'}(K), N, N' \in M_{d' \times d}(K)$

$$Id_{d''}.M = M$$

5. *La matrice nulle est absorbante : pour* $M \in M_{d'' \times d'}(K)$

$$0_{d''d'}.M = 0_{d''d'}$$

6. *Associativité*

$$(L.M).N = L.(M.N)$$

Preuve
Par le calcul direct. □

Lecture 15: Matrices

Tue 03 Nov

8.2 Rang d'une Matrice

On a déjà défini le rang d'une application linéaire.

Definition 61 (Rang d'une matrice)
Soit $M \in M_{d' \times d}(K)$.
Le rang de M

$rg(M) =$ *dimension de l'espace engendré par les colonnes de* M *dans l'espace* $Col_d(K)$

Proposition 105
Soit $\phi : V \to W$ *et* $M = mat_{B'B}\phi$, *alors*

$$rg(M) = rg(\phi) = \dim \phi(V)$$

Preuve
M *est formée de colonnes dont les coordonnées sont celle des* $\phi(e_j) j \leq d$ *dans la base* $B' = \{f_i, i \leq d'\}$. □

Remarque
Le rang de M *est* $\leq min(d, d')$.

$$\text{rang de } M = \text{ dimension d'un espace engendré par } d \text{ vecteurs}$$

Sa dimension sera toujours $\leq d$.
Cet espace est contenu dans $Col_{d'}(K)$ *qui est de* $\dim d'$

8.3 Transposition

Soient $\phi : V \to W$ et $\phi^* : W^* \to V^*$.

Theorème 107
Soit $(m_{ij}) = Mat_{B,B'}(\phi), (m^*_{ij}) = Mat_{B',B}(\phi^*)$. *Alors on a*

$$m_{ij} = m^*_{ji}$$

On dit que $mat(\phi^*)$ *est la transposée de* $mat(\phi)$ *et on la note* ${}^t mat(\phi)$

Definition 62
La transposition est l'application des matrices $d' \times d$ *vers les matrices* $d \times d'$ *définie par*

$${}^t\bullet : (m_{ij})_{i \leq d', j \leq d} \mapsto (m_{ji})_{j \leq d, i \leq d'}$$

Proposition 108
La transposition est

1. *Linéaire*
2. *Involutive :* ${}^t({}^t M) = M$
3. *Multiplicativité : pour deux matrices* M *et* N, *alors on a*

$${}^t(M.N) = {}^t N.{}^t M$$

Preuve
Il suffit de montrer que

$$\phi : U \mapsto V \quad \psi : V \to W$$

et

$$\psi \circ \phi : U \mapsto W$$

Alors

$$(\psi \circ \phi)^* = \phi^* \circ \psi^*$$

On a

$$(\psi \circ \phi)^* : l'' \to l'' \circ \psi \circ \phi = (l'' \circ \psi) \circ \phi = \phi^*(l'' \circ \psi) = \phi^*(\psi^*(l'')) \qquad \square$$

Proposition 109
Soit $M \in M_{d' \times d}(K)$ *on a*

$$rg(M) = rg({}^t M).$$

Soit $\varphi \in Hom(V,W)$, on a

$$rg(\phi) = rg(\phi^*)$$

Preuve

Soit une base $B = \{e_1, \ldots, e_d\} \subset V$, alors on a

$$\phi(B) = \{\phi(e_1), \ldots, \phi(e_d)\}$$

engendre $\phi(V)$ si $\dim \phi(V) = r = rg\phi$ oon peut extraire de $\phi(B)$ une base de $\phi(V)$.

Supposons que cette base soit

$$\{\phi(e_1) = f_1, \ldots, \phi(e_r) = f_r\} \subset W$$

C'est une famille libre de W.

On peut la compléter pour former une base de W :

$$B' = \{f_1, \ldots, f_r, f_{r+1}, \ldots, f_{d'}\}$$

On regarde

$$B' = \{f_1, \ldots, f_r, f_{r+1}, \ldots, f_{d'}\}$$

et on lui associe

$$B'^* = \{f_1^*, \ldots, f_d^*\}$$

On considère donc

$$\phi^* : W^* \to V^*$$

On a

$$rg\phi^* = \dim \phi^*(W^*) = \dim \langle \phi^*(f_1^*), \ldots \rangle$$

On va montrer que

$$\{\phi^*(f_1^*), \ldots\} \subset V^*$$

est libre.

Soient $x_1, \ldots, x_r \in K$ tel que

$$x_1\phi^*(f_1^*) + \ldots = 0_K$$

On a que $\forall j \leq d$ et $\forall e_j \in B$

$$\begin{aligned}&(x_1\phi^* + \ldots)(e_j)\\ &= x_1\phi^*(f_1^*)e_j + \ldots = x_j f_j^*(\phi(e_j)) = x_j f_j^*(f_j) = x_j\end{aligned}$$

Et donc

$$rg(\phi^*) \leq rg(\phi)$$

Donc pour toute matrice M, on a $rg({}^tM) \geq rg(M)$.
Donc en particulier

$$rg({}^t({}^t(M))) \geq rg({}^t(M))$$

Et donc

$$rg(M) = rg({}^tM)$$

Et donc

$$rg(\phi) = rg({}^*\phi)$$ □

8.4 Les matrices carrées

On note

$$M_d(K) = M_{d\times d}(K)$$

On remarque que la multiplication des matrices induit sur les matrices carrées de taille d une loi de composition interne.
Cette loi est

- distributive
- associative
- Id_d est neutrre pour la multiplication
- $0_d = 0_{d\times d}$ est absorbante

Donc

$$(M_d(K), +, \cdot)$$

est un anneau non-commutatif.
Et de plus comme $M_d(K)$ est un K-ev, donc

$$M_d(K)$$

est une K-algebre.
Soit V de $\dim d$, B = base et $B' = B$ une base

$$End(V) = Hom(V, W) \to M_d(K)$$
$$\phi \to mat_{B,B}(\phi)$$

$mat_{B,B}(\bullet)$ est un isomorphisme de K-ev mais c'est également un isomorphisme d'anneaux.
On a

$$mat_{B,B}(\psi \circ \phi) = mat_{B,B}(\psi) \cdot mat_{BB}(\phi)$$

Lecture 16: lundi

Mon 09 Nov

Theorème 110
L'espace $M_d(K)$ muni de l'addition des matrices et de la multiplication est un anneau (non-commutatif en general) dont l'element neutre est la

matrice carree nulle $0_d = 0_{d\times d}$ *et dont l'unite est la matrice identite* Id_d

Theorème 111
Soit V *de dimension finie* d *et* B *une base de* V*, l'application*

$$Mat_B : End(V) \mapsto M_d(K)$$

est un isomorphisme d'anneaux (et donc de K*-algebres) pour les lois d'addition et de multiplication decrites precedemment.*

De plus, on a que

$$^t\bullet : M_d(K) \mapsto M_d(K)$$

est un endomorphisme.

8.5 Le groupe lineaire

$End(V)^\times = \{\phi \in End(V)$ qui sont bijectifs et donc inversible pour la composition $\}$

On note

$$M_d(K)^\times = GL_d(K) = \text{ le groupe lineaire de } K^d$$

Donc

$$\begin{aligned} mat_B : GL(V) &\mapsto GL_d(K) \\ \phi &\mapsto mat_B(\phi) \end{aligned}$$

Proposition 112 (Critere d'inversibilite)
Pour qu'une matrice carree $M = (m_{ij})_{i,j\leq d} \in M_d(K)$*soit inversible il faut et il suffit que la famille des collonnes* $Col(M)$ *forme une famille libre.*

Preuve
Si $M = mat_B(\phi)\phi \in End(V)$.
Si $Col(M)$ *est une famille libre, l'ensemble des images des elements de* B *forme une famille libre, elle est de taille* d*, donc elle est generatrice.*
Donc ϕ *est surjective et injective.* □

Remarque
Dans ce critere, il est equivalent de regarder la famille des lignes.

