

# Algebre Lineaire I

David Wiedemann

## Table des matières

<b>1</b>	<b>Le language des Ensembles</b>	<b>7</b>
1.1	Notations . . . . .	7
1.2	Ensembles . . . . .	8
1.2.1	Exemples . . . . .	8
1.3	Sous-Ensembles . . . . .	8
1.4	$\mathcal{P}(E)$ l'ensemble des sous-ensembles . . . . .	8
1.4.1	Exercice . . . . .	9
1.5	Operations sur les ensembles . . . . .	9
1.6	$\times$ : Produit cartésien . . . . .	9
1.7	Applications entre ensembles . . . . .	9
1.7.1	Graphe . . . . .	10
1.8	Composition/Associativite . . . . .	10
1.8.1	Associativite . . . . .	11
1.9	Image,Preimage . . . . .	11
1.10	Relation de composition par les applications reciproques . . . . .	14
<b>2</b>	<b>Groupes</b>	<b>16</b>
2.1	Le groupe Symmetrique . . . . .	16
<b>3</b>	<b>Sous-Groupe</b>	<b>20</b>
3.1	Groupe engendre par un ensemble . . . . .	21
3.2	Morphismes de Groupes . . . . .	23
<b>4</b>	<b>Noyau et Image</b>	<b>27</b>
<b>5</b>	<b>Anneaux</b>	<b>31</b>
5.1	Elément inversible . . . . .	33
5.2	Sous-Anneau . . . . .	34
5.3	Morphismes d'anneaux . . . . .	34
5.4	Noyau/Image . . . . .	35
5.5	Modules sur un Anneau . . . . .	36
5.6	Sous-Module . . . . .	38

5.7	Module engendré par un ensemble . . . . .	39
5.8	Morphismes de Modules . . . . .	40
5.9	Structures Algebriques des espaces de morphismes . . . . .	42
<b>6</b>	<b>Corps</b> . . . . .	<b>44</b>
6.1	Corps des fractions . . . . .	44
6.2	Caractéristique des Corps . . . . .	47
6.3	Arithmétique des corps de caractéristique $p > 0$ . . . . .	49
<b>7</b>	<b>Espaces Vectoriels</b> . . . . .	<b>50</b>
7.1	Familles génératrices . . . . .	52
7.2	Famille Libre . . . . .	54
7.3	Bases . . . . .	57
7.4	Espaces vectoriels de dimension infinie . . . . .	59
7.5	Formes linéaires . . . . .	63
7.6	Espaces d'applications linéaires . . . . .	63
7.7	Formes linéaires et dualité . . . . .	65
7.8	Représentation paramétrique d'un sev cartésienne . . . . .	66
7.9	Une base de $Hom_k(V, W)$ . . . . .	67
7.10	Composition d'applications linéaires . . . . .	69
<b>8</b>	<b>Matrices</b> . . . . .	<b>70</b>
8.1	Produit de Matrices . . . . .	71
8.2	Rang d'une Matrice . . . . .	72
8.3	Transposition . . . . .	73
8.4	Les matrices carrées . . . . .	75
8.5	Le groupe lineaire . . . . .	76
8.6	Changement de Base . . . . .	77
8.7	Conjugaison . . . . .	79
<b>9</b>	<b>Le Corps des Nombres Complexes</b> . . . . .	<b>83</b>

## List of Theorems

1	Theorème (Composition de fonctions) . . . . .	11
1	Definition (Injectivite) . . . . .	12
2	Definition (Surjectivite) . . . . .	12
3	Definition (Bijectivite) . . . . .	13
2	Proposition (Injectivite et cardinalite) . . . . .	13
3	Proposition (Surjectivite et cardinalite) . . . . .	13
4	Proposition (injectivite et condition) . . . . .	13
5	Proposition (Surjectivite et condition) . . . . .	13