Proposition 114
La transposition est une bijection de $GL_d(K)$ sur lui-meme qui verifie

$$\forall M, N \in GL_d(K) {}^tM^{-1} = {}^t\ M^{-1}, {}^t\,(M.N) = {}^t\ N.{}^tM$$

Preuve
Si M est inversible

$$\exists N = M^{-1}$$

tel que

$$M.M^{-1} = Id \quad M^{-1}M = Id$$ □

On utilise la formule de transposition sur $M.M^{-1}$

8.6 Changement de Base

Soient $B \subset V$ et $B' \subset W$ et $\phi : V \to W$.
A nouveau, supposons que $B_n \subset V$ et $B'_n \subset W$, avec

$$\phi \to mat_{B'_n B_n}(\phi) = M_n$$

Quelle est la relation entre M et M_n.

Proposition 115 (Formule de changement de base)
Soient $B, B_n \subset V$ et $B', B'_n \subset W$ des bases de V et W. On a la relation

$$Mat_{B'_n B_n}(\phi) = Mat_{B'_n B'}(\underset{w}{\mathrm{Id}}) Mat_{B'B}(\phi).Mat_{B,B_n}(\underset{v}{\mathrm{Id}})$$

Preuve
On a

$$\phi = \underset{w}{\mathrm{Id}} \circ \phi \circ \underset{v}{\mathrm{Id}}$$

On utilise le calcul des matrices associee a des compositions d'applications lineaires dans ces bases convenables.
On a

$$\phi : V \to V \to W$$

avec

$$mat_{B'B'}(\phi \circ \underset{v}{\mathrm{Id}}) = mat_{B'B}(\phi) mat_{BB_n}(\phi)$$ □

Definition 63 (Matrice de Passage)

$M_{BB_n} = M_{BB_n}(\underset{v}{\mathrm{Id}}) =$ *la matrice exprimant les coordonnees de* $\left\{\underset{v}{\mathrm{Id}}(e_n j \leq d)\right\} = B_n$ *exprimes dans la base B.*

Remarque
Les M_{BB_n} sont inversibles.

Proposition 117
Soit trois bases $B, B_1, B_2 \subset V$, on a

1. *Formule d'inversion*

$$Mat_{BB_1} Mat_{BB_1} = \underset{d}{\mathrm{Id}}$$

En particulier une matrice de passage est inversible (dans $M_d(K)$) et son inverse est la matrice de passage de la base initiale a la nouvelle base

2. *Formule de transitivite*

$$Mat_{BB_2} = Mat_{BB_1} Mat_{B_1 B}$$

Preuve
Consequence directe de la formule de la matrice associee a la composition de 2 applications lineaires appliquees a

$$\phi = \underset{V}{\mathrm{Id}} \quad \psi = \mathrm{Id}$$

□

Si on applique la formule a $B_2 = B$ on trouve le resultat desire.

Le cas des endomorphismes si $W = V$, $B' = B$ et $B'_n = B_n$.
Soit $\phi \in End(V)$

$$mat_{B_n B_n}(\phi) = mat_{B_n B} mat_{BB}(\phi) mat_{BB_n}$$

On a vu que

$$mat_{B_n B} = mat^{-1}_{BB_n}$$

Donc la formule de changement de base de ϕ.

$$mat_{B_n B_n}(\phi) = mat^{-1}_{BB_n} mat_{BB}(\phi) mat_{BB_n}$$

Si la base de depart egal a la base d'arrivee, on le note

$$mat_{B_n}(\phi) = mat_{B_n B} mat_B(\phi) mat^{-1}_{B_n B}$$

Definition 64
Deux matrices M et $N \in M_{d' \times d}(K)$sont dites equivalentes si il existe des matrices inversibles $A \in GL_{d'}(K), B \in GL_d(K)$ telles que

$$N = A.M.B$$

Proposition 118
Deux matrices sont equivalents si et seulement si il existe V de dimension d et W de dimension d', des bases $B, B_n \subset V$ et $B'B'_n \subset W$ et une application lineaire $\phi > V \to W$ telles que

$$M = mat_{B'B}(\phi)N = mat_{B'_nB_n}(\phi)$$

Preuve
Si $M = mat_{B'B}(\phi)$ et $N = mat_{B'_nB_n}(\phi)$, alors

$$N = mat_{B'_nB'}M.mat_{BB_n}$$ □

Proposition 119
Si M et N sont equivalents alors

$$rg(M) = rg(N)$$

Preuve

$$rg(M) = rg(\phi) = rg(N)$$ □

Remarque
La relation "etre equivalent" est une relation d'equivalence.

8.7 Conjugaison

Definition 65
Soit $C \in GL_d(K)$ une matrice inversible. On note $Ad(C)$ l'application dite de conjugaison par C :

$$Ad(C) : M \mapsto C.M.C^{-1}$$

Proposition 121
La conjugaison $Ad(C)$ est un automorphisme de l'algebre $M_d(K)$

Preuve

$$C.(\lambda M + N).C^{-1} = \lambda Ad(C).M + Ad(C).N$$

Multiplicativite

$$CMNC^{-1} = CM\,\mathrm{Id}\,NC^{-1} = CMC^{-1}CNC^{-1}$$

Identite

$$C^{-1}CMC^{-1}C = M$$ □

Definition 66 (Application Adjointe)

$$Ad : C \in GL_d(K) \to Ad(C) \in GL(M_d(K))$$

Ad est un morphisme de groupe.
On le verifie...

On donne un nom a $\Im(Ad) = Ad(GL_d)$, on l'appelle le groupe des automorphismes interieurs.

Proposition 122
L'application adjointe $Ad(\bullet)$ est un morphisme de groupes. Son noyau est forme par les matrices scalaires

$$\ker Ad = K^\times \operatorname{Id}$$

Preuve
Si $C = \lambda.\operatorname{Id}$, avec $\lambda \neq 0$, $\lambda \in K^\times$, alors

$$C^{-1} = \lambda^{-1} \operatorname{Id}$$

Donc

$$CMC^{-1} = M$$

Donc

$$K^\times \operatorname{Id} \subset \ker Ad(\bullet)$$

Soit Donc $C \in GL_d(K)$ telle que

$$\forall M \in M_d(K)$$

on a

$$CMC^{-1} = M$$

Il suit

$$CM = MC \Rightarrow CM - MC = 0$$

Donc

$$\forall M[C, M] = CM - MC = 0$$

L'application $M \to [C, M]$ est lineaire et dire que pour tout M

$$[C, M] = 0 \iff [C, E] = 0$$

pour E une base des matrices carrees.
On prend la base canonique.

Lemme 123

$$E_{ij}E_{kl} = \delta_{jk}E_{il}$$

Preuve (du lemme)

$$E_{ij} = mat_{B_0}E_{ij}$$

Donc

$$E_{ij}(v) = e_j^*.e_i$$

Donc

$$E_{ij}E_{kl}(v) = E_{ij}(E_l^*(v)e_k) = e_l^*(v)E_{ij}(e_k) = e_l^*(v)e_j^*(e_k)e_i$$

Or $e_j^*(e_k) = \delta_{jk}$.

Donc

$$E_{ij}E_{kl}(v) = \delta_{jk}e_l^*(v)e_i = \delta_{jk}E_{il}(v)$$ □

Soit C *tel que pour tout* E_{ij} *on a*

$$CE_{ij} = E_{ij}C$$

Donc

$$C = \sum_{k,l\leq d} c_{kl}E_{kl}$$

Donc

$$\begin{aligned} E_{ij}.C &= E_{ij}(\sum_{k,l} c_{kl}E_{kl}) \\ &= \sum_{k,l} c_{kl}E_{ij}E_{kl} \\ &= \sum_{k,l} c_{kl}\delta_{jk}E_{il} \\ &= \sum_{l\leq d} c_{jl}E_{il} \end{aligned}$$

De meme

$$\begin{aligned} C.E_{ij} &= \sum_{k,l\leq d} c_{kl}E_{kl}E_{ij} \\ &= \sum_{k,l\leq d} c_{kl}\delta_{li}E_{kj} \\ &= \sum_{k\leq d} c_{ki}E_{kj} \end{aligned}$$

Seule possibilite pour l'egalite est que $c_{ki} = 0$ sauf si $k = i$ de meme $c_{jl} = 0$ sauf si $l = j$.
Donc

$$CE_{ij} = E_{ij}C$$

si et seulement si

$$c_{ii}E_{ij} = C_{jj}E_{ij}$$

et les $c_{ki} = 0$ si $k \neq i$ et $c_{jl} = 0$ si $l \neq j$. Donc $c_{ii} = c_{jj}$ valable $\forall i, j \leq d$ et $C_{ii} \neq 0$ car C inversible. □

Definition 67
On dit que deux matrices $M.N$ sont semblables on conjuguees si il existe $C \in GL_d(K)$ tel que

$$N = CMC^{-1}$$

Proposition 124
La relation etre semblable est une relation d'equivalence.

Preuve

— *Reflexive*

$$M = \mathrm{Id}\, M\, \overset{-1}{\mathrm{Id}}$$

— *Symmetrique si $N = CMC^{-1}$*

$$M = C^{-1}NC$$

— *Transitive*

$$N = CMC^{-1} \text{ et } O = DND^{-1}$$

Alors

$$O = DCMC^{-1}D^{-1} = (DC)M(DC)^{-1}$$ □

La classe d'equivalence de M s'appelle la classe de conjugaison de M.

Remarque
M et $N \in M_d(K)$sont semblables si et seulement il existe V de $\dim d$, deux bases B, B_n de V et $\phi \in End(V)$ tel que

$$M = mat_B \phi$$

et

$$N = mat_{B_n} \phi$$

Lecture 17: Changements de Base Tue 10 Nov

Lecture 18: Corps des Nombres Complexes Mon 16 Nov

9 Le Corps des Nombres Complexes

Prenons $K = \mathbb{R}$ et $\mathcal{M} = M_2(\mathbb{R})$. Soit I la matrice

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Definition 68
L'espace des nombres complexes $\mathbb{C}$ *est le sous-espace vectoriel engendre par* Id *et* I

$$\mathbb{C} = \mathbb{R}.\,\mathrm{Id} + \mathbb{R}.I$$

Theorème 126
L'espace des nombres complexes est de dimension 2 et $\{\mathrm{Id}, I\}$ *en forme une base.*
De plus $\mathbb{C}$ *est une sous-algebre commutative de* $M_2(\mathbb{R})$ *et est en fait un corps. Le corps des nombres reel s'injecte dans* $\mathbb{C}$ *via l'application*

$$x \in \mathbb{R} \mapsto x.\,\mathrm{Id} \in \mathbb{C}$$

(les nombres reels s'identifient aux matrices scalaires).

Preuve
La famille $\{\mathrm{Id}, I\}$ *est libre* $\Rightarrow$ *base de* $\mathbb{C}$.
$\mathbb{C}$ *est un sev de* $M_2(\mathbb{R})$*, pour montrer que* $\mathbb{C}$ *est un sous-anneau de* $M_2(\mathbb{R})$*, il suffit de montrer que* $\mathbb{C}$ *est stable par produit.*

Remarque
$I^2 = -\mathrm{Id}$
En particulier, I *est inversible et*

$$I^{-1} = -I = {}^t I$$

Soit $z = x\,\mathrm{Id} + yI$ *et* $z' = x'\,\mathrm{Id} + y'I$.

$$\begin{aligned} z.z' &= xx'\,\mathrm{Id} + x'yI + xy'I - yy'\,\mathrm{Id} \\ &= (xx' - yy')\,\mathrm{Id} + (xy' + yx')I \end{aligned}$$

Donc $\mathbb{C}$ *est un sous-anneau de* $M_2(\mathbb{R})$.
Montrons que $\mathbb{C}$ *est un corps.*

$\mathbb{C}$ *est un corps :* $0_2 = 0_{\mathbb{C}} \neq \mathrm{Id} = 1_{\mathbb{C}}$.
Il reste a montrer que $z \in \mathbb{C} \setminus 0_{\mathbb{C}}$ *est inversible.*

$$\begin{aligned} z^2 - 2xz &= (x^2 - y^2)\,\mathrm{Id} + 2xyI - 2x(x\,\mathrm{Id} + yI) \\ &= -(x^2 + {}^2)\,\mathrm{Id} \end{aligned}$$

Or $z \neq 0_2 \iff (x, y) \neq (0, 0) \iff x^2 + y^2 \neq 0$.
Et donc

$$\mathrm{Id} = \frac{-1}{x^2 + y^2}(z^2 - 2xz)$$

Donc

$$z^{-1} = \frac{-1}{x^2 + y^2}(z - 2x)$$

On trouve, en developpant que

$$\frac{1}{x^2 + y^2} \quad {}^t z = z^{-1}$$

□

Remarque
On peut identifier $\mathbb{R}$ *avec l'algebre* $\mathbb{R}\,\mathrm{Id}$ *des matrices scalaires*

$$x \in \mathbb{R} \to x\,\mathrm{Id}$$

Definition 69
Le reel x *est appele partie reelle de* z *et le reel* y *est la partie imaginaire de* z

$$x = \mathrm{Re}\, z, y = \mathrm{Im}\, z$$

Dans la notation matricielle, la transposition $z \mapsto^t z$ *envoie*

$$x + iy \mapsto x - iy$$

Avec la notation simplifiee, on note

$$\bar{z} = x - iy$$

et s'appelle la conjugaison complexe de z. *On a alors*

$$z.\bar{z} = x^2 + y^2 \geq 0$$

Le nombre $(z.\bar{z})^{\frac{1}{2}}$ *se note*

$$|z| = (x^2 + y^2)^{\frac{1}{2}}$$

et s'appelle le module de z. *On a donc*

$$z\bar{z} = |z|^2$$

Proposition 129
On a les proprietes suivantes

1. *Les applications partie reelle et imaginaire sont lineaires*
2. *La conjugaisonn complexe est un automorphisme du corps* $\mathbb{C}$.
   De plus $\bar{\bar{z}} = z$ *et on a*

$$\bar{z} = z \iff z = x \in \mathbb{R}$$

3. *Le module* $z \mapsto |z|$ *est multiplicatif :*

$$|z.z'| = |z|.|z'|$$

et on a

$$z = 0 \iff |z| = 0$$

Preuve
Re, Im *sont lineaires car ce sont les formes lineaires 1ere et 2eme coordonnees de* $z \in \mathbb{C}$ *dans la base* $\{\mathrm{Id}, I\}$.
De meme $z \mapsto \bar{z}$ *est lineaire.*
etc □

On remarque que $|\bullet|$ est un morphisme de groupe multiplicatif

Proposition 130
On a un isomorphisme de groupes

$$pol : \mathbb{C}^\times \simeq \mathbb{R}_{>0} \times \mathbb{C}^{(1)}$$

donne par

$$z \in \mathbb{C}^\times \mapsto pol(z) = (|z|, \frac{z}{|z|})$$

Preuve
On a que

$$\frac{z.z'}{|z.z'|} = (\frac{z}{|z|})(\frac{z'}{|z'|})$$

et

$$|\frac{z}{|z|}| = \frac{(x^2+y^2)^{\frac{1}{2}}}{|(x^2+y^2)^{\frac{1}{2}}|}$$

□

Donc l'application pol est un morphisme.