7	Lemme (Composition d'applications surjectives et injectives) . .	14
8	Proposition (Inverse d'une composition) . . . . .	15
4	Definition (Notations Injection) . . . . .	16
5	Definition (Notations Surjection) . . . . .	16
6	Definition (Notations Bijection) . . . . .	16
7	Definition (Groupe abstrait) . . . . .	17
8	Definition (Groupes commutatifs) . . . . .	18
9	Definition (Notation additive) . . . . .	18
9	Proposition (Lois de Groupe) . . . . .	18
10	Definition (Notation exponentielle) . . . . .	19
11	Definition (exponentielle) . . . . .	19
12	Definition (Notation multiple) . . . . .	19
13	Definition (Sous-groupe) . . . . .	20
11	Proposition (Critere de Sous-groupe) . . . . .	20
14	Theorème (Sous groupe de $\mathbb{Z}$ ) . . . . .	21
15	Proposition (Intersection de sous-groupes) . . . . .	22
14	Definition (Sous-groupe engendre) . . . . .	22
17	Theorème . . . . .	22
15	Definition (Morphisme de Groupe) . . . . .	23
18	Theorème . . . . .	23
16	Definition (Notations) . . . . .	24
21	Proposition . . . . .	25
22	Proposition . . . . .	26
17	Definition (Groupes Isomorphes) . . . . .	26
24	Theorème . . . . .	27
25	Proposition . . . . .	27
18	Definition . . . . .	28
26	Theorème (Critere d'injectivite) . . . . .	28
19	Definition (Anneaux) . . . . .	31
30	Lemme . . . . .	31
20	Definition (Element Inversible) . . . . .	33
33	Proposition . . . . .	33
21	Definition (Sous-Anneau) . . . . .	34
35	Lemme (Critère de sous-anneau) . . . . .	34
22	Definition (Morphisme d'anneaux) . . . . .	34
39	Proposition (Noyau d'un morphisme d'anneau) . . . . .	35
40	Theorème . . . . .	36
23	Definition (Modules sur un Anneau) . . . . .	36
24	Definition ( $A$ -Algebre) . . . . .	37
25	Definition (Sous-Module) . . . . .	38
26	Definition (Ideal) . . . . .	38

45	Lemme (Critère de Sous-Module) . . . . .	38
47	Proposition . . . . .	39
27	Definition . . . . .	39
48	Theorème . . . . .	39
28	Definition (Morphismes de Module) . . . . .	40
50	Lemme (Critere de l'application lineaire) . . . . .	41
51	Proposition . . . . .	41
29	Definition . . . . .	42
53	Proposition . . . . .	42
54	Proposition . . . . .	43
55	Theorème . . . . .	43
30	Definition (Corps) . . . . .	44
57	Proposition . . . . .	44
58	Lemme . . . . .	45
31	Definition . . . . .	45
59	Proposition . . . . .	45
32	Definition . . . . .	45
33	Definition (Caractéristique) . . . . .	47
61	Lemme . . . . .	48
34	Definition . . . . .	48
62	Lemme . . . . .	48
63	Lemme . . . . .	49
35	Definition . . . . .	49
65	Proposition . . . . .	49
36	Definition . . . . .	49
66	Lemme . . . . .	50
37	Definition (Espace Vectoriel) . . . . .	50
38	Definition (Produit) . . . . .	50
39	Definition . . . . .	50
68	Proposition (Critere de SEV) . . . . .	51
40	Definition . . . . .	51
70	Proposition (Critere d'application linéaire) . . . . .	51
71	Proposition . . . . .	51
72	Proposition . . . . .	51
41	Definition (Notations) . . . . .	51
42	Definition . . . . .	51
73	Proposition . . . . .	52
43	Definition . . . . .	52
44	Definition . . . . .	52
74	Lemme . . . . .	52
45	Definition (Notations) . . . . .	53

75	Proposition . . . . .	53
46	Definition (Famille génératrice) . . . . .	53
47	Definition (Espace vectoriel fini) . . . . .	53
76	Theorème . . . . .	54
48	Definition (Famille Libre) . . . . .	54
49	Definition . . . . .	54
79	Proposition . . . . .	55
80	Theorème . . . . .	55
81	Corollaire . . . . .	56
50	Definition . . . . .	57
83	Theorème . . . . .	57
84	Theorème (Dimension de SEV) . . . . .	59
51	Definition . . . . .	59
52	Definition . . . . .	59
53	Definition . . . . .	59
86	Theorème . . . . .	60
87	Lemme (Lemme de Zorn) . . . . .	60
88	Proposition . . . . .	60
54	Definition . . . . .	60
89	Corollaire . . . . .	61
90	Theorème (Le théorème noyau-image) . . . . .	61
91	Corollaire . . . . .	62
92	Corollaire . . . . .	63
93	Theorème . . . . .	63
55	Definition . . . . .	65
56	Definition . . . . .	65
96	Proposition . . . . .	65
57	Definition (Application linéaire duale) . . . . .	66
98	Proposition . . . . .	66
99	Lemme . . . . .	67
100	Theorème . . . . .	68
101	Proposition . . . . .	68
102	Proposition . . . . .	69
103	Theorème . . . . .	69
58	Definition . . . . .	70
59	Definition . . . . .	71
60	Definition (Multiplication Matricielle) . . . . .	71
104	Theorème . . . . .	71
61	Definition (Rang d'une matrice) . . . . .	72
105	Proposition . . . . .	72
107	Theorème . . . . .	73