Lecture 19: Nombres Complexes 2

Tue 17 Nov

Definition 70

$pol(z)$ s'appelle la decomposition polaire de z. Le premier terme $|z|$ est le module et se note aussi $\rho(z)$ et le second terme $\frac{z}{|z|}$ est appele argument complexe de z et on le note

$$\frac{z}{|z|} = e^{i\theta(z)}$$

Si on decompose l'argument complexe en partie reelle et imaginaire

$$\frac{z}{|z|} = e^{i\theta(z)} = c(z) + is(z)$$

On a donc

$$c(z) \in [-1, 1] \text{ s'appelle le cosinus de } z$$

$$s(z) \in [-1, 1] \text{ s'appelle le sinus de } z$$

Proposition 131 (Formules de trigonometrie)

On retrouve les formules habituelles de trigonometrie

- *Formules de produit : pour $z, z' \in \mathbb{C}^\times$*

$$c(z.z') = c(z)c(z') - s(z)s(z'), s(z.z') = s(z).c(z') + s(z')c(z)$$

- *Formule d'inveresion*

$$e^{i\theta(\frac{1}{z})} = c(z) - is(z)$$

- *Formule de l'angle double*

$$c(z^2) = c(z)^2 - s(z)^2, s(z^2) = 2s(z)c(z)$$

et plus generalement

- *Formules de Moivre : pour $n \geq 0$*

$$c(z^n) + is(z^n) = (c(z) + is(z))^n = \sum_{k=0}^{n} C_n^k c^{n-k} s^k$$

Preuve

Pour les formules de Moivre, on a

$$\begin{aligned} e^{i\theta(z^n)} &= (e^{i\theta(z)})^n = (c(z) + is(z))^n \\ &= c(z)^n + nc(z)^{n=1} is(z) + \sum_{k=2}^{n} C_n^k c(z)^{n-k} (is(z))^k \\ &= \sum_{k=0}^{n} C_n^k c(z)^{n-k} (is(z))^k \end{aligned}$$

$$= \sum_{k=0}^{n} C_n^k i^k c(z)^{n-k} s(z)^k$$

En posant

$$k' = 2[\frac{k}{2}], \quad k = k' + \begin{cases} 0 \ si \ pair \\ 1 \ si \ impair \end{cases}$$

on obtient que

$$e^{i\theta(z^n)} = (e^{i\theta(z)})^n = (c(z) + is(z))^n$$
$$= \sum_{k'=0}^{\frac{n}{2}} C_n^{2k'} (-1)^{k'} c(z)^{n-2k'} s(z)^{2k'} + \sum_{k'=0}^{\frac{n}{2}} C_n^{2k'+1} (-1)^{k'} i c(z)^{n-(2k'+1)} s(z)^{2k'+1}$$

Theorème 132
Il existe un unique morphisme de groupe

$$\theta \in (\mathbb{R}, +) \mapsto \exp i\theta \in (\mathbb{C}^{(1)}, \times)$$

qui est derivable et qui verifie

$$e^{i\bullet'}(0) = i$$

Ce morphisme est surjectif et son noyau est de la forme

$$\ker e^{i\bullet} = 2\pi.\mathbb{Z}$$

On dit que $\theta \to e^{i\theta}$ est derivable si les fonctions partie reelle et partie imaginaires sont derivables

$$(e^{i\theta})' = (\mathrm{Re}\, e^{i\theta})' + i(\mathrm{Im}\, e^{i\theta})'$$

Theoreme sans preuve.

Definition 71
Soit z un nombre complexe de module 1.
L'argument de z

$$\arg(z) = \theta(\mod 2\pi)$$

Plus generalement, pour $z \in \mathbb{C}^\times$, on definit son argument par

$$\arg z = \arg \frac{z}{|z|}$$

Definition 72
Soit $\theta \in \mathbb{R}$, on a

$$e^{i\theta} = \cos\theta + i \sin\theta$$

De ceci, on retrouve les formules d'addition.

Lecture 20: Operations Elementaires

Mon 23 Nov

Theorème 133
Soit $P(X)$ un polynome reel non-constant alors l'equation admet au moins une solution dans $\mathbb{C}$.

Theorème 134 (Gauss-Wantzel)
On peut exprimer les parties reelles et imaginaires du nombre complexe $\omega_n = e^{i2\pi/n}$ par extraction successive de racines carrees si et seulement si

$$n = 2k \text{ ou bien } n = 2^k \prod_i p_i$$

ou $\prod_i p_i$ est un produit (non-vide) de nombres premiers tous distincts et "de Fermat" : on dit qu'un nombre premier p_i est de Fermat si $p_i = F_{f_i} = 2^{2^{f_i}} + 1$, avec $f_i \geq 0$ un entier

10 Operations Elementaires Sur Les Matrices

Definition 73 (Operations Elementaires)

1. $T_{ij} \quad L_i \rightleftarrows L_j \quad i, j \leq d'$
2. $D_{i,\lambda}\lambda \neq 0 L_i \to \lambda L_i$
3. $CL_{ij,\mu} : L_i \to L_i + \mu L_j$

Proposition 135
Ces operations sont des applications lineaires bijectives

Proposition 136
Les trois operations elementaires sont obtenues par multiplication a gauche de M par des matrices convenables : pour $1 \leq i, j \leq d'$

- T_{ij}
- $D_{i,\lambda}$
- $Cl_{ij,\mu}$

ou les matrices carrees $T_{ij}, D_{i\lambda}, Cl_{ij,\mu}$ sont definies par

$$T_{ij} = \mathrm{Id} - E_{ii} - E_{jj} + E_{ij} + E_{ji}$$
$$D_{i,\lambda} = \mathrm{Id} + (\lambda - 1)E_{ii}, \lambda \neq 0$$
$$Cl_{ij,\mu} = \mathrm{Id} + \mu . E_{ij}$$

Lecture 21: Matrices Elementaires

Tue 24 Nov

Les matrices ci-dessus s'appellent les matrices de transformation elementaire, ce sont tous des matrices inversibles.

Definition 74
On dit que N est ligne-equivalente a M si et seulement si il existe une suite de transformations elementaires qui transforme M en N.

Proposition 137
La relation etre "ligne-equivalente" est une relation d'equivalence sur $M_{d'\times d}(K)$. De plus deux matrices M, N ligne-equivalentes sont equivalentes au sens de la notion d'equivalence de deux matrices.

Preuve
La "ligne-equivalence" est reflexive $M \sim M$ car l'identite est une transformation elementaire.
Elle est symetrique : si N est obtenue a partir de M par une suite de transformations elementaires M est obtenue a partir de N en appliquant la suite des transformations inverses dans l'ordre oppose.
C'est transitif, car si $N \sim M$ et M et $O \sim N$, alors $O \sim M$.
Si $N \sim M$, alors $N = T_1 T_2 \dots T_k M$, et donc $N = TM\,\mathrm{Id}$. □

Proposition 138
Si $N \in M_{d'\times d}(K)$ est ligne equivalente a M, alors toute ligne de N est combinaison lineaire des lignes de M.

$$\forall i \leq d', Lig_i(N) \in \langle L_1, \dots, L_{d'} \rangle \subset K^d$$

et inversement les lignes de M sont combinaisons lineaires des lignes de N.