62	Definition . . . . .	73
108	Proposition . . . . .	73
109	Proposition . . . . .	73
110	Theorème . . . . .	75
111	Theorème . . . . .	76
112	Proposition (Critere d'inversibilite) . . . . .	76
114	Proposition . . . . .	77
115	Proposition (Formule de changement de base) . . . . .	77
63	Definition (Matrice de Passage) . . . . .	77
117	Proposition . . . . .	78
64	Definition . . . . .	78
118	Proposition . . . . .	79
119	Proposition . . . . .	79
65	Definition . . . . .	79
121	Proposition . . . . .	79
66	Definition (Application Adjointe) . . . . .	80
122	Proposition . . . . .	80
123	Lemme . . . . .	81
67	Definition . . . . .	82
124	Proposition . . . . .	82
68	Definition . . . . .	83
126	Theorème . . . . .	83
69	Definition . . . . .	84
129	Proposition . . . . .	85
130	Proposition . . . . .	85
70	Definition . . . . .	86
131	Proposition (Formules de trigonometrie) . . . . .	86
132	Theorème . . . . .	87
71	Definition . . . . .	87
72	Definition . . . . .	87

## Lecture 1: Le langage des Ensembles

Mon 14 Sep

### 1 Le langage des Ensembles

Le terme “Algebre” est derive du mot arabe al-jabr tire du titre 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.

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

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 éléments, 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'était 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 ?  $\nexists$

## 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  $B$ .

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

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

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

Difference symmetrique :

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

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

On peut noter une grande reunion ainsi :

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

## 1.6 $\times$ : Produit cartésien

Si  $A$  et  $B$  sont des ensembles

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

On peut bien sur iterer

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

## 1.7 Applications entre ensembles

Soient  $X$  et  $Y$  deux ensembles.

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

$$f : X \rightarrow Y$$

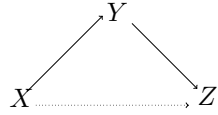


FIGURE 1 – Schema de la composition de 2 applications

### 1.7.1 Graphe

Se donner une application

$$f : X \rightarrow Y$$

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

$$f : X \rightarrow Y$$

$$g : Y \rightarrow Z$$

$$\begin{aligned} g \circ f : X &\longrightarrow Z | x \in X \longrightarrow f(x) \in Y \\ &\longrightarrow g(f(x)) \in Z \end{aligned}$$

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

$$\begin{aligned} (g \circ f) : X &\longrightarrow Z \circ h : Z \longrightarrow W \\ &\Rightarrow h \circ (g \circ f) \end{aligned}$$

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

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  $\mathcal{P}(X), \mathcal{P}(Y)$ .

$$— \text{ } Im(f) : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$$

$$A \subset X \longrightarrow Im(f)(A) = f(A)$$

C'est ce qu'on appelle l'image de  $A$  par  $f$

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

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

— 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

$$\begin{aligned} "f'' : X &\mapsto Y \\ x &\mapsto f(x) \end{aligned}$$

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

$$C : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$$

$$(m, n) \mapsto \frac{1}{2}((m+n)^2 + m + 3n)$$

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  $f : X \twoheadrightarrow Y$  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

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

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

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

$$(g \circ f)(x) = z = (g \circ f)(x') \quad \square$$

$\Rightarrow x$  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 noté*

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

**Definition 5 (Notations Surjection)**

*L'ensemble des applications surjectives sera noté*

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

**Definition 6 (Notations Bijection)**

*L'ensemble des applications bijectives sera noté*

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

*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 :

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

$\circ$  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 ( appelee loi de composition interne)  $\star$  tq

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

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

$$\begin{aligned} \cdot^{-1} : G &\mapsto G \\ g &\mapsto g^{-1} \end{aligned}$$

ayant les proprietes suivantes

- Associativite :  $\forall g, g', g'' \in G, (g \star g') \star g'' = g \star (g' \star g'')$ .
- Neutralite  $e_G$  :  $\forall g \in G, g \star e_G = e_G \star g = g$ .
- 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  $(G, \star, e_G, \cdot^{-1})$  est dit commutatif si  $\star$  possède la propriété supplémentaire de commutativité :

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

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

**Lecture 3: Groupes, Anneaux, Corps**

Tue 22 Sep

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

**Definition 9 (Notation additive)**

Si un groupe est commutatif on pourra utiliser une notation "additive" :

- La loi sera notée  $+$ .
- L'élément neutre sera noté  $0_G$ .
- L'inversion sera appelée opposé et notée  $-g$  et  $g + (-g) = 0_G$ .

**Proposition 9 (Lois de Groupe)**

- Involutive de l'inversion :  $\forall g, (g^{-1})^{-1} = g, g^{-1} \star g = e_G$ .
- L'élément neutre est unique, si  $\exists e'_G$  tq  $g \in G$  vérifiant  $g \star e'_G = g$ , alors  $e'_G$  est l'élément neutre.
- Unicité de l'inverse : si  $g' \in G$  vérifie  $g \star g' = e_G$ , alors  $g' = g^{-1}$ .
- On a  $(g \star g')^{-1} = g'^{-1} \star g^{-1}$

**Preuve**

La preuve de toutes les propriétés est donnée dans le support de cours.

On montre l'unicité de l'élément neutre.

Si  $e'_G$  est telle que pour un certain  $g \in G$ , tq

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

Alors on a à 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  $(g \star g')^{-1}$ .  $\square$

**Definition 10 (Notation exponentielle)**

$(G, \cdot)$  un groupe et  $g \in G$ . On peut :

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

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

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

si  $n < 0$  :

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

et  $g^0 := e_G$

**Exercice 10**

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

**Definition 11 (exponentielle)**

$$\begin{aligned}\exp_g : \mathbb{Z} &\rightarrow G \\ n &\rightarrow g^n\end{aligned}$$

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

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

Si  $n < 0$

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

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 suffit 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

$$((h')^{-1})^{-1} = h' \Rightarrow h \star h' \in H \quad \square$$

**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  $h^{-1} \in g^{\mathbb{Z}}$   $\square$

**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  $\mathbb{Z}$ )**

Reciproquement 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  $r \in \{0, \dots, q-1\}$  tq

$$\begin{aligned} h &= qk + r \\ r &= h - qk \in H \end{aligned}$$

□

Donc  $0 \leq r < q \Rightarrow r = 0$  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 généralement 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 deuxième version du critère 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 engendré par  $A$ , noté  $\langle A \rangle \subset G$  est par définition 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-vidé car il contient  $G$ .

Par la proposition précédente, on considère

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

Par la proposition cette intersection est un sous groupe qui contient  $A$  et c'est le plus petit possible au sens où 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

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

l'image de  $A$  par l'inversion alors

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

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 comme  $H$  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  $g_1, \dots, g_n \in A \cup A^{-1}$  Le produit  $g_1 \star g_2 \star \dots \star g_n \in H$

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

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

Critere de ss-groupe :

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

b) Soit  $g = g_1 \star g_2 \star \dots \star g_n$  et  $g' = g'_1 \star g'_2 \star \dots \star g'_n$

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

Alors

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

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

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

$\{\dots\}$  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  $\phi : G \rightarrow H$  est une application telle que

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

### Theorème 18

Soit  $\phi : G \rightarrow H$  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

$$\begin{aligned} h &= h \bullet \phi(e_G) \\ h^{-1} \bullet h &= h^{-1} \bullet h \bullet \phi(e_G) \end{aligned}$$

2)

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

On conclut en utilisant l'unicite de l'inverse

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

### Definition 16 (Notations)

- $\text{Hom}_{Gr}(G, H)$  l'ensemble des morphismes de groupe entre  $G$  et  $H$ .
- $\text{End}_{Gr}(G) = \text{Hom}_{Gr}(G, G)$  les endomorphismes du groupe  $G$ .
- $\text{Isom}_{Gr}(G, H)$  l'ensemble des morphismes bijectifs
- $\text{Aut}_{Gr}(G) = \text{Isom}_{Gr}(G, G)$  l'ensembles des automorphismes du groupe  $G$ .