10.1 Echelonage

Definition 75
Une matrice $M = (m_{ij}) \in M_{d'\times d}(K)$ est echelonnee si elle est nulle ou bien si

1. *Il existe $1 \leq j_1 \leq j_r \leq d$ tels que*
   - *Pour la ligne L_1, le premier terme non-nul est le j_1-ieme : on a $m_{1j} = 0$ pour tout $j < j_1$ et $m_{1j_1} \neq 0$*
   - *Pour la ligne L_2, le premier terme non-nul est le j_2-ieme : on a $m_{2j} = 0$ pour tout $j < j_2$ et $m_{2j_2} \neq 0$*

⋮

   -

2. *Si $r < d$ les lignes $L_{r+1,\dots,L_{d'}}$ sont toutes nulles.*

Les $j_1 < \dots < j_r$ sont appeles les echelons de M et les m_{ij_i} sont les pivots

Definition 76
Si de plus

$$m_{ij_1} = m_{2j_2} = \ldots = 1$$

La matrice est echelonnee reduite

Theorème 139
Toute matrice est ligne-equivalente a une matrice echelonnee reduite.

Preuve
$M \in M_{d' \times d}(K)$.
Si $M = 0$, on a fini.
Si $M \neq 0$, soit $j_1 \leq$, le plus petit indice d'une colonne qui est non-nul.
Par definition, il existe $i \leq d'$ tel que $m_{ij_1} \neq 0$.
On echange la ligne L_1, avec la ligne L_i.
On remplace $L_2 L_3 \ldots L_{d'}$ par $L_2 - m_{2j_1} L_1, \ldots$
En appliquant ceci recursivement, on trouve une matrice echelonnee. □

Proposition 140
Deux matrices ligne-equivalentes et echelonnees reduites sont egales.

Lecture 22: Engendrement du groupe lineaire

Mon 30 Nov

Proposition 141
Si M et N sont lignes equivalents

$$rg(M) = rg(N)$$

Preuve
Si $M \sim_{lig} N \Rightarrow M \sim N$. □

10.2 Engendrement du groupe lineaire

Proposition 142
Soit $M \in M_d(K)$ une matrice carree alors M est inversible si et seulement si M est ligne equivalente a la matrice identite Id.

Preuve
M est inversible si et seulement si $rg(M) = d$, et donc M inversible si et seulement si M est ligne equivalente a R, $R \in M_d(K)$ une matrice a d echelons.
$R = \mathrm{Id}$. □

Corollaire 143
Le groupe lineaire $GL_d(K)$ est engendre par les matrices de transformation

elementaires.

Preuve
Soit $M \in GL_d(K)$, donc

$$M \sim_{lig} \mathrm{Id}$$

Donc, il existe $T_1, \ldots, T_k$ des matrices de transformations elementaires tel que

$$\mathrm{Id} = T_k \ldots T_1 M$$

Donc

$$M = T_1^{-1} \ldots T_k^{-1}$$

□

10.3 Extraction d'une base

Soit

$$G = \{w_1, \ldots, w_l\} \subset K^d$$

et $W = \langle G \rangle$.

Proposition 144
Soit $M \in M_{l \times d}(K)$ la matrice dont les l lignes sont formees des vecteurs lignes $w_i, i \leq l$. Soit R la matrice echelonee reduite associee a M et

$$w'_i = Lig_I(R)$$

Les lignes de R possedent r echelons on a

$$\dim W = r$$

et les r premieres lignes

$$\mathcal{B}_W = \{w'_i, i \leq r\}$$

forment une base de W.

Preuve
On a vu que les lignes de R sont CL des lignes de M.
Mais on sait que les $w'_i, i \leq r$ forment une famille libre et

$$rgR = rgM = \dim W$$

□

10.4 Resolution de systemes lineaires

Soit $\phi : V \to W$ et $w \in W$, on cherche l'ensemble des $v \in V$ tel que

$$\phi(v) = w$$

On cherche l'ensemble des antecedents de $w \in W$ par l'application ϕ.
On cherche

$$\phi^{-1}(\{w\}) = \{v \in V \quad \phi(v) = w\}$$

C'est un cas particulier d'une question sur les groupes

$$\phi : (G, \cdot) \to (H, \cdot)$$

Lemme 145
Soit $\phi : G \mapsto H$ un morphisme de groupes, alors pour tout $h \in H$, on pose

$$Sol_\phi(h) = \phi^{-1}(\{h\}) = \{g \in G, \phi(g) = h\} \subset G$$

la preimage de h par ϕ. En particulier, $Sol_\phi(e_H) = \ker \phi$. Alors $Sol_\phi(h)$ est

- *soit l'ensemble vide (ssi $h \notin \phi(G)$)*
- *soit il existe $g_0 \in Sol_\phi(h)$ et*

$$Sol_\phi(h) = g_0 Sol_\phi(e_H) = g_0 \ker \phi = \{g_0.k, \phi(k) = e_H\}$$

Preuve
Si $h \notin \phi(G)$, il n'existe pas de g tel que

$$\phi(g) = h$$

et

$$Sol_\phi(h) = \emptyset$$

Si $h \in \phi(G)$, alors $\exists g_0 \in G$ tel que $\phi(g_0) = h$, donc l'ensemble n'est pas vide. Alors

$$\phi(g) = h = \phi(g_0)$$

et donc

$$\phi(g_0)^{-1}\phi(g) = e_h$$

Donc

$$g_0^{-1} g = k \in \ker \phi = Sol_\phi(e_H)$$

Reciproquement, soit $g = g_0 k, k \in \ker \phi$, alors

$$\phi(g) = \phi(g_0)\phi(k) = \phi(g_0) = h$$

□

Corollaire 146
$G = (V, +), H = (W, +), \phi : V \to W$ une application lineaire.
Soit $w \in W$.
Si $w \notin \phi(W)$, l'ensemble des solutions est vide.

Sinon, $w \in \phi(V)$, soit v_0, un antecedent, alors

$$Sol_\phi(w) = \{v \in V | \phi(v) = w\} = v_0 + \ker \phi$$

Definition 77
Les inconnues v_{j_i} pour j_i etant un echelon sont appellees inconues principales du systeme. Les inconnues v_j pour $j \leq d$ qui n'est pas un echelon sont appellees inconnues libres dy systeme.

Lecture 23: Determinant

Tue 01 Dec

11 Determinants

11.1 Formes multilineaires

Definition 78
Soit V un K-espace vectoriel et $n \geq 1$ un entier. Une forme multilineaire en n variables sur V est une application Λ

$$V^n \mapsto K$$
$$(v_1, \ldots, v_n) \mapsto \Lambda(v_1, \ldots, v_n)$$

telle que pour tout $i = 1, \ldots, n$ et tous $v_j \in V$, $j \neq i$, l'application "restriction a la i-ieme composante" est lineaire.
L'ensemble des formes multilineaires en n variables sur V est note

$$Mult^{(n)}(V, K) \text{ ou bien } (V^*)^{\otimes n}$$

Definition 79
Soit $l_1, \ldots, l_n \in V^*$, on note

$$l_1 \otimes \ldots \otimes l_n : (v_1, \ldots, v_n) \to l_1(v_1) \ldots l_n(v_n)$$

Le produit tensoriel des n formes lineaires.

Proposition 147
L'ensemble $Mult^{(n)}(V, K)$ des formes multilineaires en n variables est un K-espace vectoriel quand on le munit de l'addition et de la multiplication par les scaleurs usuelle pour les fonction a valeurs dans K.