### Exemple

—

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

— Soit  $g \in G$

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

Si  $G$  est commutatif note additivement

$$\bullet \cdot g : \begin{cases} \mathbb{Z} \rightarrow G \\ n \rightarrow n \cdot g \end{cases}$$



Conjugaison dans un groupe :  $(G, \cdot)$

$$h \in G$$

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

**Preuve**

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

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

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

Terminologie :

$$Ad_h(g) = h.g.h^{-1} \quad \square$$

Le conjugué de  $g$  par  $g$ .

**Remarque**

$Ad_h : G \rightarrow G$  est bijectif.  $Ad_h$  admet une application réciproque 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.

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

$$\text{car } (h^{-1})^{-1} = h \quad \square$$

$$\forall h \in G,$$

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

**Proposition 21**

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

---

**Preuve**

On veut montrer que

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

on a :

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

**Proposition 22**

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

**Preuve**

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

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

On calcule

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

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

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  $(Bij(G), \circ, Id_G, \bullet^{-1})$

### Preuve

Si  $\phi$  et  $\psi \in Isom_{Gr}(G, G)$ , alors  $\psi \circ \phi$  est un morphisme et  $\psi \circ \phi$  est bijectif

$\Rightarrow \psi \circ \phi \in Isom_{Gr}(G, G)$

Si  $\phi \in Isom_{Gr}(G, G) \cup Bij(G, G)$  alors  $\phi^{-1}$  est un morphisme donc

$$Isom_{Gr}(G, G) = Aut_{Gr}(G) \quad \square$$

## 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'image de  $\phi$ ,

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

— 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  $\phi(k) = h, \phi(k') = h'$

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

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

car  $K$  sous-groupe.

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

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  $\phi(g) = h \in L, \phi(g') = h' \in L$

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

on a

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

### Definition 18

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

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

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

### Theorème 26 (Critère d'injectivité)

Soit  $\phi \in \text{Hom}_{Gr}(G, H)$  un morphisme de groupes alors les propriétés suivantes sont équivalentes

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

### Preuve

1  $\rightarrow$  2

si  $\phi$  est injectif, l'image réciproque de  $\{e_H\}$  possède au plus un seul élément.

Mais comme  $\phi$  est un morphisme  $\phi(e_G) = e_H \Rightarrow \phi^{-1}(\{e_H\}) = \{e_G\}$

2  $\rightarrow$  1

On se donne  $h \in H$  et on veut montrer que  $\phi^{-1}(\{h\}) = \{g \in G, \phi(g) = h\}$  n'a pas plus d'un élément.

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 définition,  $\phi(g) = \phi(g') = h$

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

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

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

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

### Exemple

Ordre d'un element

Soit  $g \in G$  groupe

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

est un morphisme de groupes.

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

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

$$\Rightarrow \mathbb{Z} \rightarrow G$$

$n \rightarrow g^n$  est injective

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

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

donc  $g$  est d'ordre infini.

Si  $q > 0$ , alors

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

est un sous-groupe de cardinal  $q$  (à démontrer en exercice) et donc  $G$  contient un sous-groupe d'ordre  $q$

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

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

$$g^q = e_G$$

### Exemple (Conjugaison)

$G \ni h$

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

On a montré que  $Ad_h \in \text{Aut}_{Gr}(G)$

On considère l'application

$$h \in G \rightarrow Ad_h \in \text{Aut}_{Gr}(G)$$

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  $g \in G$

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

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

On dit que  $h$  commute avec  $g$ .

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

$Z_G$  est un groupe commutatif de  $G$

### Exemple (Translation)

Soit  $h \in G$  la translation a gauche par  $h$

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

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  $t_{h^{-1}}$

$t_\bullet : h \in G \rightarrow t_h \in \text{Bij}(G)$  est un morphisme de groupe injectif, l'image s'appelle le groupe des translations ( a gauche ) de  $G$ .

Donc  $G \simeq t_G \subset \text{Bij}(G)$

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  $(A, +, \cdot, 1_A)$  est la donnée, d'un groupe commutatif  $(A, +)$  (note additivement) d'élément neutre noté  $0_A$ , d'une loi de composition interne (dite de multiplication)

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

et d'un élément unité  $1_A \in A$  ayant les propriétés suivantes

1. Associativité de la multiplication

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

2. Distributivité

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

3. Neutralité de l'unité

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

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'élément neutre de l'addition  $0_A$  est absorbant. Pour l'opposé, on a