Preuve
exercice □

Proposition 148
Soit $d = \dim V$ et B une base, B^* une base du dual. Alors $V^{*\otimes n}$ est de dimension finie egale a d^n ; une base de $V^{*\otimes n}$ est donne par l'ensemble des

formes multilineaires de la forme

$$e^*_{j_1} \otimes \ldots \otimes e^*_{j_n} \text{ quand } j_1, \ldots, j_n \text{ parcourent } \{1, \ldots d\}.$$

On note cette base $B^{*\otimes n}$.

Preuve

Soit V *un espace vectoriel.*

Pour i *un indice entre 1 et* n, v_i.

$$\Lambda(v_1, \ldots, v_i, \ldots, v_n)$$

On a

$$v_i = \sum_{j=1}^{d} x_{ij} e_j = \sum e^*_j(v_i) e_j$$

On a donc

$$\begin{aligned}
\Lambda(v_1, \ldots, v_n) &= \Lambda\left(\sum e^*_j(v_1) e_j, \ldots\right) \\
&= \sum_{j_1=1}^{d} \cdots \sum_{j_n=1}^{d} \Lambda(e_{j_1}, \ldots, e_{j_d}) \times e^*_{j_1}(v_1) \ldots . e^*_{j_n}(v_n) \\
&= \sum_{(j_1,\ldots,j_n)\in\{1,\ldots,d\}} \Lambda(e_{j_1}, \ldots, e_{j_d}) e^*_{j_1} \otimes \ldots \otimes e^*_{j_d}(v_1, \ldots, v_n)
\end{aligned}$$

Donc, la famille des formes multilineaires

$$\left\{e^*_{j_1} \otimes \ldots \otimes e^*_{j_n}(j_1, \ldots, j_n) \in [1, \ldots, d]\right\}$$

est generatrice de $V^{*\otimes n}$.

Montrons que la famille est libre.

Soient $\lambda_{j_1 \ldots j_n} \in K$ *et supposons que*

$$\sum_{j_1=1}^{d} \cdots \sum_{j_n=1}^{d} \lambda_{j_1 \ldots j_n} e^*_{j_1} \otimes \ldots \otimes e^*_{j_n} = 0$$

Prenons

$$(v, e_1, e_1, \ldots, e_1)$$

Alors

$$\Lambda(v, e_1, e_1, \ldots, e_1) = \sum_{j_1=1}^{d} \lambda_{j_1,1,11,1} e^*_{j_1}(v) = 0$$

On a une expression d'une forme lineaire

$$v \to \sum_{j_1=1}^{d} \lambda_{j_1,1,\ldots,1} e^*_{j_1}(v) = 0$$

En changeant les vecteurs de toutes les manieres possibles, on deduit que tous les coefficients sont nuls. □

Lecture 24: Determinants

Mon 07 Dec

11.2 Formes Symmetriques/Alternees

Definition 80

Une forme multilineaire

$$\Lambda : V^n \mapsto K$$

est dite

- *Symetrique si* $\forall i \neq j \leq n$

$$\Lambda(v_1, \ldots, v_i, \ldots v_j) = \Lambda(v_1, \ldots, v_j, \ldots, v_i, \ldots)$$

  Autrement dit si sa valeur ne change pas quand on echange deux composantes.

- *Alternee si* $\forall i \neq j \leq n$

$$\Lambda(v_1, \ldots, v_i, \ldots v_j) = -\Lambda(v_1, \ldots, v_j, \ldots v_i)$$

  Autrement dit si sa valeur est changee en son opposee si on echange deux composantes distinctes.

Theorême 149

On suppose que $car(K) \neq 2$. *Soit* $d = \dim V$. *On a*

$$\dim Alt^n(V; K) = \begin{cases} 0 \ si \ n > d \\ 1 \ si \ n = d \\ C_d^n \ si \ n \leq d \end{cases}$$

Preuve

Soit Λ *qui est alternee, alors* $\forall i \neq j$

$$\Lambda(v_1, \ldots, v, \ldots, v, \ldots v_n)$$

Donc

$$2\Lambda(v_1, \ldots, v \ldots, v, \ldots) = 0$$

Donc

$$\Lambda(v_1, \ldots, v, \ldots, v, \ldots, v_n) = 0$$

Plus generalement, si la famille

$$\{v_1, \ldots, v_n\}$$

est liee alors

$$\Lambda(v_1, \ldots, v_n) = 0$$

Si la famille est liee, un des vecteurs s'exprime en fonction des autres.
Supposons que c'est v_n.
Alors

$$v_n = \sum \lambda_i v_i$$

Donc

$$\Lambda(v_1, \ldots, v_n) = \lambda_1 \Lambda(v_1, \ldots, v_1) + \ldots + \lambda_{n-1} \Lambda(v_1, \ldots, v_{n-1}) = 0$$

Si $n > d$, *toute famille* $\{v_1, \ldots, v_n\}$*de* n *vecteurs dans un espace de* $\dim d < n$ *est liee et donc*

$$\Lambda(v_1, \ldots, v_n) = 0$$

Cas $d = n$.
On va montrer que $\dim Alt^{(d)}(V, K) \leq 1$.
Comme Λ *est multilineaire,*

$$\Lambda = \sum_{j_1=1} \ldots \sum_{j_d=1} \Lambda(e_{j_1}, \ldots, e_{j_d}) e^*_{j_1} \otimes \ldots \otimes e^*_{j_d}$$

Si pour $l, l' \leq d$, *on a*

$$j_l = j_{l'} \Rightarrow e_{j_l} = e_{j'_l}$$

et comme la forme est alternee

$$\Lambda(\ldots, e_{j_l}, \ldots, e_{j_{l'}}, \ldots) = 0$$

Donc les seuls termes non nuls de la decomposition precedente sont ceux tels que $j_1 \neq j_2 \neq \ldots$ *et donc les coefficients sont des* $\lambda(e_1, \ldots, e_d)$ *et des permutations de ces vecteurs.*
La forme Λ *est determinee des qu'on connait la valeur de*

$$\Lambda(e_1, \ldots, e_d) \in K$$

Donc

$$\dim Alt^{(d)}(V, K) \leq 1$$ □

Pour montrer que $\dim Alt^d(V; K) = 1$, *il suffit de construire une forme alternee en* d *variables qui est* $\neq 0$.

Soit σ une permutation, on note alors $\Lambda_{|\sigma}$est la forme lineaire associee a la permutation des index.

Proposition 150
Pour tou $\sigma \in S_n$ *l'application* $\bullet_{|\sigma}$ *definit un endomorphisme du* $K - ev$ $Mult^n(V; K)$.
L'application

$$\sigma \in S_n \mapsto \bullet_{|\sigma}$$

verifie

$$\forall \Lambda, \Lambda_{|Id_n} = \Lambda$$

$\forall \Lambda, \forall \sigma\tau \in S_n$, *on a*

$$\Lambda_{|\sigma\circ\tau} = (\Lambda_{|\tau})_\sigma$$

Preuve

$$\Lambda_{|\sigma\circ\tau}(v_1, \ldots, v_n)$$
$$= \Lambda(v_{\sigma(\tau(1))}, \ldots)$$

De meme

$$\bullet_{|\sigma}(\bullet_{|\tau}(\Lambda))(v_1, \ldots)$$
$$= \Lambda_\sigma(v_{\tau(1)}, \ldots,)$$
$$= \Lambda(v_{\sigma(\tau(1))}, \ldots)$$ □

Theorème 151
Les formes multilineaires alternees $Alt^n(V; K)$ *sont exactement les formes multilineaires verifiant* $\forall \sigma \in S_n \Lambda_{|\sigma} = sgn(\sigma)\Lambda$