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

### Preuve

$\forall a \in A$

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

$$0_A = a.0_A$$

□

### 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  $\mathbb{R}$ .

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

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

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

$(\mathcal{F}(X, A), +, \bullet)$  est un anneau (commutatif si  $A$  commutatif) generalisation du cas des fonctions reelles

- $\mathbb{R}[x] = \{P(x) = a_0 + a_1x + \dots + a_dx^d, a_0, a_1, \dots, a_d \in \mathbb{R}, d \geq 0\}$
- $A[x] = \{P(x) = a_0 + a_1x + \dots + a_dx^d, a_0, \dots, a_d \in A, d \geq 0\}$   
Anneau des polynomes a coefficients dans  $A$ .
- $(M, +)$  un groupe commutatif

$$\text{End}(M) = \text{End}_{Gr}(M) = \text{Hom}_{Gr}(M, M)$$

$$+ : \psi, \phi \in \text{End}(M)$$

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

Soient  $\phi, \psi \in \text{End}(M)$

$$\phi \circ \psi \in \text{End}(M)$$

$$0_{\text{End}(M)} : m \in M \rightarrow 0_M \in M$$

$$1_{\text{End}(M)} : Id_M : m \in M \rightarrow m \in M$$

$(\text{End}(M), +, \circ, 0_M, Id_M)$  est un anneau

## Lecture 6: Anneaux 2

Mon 05 Oct

### Preuve

Soit  $\phi, \psi \in \text{End}_{Gr}(M)$ , on veut montrer que

$$\phi + \psi \in \text{End}_{Gr}(M)$$

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

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

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

$+$  est commutative

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



Soit  $\phi, \psi, \psi' \in \text{End}_{Gr}(M)$  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 Élément 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

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

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

### Exemple

- $\mathbb{Z}^\times = \{\pm 1\}$ ,  $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- $\mathcal{F}(X, \mathbb{R})^\times = \{f : X \rightarrow \mathbb{R} \mid f(x) \neq 0_{\mathbb{R}} \text{ pour tout } x \in X\}$
- $\mathbb{R}[x]^\times = \{a_0 \mid a_0 \in \mathbb{R}^\times\}$
- $\text{End}_{Gr}(M)^\times = \text{Aut}_{Gr}(M) = \text{Isom}_{Gr}(M, M)$

## 5.2 Sous-Anneau

### Definition 21 (Sous-Anneau)

Soit  $(A, +, \cdot)$  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  $\cdot$  :

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

Ainsi  $(B, +, \cdot)$  est un anneau.

### Lemme 35 (Critère de sous-anneau)

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

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

### Preuve

Si  $B = \{0_A\}$  c'est un sous-anneau.

Sinon  $1_A \in B$  si on prend  $b \in B$  alors

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

Alors

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

$$b - b' = 1_A \cdot b - b' \in B$$

Donc  $(B, +)$  est un sous-groupe.

Soient  $b, b' \in B$  alors

$$b \cdot b' - 0_A \in B$$

□

$$= b \cdot b'.$$

### Exemple

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

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

est un sous-anneau

## 5.3 Morphismes d'anneaux

### Definition 22 (Morphisme d'anneaux)

Soient  $(A, +, \cdot)$ , et  $(B, +, \cdot)$  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  $B$

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

**Exemple (Le morphisme canonique)**

Le morphisme canonique :

$$Can_A : (\mathbb{Z}, +, \cdot) \rightarrow (A, +, \cdot)$$

$$n \rightarrow n.1_A = 1_A + 1_A + \dots + 1_A \text{ } n \text{ fois si } n \geq 0 \text{ et } -n \text{ fois si } n < 0$$

est un morphisme d'anneaux.

On doit vérifier que  $Can_A$  est un morphisme entre les groupes additifs.

On doit montrer que  $\forall m, n \in \mathbb{Z}$

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

si  $m$  et  $n \geq 0$

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

## 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  $k \in \ker \phi, a \in A$

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

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

□

**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

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

**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 les 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

$$\begin{aligned} \mathbb{Z} \times M &\rightarrow M \\ (n, \vec{m}) &\rightarrow n * \vec{m} = \underbrace{\vec{m} + \vec{m} + \dots}_{n \text{ fois}} \end{aligned}$$

## Lecture 7: Anneaux Et Modules

Tue 06 Oct

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

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

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

Soit

$$\begin{aligned}a \in A, \vec{x} &\in A^d \\ a \cdot \vec{x} &:= (a \cdot a_1, \dots, a \cdot a_d)\end{aligned}$$