Preuve
Pour les formes alternees, si Λ *verifie* $\forall \sigma \Lambda_{|\sigma} = sgn(\sigma)\Lambda$, *en particulier si* $\sigma = \tau_{ij}$*est la transposition qui permute* i *et* j *sa signature vaut* -1.
Reciproquement si $\forall i \neq j$

$$\Lambda_{|_{\tau_{ij}}} = -\Lambda$$

Alors $\forall \sigma \in S_n$

$$\sigma = \tau_1 \circ \ldots \circ \tau_t$$

Alors

$$\Lambda_{|\sigma} = \Lambda_{\tau_{t-1}\ldots|\tau 1} = (-1)^t \Lambda = sgn(\sigma)(\Lambda)$$ □

Theorème 152
Soit K *un corps,* $(G, \cdot)$ *un groupe fini,* V *un* K*-ev de dimension finie et*

$$\iota : G \mapsto GL(V)$$

un morphisme de groupe de G *vers le groupe des automorphismes de* V. *Soit*

$$\Xi : G \mapsto (K^\times, \times)$$

un morphisme de G *vers le groupe multiplicatif de* K. *Soit* $v \in V$, *alors le*

vecteur

$$v_\Xi = \sum_{h\in G} \Xi^{-1}(h)\iota(h)(v)$$

verifie pour tout $g \in G$

$$\iota(g)(v_\Xi) = \Xi(g)v_\Xi$$

Preuve

Abus de notation : on notera $g \in G, v \in V, \quad g.v$ *pour* $\iota(g)(v)$.

$$v_\Xi = \sum_{h\in G} \Xi(h)^{-1}.h(v)$$

Soit $g \in G$

$$\begin{aligned} g(v_\Xi) &= g\left(\sum_{h\in G} \Xi(h)^{-1}h(v)\right) \\ &= \sum_{h\in G} \Xi(h)^{-1}g(h(v)) \\ &= \sum_{h\in G} \Xi(h)^{-1}(g.h)(v) \end{aligned}$$

On pose $h' = g.h$

$$\begin{aligned} g(v_\Xi) &= \sum_{h'\in G} (\Xi(g)^{-1}\Xi(h'))h'(v) \\ &= \Xi(g)\sum_{h'\in G} \Xi(h')^{-1}h'(v) \end{aligned}$$

Donc

$$g(v_\Xi) = \Xi(g)v_\Xi$$ □

Lecture 25: Determinant d'une matrice

Tue 08 Dec

Corollaire 153

Soit Λ *une forme multilineaire en* n *variables sur* V*, alors*

$$\Lambda_{sgn} = \sum_{\sigma\in S_n} sgn(\sigma)\Lambda_{|\sigma}$$

est alternee.

Theorème 154

L'espace $Alt^d(V;K)$ *est de dimension 1 exactement et on a*

$$Alt^d(V;K) = K(e_1^* \otimes \ldots \otimes e_d^*)_{sgn}$$

Preuve
Soit

$$\Lambda = e_1^* \otimes \ldots \otimes e_d^*$$

et $\Lambda_{|sgn}$ *la forme correspondante symmetrisee.*
Montrons qu'elle est non nulle. On montre deux methodes. Calculons

$$\Lambda_{|sgn}(e_1, \ldots, e_d) = \sum_{\sigma \in S_n} sgn(\sigma) e^*_{\sigma(1)}(e_1) \ldots e^*_{\sigma(d)}(e_d)$$

$$= sgn(\mathrm{Id}) \qquad \square$$

Donc la forme est non-nulle.

Definition 81
La forme alternee $(e_1^* \otimes \ldots \otimes e_d^*)$ *est appellee le determinant de* V *relatif a la base* $B = \{e_1, \ldots, e_d\}$ *et est notee* $\det_B$*. C'est l'unique forme lineaire alternee satisfaisant*

$$\Lambda(e_1, \ldots, e_d) = 1$$

Proposition 155
On a la formule suivante

$$det_B(v_1, \ldots, v_d) = \sum_{\sigma \in S_d} sgn(\sigma) \prod_{i=1}^{d} x_{i\sigma(1)} = \sum_{\sigma \in S_d} x_{1\sigma(1)} \ldots x_{d\sigma(d)}$$

Preuve

$$det_B(v_1, \ldots, v_d) = \sum_{\sigma \in S_d} sgn(\sigma) e^*_{\sigma(1)} \ldots \qquad \square$$

Soit $\phi : V \to V$ et $\phi^*(\Lambda) \in Alt^n(V; K)$ tel que

$$\phi^*(\Lambda)(v_1, \ldots, v_n) = \Lambda(\phi(v_1), \ldots)$$

Definition 82
Le determinant de ϕ *est le scalaire verifiant*

$$\phi^*(det_B) = det(\phi) det_B$$

Theorème 156
Soit $\phi : V \to V$ *un endomorphisme. Pour tout* $\Lambda \in Alt^d(V, K)$*, on a*

$$\phi^*(\Lambda) = det(\phi)\Lambda$$

En particulier $det(\phi)$ *ne depend pas du choix de la base* B*.*

L'application det a les proprietes suivantes

1. *Homogeneite : soit $\lambda \in K$, alors*

$$det(\lambda\phi) = \lambda^d det(\phi)$$

2. *Multiplicativite : on a*

$$det(\psi \circ \phi) = det(\phi)det(\psi)$$

3. *Critere d'inversibilite : on a*

$$det(\phi) \neq 0 \iff \phi \in GL(V)$$

4. *Morphisme : L'application*

$$det : GL(V) \to K^\times$$

est un morphisme de groupes. En particulier $det(Id_V) = 1$.

Preuve

Soit $\Lambda \in Alt^d(V;K)$, alors $\Lambda = \lambda det_B$.

On a

$$\phi^*(\Lambda) = \phi^*(\lambda det_B) = \lambda\phi^*(det_B)$$

De meme

$$\phi^*(\lambda det_B)(v_1, \ldots, v_d) = \lambda det(\phi(v_1), \ldots)$$

1.

$$\begin{aligned} &det(\lambda\phi) \\ &= (\lambda.\phi)^*(\Lambda)(v_1, \ldots) \\ &= \lambda^d \phi^*(\Lambda)(v_1, \ldots) \\ &= \lambda^d det(\phi)\Lambda(v_1, \ldots) \end{aligned}$$

2. *Soit $\Lambda \in Alt^{(d)}(V;K)$.*

$$\begin{aligned} (\psi \circ \phi)^*(\Lambda) &= det(\psi \circ \phi)\Lambda \\ &= \Lambda(\psi \circ \phi(v_1), \ldots) \\ &= \psi^*(\Lambda)(\phi(v_1), \ldots) \\ &= det\psi\Lambda(\phi(v_1), \ldots) \\ &= det\psi det\phi\Lambda(v_1, \ldots) \end{aligned}$$

3. *Si ϕ est inversible*

$$\phi \circ \phi^{-1} = \mathrm{Id}$$

Donc

$$det\phi \circ \phi^{-1} = 1$$

Donc $det\phi \neq 0$.

4. *Si* $det\phi \neq 0$.
   On va montrer que si ϕ *n'est pas inversible* $det\phi = 0$.
   Si $\{\phi(e_1), \ldots\}$ *est liee, donc*

$$det_B(\phi(e_1), \ldots) = 0 \qquad \square$$

5. *Morphisme resulte du critere d'inversibilite et de multiplicativite.*

Lecture 26: Calcul de Determinants

Mon 14 Dec

Definition 83

Le noyau du morphisme det *est appele groupe speciale lineaire de* V *et on le note*

$$SL(V) = \ker \det$$

C'est un sous-groupe normal.

Remarque

Soit $\phi, \psi \in GL(V)$, *alors*

$$\det(Ad(\psi)(\phi)) = \det \phi$$

Definition 84

Soit $M \in M_d(K)$ *une matrice carree. Le determinant* $\det M$ *de* M *est*

1. *Le scalaire*

$$\det M = \det \phi$$

   ou ϕ *est est l'application lineaire associe a* M.

2. *Le determinant relativement a la base canonique des vecteurs d colonnes de* M *dans l'espace des vecteurs colonnes.*

3. *Le determinant relativement a la base canonique dans l'espace des vecteurs lligne*

4. *La somme*

$$\det M = \sum_{\sigma \in S_d} sgn(\sigma) m_{\sigma(1)1} \ldots$$

5. *La somme*

$$\det M = \sum_{\sigma \in S_d} sgn(\sigma) m_{1\sigma(1)} \ldots$$

Preuve
2)C'est tautologique, les colonnes de M C_i sont les coordonnees de $\phi(e_i)$ mises en colonnes

$$\det M = \det \phi = \det(C_1, \ldots)$$

4)

$$v_j = \phi(e_j)$$

On applique la formule generale a $m_{ij} = x_{ji}$, on a

$$\det_B(v_1, \ldots) = \sum_\sigma sign(\sigma) m_{\sigma(1)1} \ldots$$

5) On fait un changement de variable, on pose $i = 1, \ldots, d$, on pose $j = \sigma(i)$, alors $i = \sigma^{-1}(j)$, et quand i parcourt $\{1, \ldots, d\}$, j parcourt egalement cet ensemble. Donc

$$\det M = \sum_\sigma sgn(\sigma) \prod_{i=1}^{d} m_{\sigma(i)i} = \sum sgn(\sigma) \prod_{j=1}^{d} m_{j\sigma^{-1}(j)}$$

□

Cet expression est precisement le determinant dans la base canonique de K^d

Corollaire 158
soit $\phi : V \to V$ et $\phi^* : V^* \to V^*$, alors

$$\det \phi^* = \det \phi$$

Preuve
On a $\det \phi = \det M = \det^t M$ □

Corollaire 159
Soit M et N deux matrices semblables, alors

$$\det M = \det N$$

11.3 Calculs de Determinants

11.3.1 Blocs de Matrices

Theorème 160
Supposons que la matrice $M \in M_d(K)$ s'ecrit sous forme triangulaire superieure par blocs

$$M = \begin{pmatrix} M_1 & * \\ 0 & M_2 \end{pmatrix}$$

Alors

$$\det M = \det M_1 \det M_2$$

Preuve

Soit $M = (m_{ij})$*, alors*

$$\det M = \sum_{\sigma \in S_d} sign(\sigma) m_{\sigma(1)1} \dots$$

Dans la somme ci-dessus, on a alors

$$j \leq d_1, \sigma(j) > d_1$$

La contribution de ces termes sera donc nulle.
Il ne reste donc dans la somme que les termes correspondant aux permutations σ *telles que* $\forall j \leq d_1, \sigma(j) \leq d_1$*.*
Donc σ *laisse* $\{1, \dots, d_1\}$ *et definit donc une permutation*

$$\sigma_1 : \{1, \dots, d_1\} \to \{1, \dots, d_1\}$$

Comme σ *est une permutation de* $\{1, \dots, d\}$*, donc* σ *laisse stable* $\{d_1, \dots, d\}$*, et induit donc une permutation de cet ensemble.* □

Lecture 27: Fin Determinants

Tue 15 Dec

Remarque

Les resultats precedents valent aussi si M *est "triangulaire superieure par bloc".*

11.3.2 Operations sur les lignes/Colonnes

Lemme 162

Soient $T_{ij}, D_{i,\lambda}, CL_{ij,\mu}$ *les matrices des transformations elementaires des lignes d'une matrice, on a*

$$\det T_{ij} = -1$$
$$\det D_{i,\lambda} = \lambda$$
$$\det CL_{ij,\mu} = 1$$

Preuve

T_{ij} *est une matrice de transposition*

$$\det T_{ij} = sign(ij) = -1$$

$D_{i,\lambda}$ *est une matrice diagonale avec des 1 sur la diagonale sauf a la* i *eme ligne ou on a* λ*.*

$CL_{ij,\mu}$ est triangulaire superieure ou inferieure, donc

$$\det CL_{ij,\mu} = 1$$

□

Corollaire 163
Supposons que N soit deduite de M par un des trois types de transformations elementaires sur les lignes de M, alors on a

- $\det M = -\det N$
- $\det M = \lambda^{-1} \det N$
- $\det M = \det N$

Preuve
immediat par lemme. □

11.3.3 Developpement de Lagrange suivant une colonne /ligne

Soit M une matrice, on definit $M(k|l)$ contient tous les indices de $M = (m_{ij})$, pour $i \neq k$ ou $i \neq j$

Definition 85
Pour $k, l \leq d$

- *Le determinant de $M(k|l)$ est le (k,l) mineur de M.*
- *$(-1)^{k+l} \det(M(k|l))$ est le (k,l) cofacteur de M.*

Theorème 164
On a pour tout $j \leq d$

$$\det M = \sum_{i=1}^{d} m_{ij} (-1)^{i+j} \det(M(i|j))$$

11.4 Le polynome caracteristique

Definition 86
Le polynome caracteristique de M est le determinant

$$P_{car,M}(X) = \det(X.\,\mathrm{Id} - M) = \sum_{\sigma} sign(\sigma) \prod_{i=1}^{d} (X\delta_{i\sigma(i)} - m_{i\sigma(i)}) \in K[X]$$

Proposition 165
Le polynome caracteristique est un polynome unitaire de degre d et si on ecrit

$$\det(X.\,\mathrm{Id} - M) = X^d + a_{d-1}X^{d-1} + \ldots + a_d$$

On a

$$a_0 = P(0) = (-1)^d \det M$$
$$a_{d-1} = -tr(M) = m_{11} + \dots$$

Preuve

$$P_{car,M}(X) = \sum_{\sigma} sign(\sigma) \prod_{i=1}^{d} (X\delta_{i\sigma(i)} - m_{i\sigma(1)})$$

On trouve que $P_{car,M}(X)$ a son terme de plus haut degre provenant de $\sigma = \mathrm{Id}$ et donc $P_{car,M}(X)$ est unitaire de degre d.
Si $\sigma \neq \mathrm{Id}$, $\exists i$ tel que $\sigma(i) = j \neq i$, mais alors $\sigma(j) \neq j$.
Donc le produit

$$sign(\sigma) \prod_{i=1}^{d} (X\delta_{i\sigma(i)} - m_{i\sigma(i)})$$

contient au moins 2 facteurs de degre ≤ 0 et le produit est donc de degre $\leq d-2$, et donc

$$P_{car,M}(X) = X^d + a_{d-1}X^{d-1} + \dots + a_0 \qquad \square$$

Proposition 166
Le polynome est invariant de la classe de conjugaison de la matrice M

Preuve

$$\begin{aligned} &\det(XP\,\mathrm{Id}\,P^{-1} - PMP^{-1}) \\ &= \det(P(X\,\mathrm{Id} - M)P^{-1}) \\ &= -\det(X\,\mathrm{Id} - M) \end{aligned} \qquad \square$$

Definition 87
Soit $\phi \in End(V)$ une application lineaire, on definit son polynome caracteristique par

$$P_{car,\phi}(X) = P_{car,M}(X)$$

ou $M = Mat(\phi)$ est la matrice de ϕ dans une base quelconque de V.

Definition 88
On definit la trace de ϕ comme etant la trace de M

$$tr(\phi) = tr(M) = m_{11} + \dots$$

et cette definition ne depend pas du choix de la base B.