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

$$1_A \cdot \vec{x} = \vec{x}$$

### Exemple

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

$$\begin{aligned}\bullet \bullet : A \times \ker \phi &\rightarrow \ker \phi \\ (a, k) &\rightarrow a \cdot k\end{aligned}$$

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

$$\begin{aligned}A \times \mathcal{F}(X, A) &\rightarrow \mathcal{F}(X, A) \\ (a, f) &\rightarrow a \cdot f : x \mapsto a \cdot f(x)\end{aligned}$$

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

$$\begin{aligned}a \in A, f : X &\rightarrow M \\ a * f : x &\rightarrow a * f(x) \in M\end{aligned}$$

### 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  $(B, +, \cdot)$  possédant une structure de  $A$ -module qui vérifie la propriété d'associativité suivante :

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

$\mathbb{R}[x]$  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 multiplication par les scalaires

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

### Definition 26 (Ideal)

Un idéal 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 d'un  $A$ -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

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

$$\vec{x} = (a_1, \dots, a_d), A.\vec{x} = \{a.\vec{x} = (a.a_1, \dots, a.a_d) | a \in A\}$$

est un sous-module de  $A^d$ .

**Preuve**

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

$$\begin{aligned}\vec{v} &= a'.(a_1, \dots, a_d) = a'.\vec{x} \\ \vec{v'} &= a''.(a_1, \dots, a_d) = a''.\vec{x}\end{aligned}$$

Critère de sous-module :

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

**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-module de  $M$  contenant  $X$  ( 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  $A$  :

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

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

$$\begin{aligned} N &\supset CL_A(X) \\ \Rightarrow CL_A(X) &\subset \langle X \rangle \end{aligned}$$

---

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

$$\begin{aligned} u &= a_1 x_1 + \dots + a_n x_n, a_i \in A, x_i \in X \\ v &= a'_1 x'_1 + \dots + a'_m x'_m a'_j \in A, x'_j \in X \\ a * u + v &= a.a_1 * x_1 + \dots + a.a_n * x_n + a'_1 * x'_1 + \dots + a'_m * x'_m \in CL_A(X) \end{aligned}$$

$$X \subset CL_A(X)$$

car

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

---

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

$$x_1, \dots, x_n \in X$$

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

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

## Lecture 8: Modules et Corps

Mon 12 Oct

### 5.8 Morphismes de Modules

**Definition 28** (Morphismes 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

$$\phi : M \rightarrow N$$

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  $\phi$  est une application  $A$ -linéaire.



**Remarque**

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

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

**Lemme 50 (Critere de l'application lineaire)**

Soit  $\phi : M \rightarrow N$  une application entre deux modules alors  $\phi$  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

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

$\Rightarrow \phi$  est un morphisme de groupes additifs.

Si on prend  $m' = 0_M$

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

**Proposition 51**

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

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

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

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

**Preuve**

Comme  $\phi$  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  $\phi$  est linéaire

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

- 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 à vérifier 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

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

□

### Remarque

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

## 5.9 Structures Algébriques des espaces de morphismes

### Definition 29

On note

$$\begin{aligned} \text{Hom}_{A\text{-mod}}(M, N), \text{Isom}_{A\text{-mod}}(M, N) \\ \text{End}_{A\text{-mod}}(M), = \text{Hom}_{A\text{-Mod}}(M, M) \\ \text{Aut}_{A\text{-mod}}(M) = \text{GL}_{A\text{-mod}}(M) = \text{Isom}_{A\text{-mod}}(M, M) \end{aligned}$$

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

### Proposition 53

Soient  $\phi : L \rightarrow M$  et  $\psi : M \rightarrow N$  des morphismes de  $A$ -modules alors  $\psi \circ \phi : L \rightarrow N$  un morphisme.

### Preuve

Soit  $\phi : L \rightarrow M$ ,  $\psi : M \rightarrow N$  des applications linéaires alors

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

On sait que  $\psi \circ \phi$  est un morphisme de groupes.

Reste à voir que  $\forall a \in A, l \in L$

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

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

**Proposition 54**

Soient  $M$  et  $N$  des  $A$ -modules alors  $\text{Hom}_{A\text{-mod}}(M, N)$  a une structure naturelle de groupe commutatif.

Si de plus  $A$  est commutatif alors  $\text{Hom}_{A\text{-mod}}(M, N)$  a une structure de  $A$ -module

**Preuve**

Si  $\phi$  et  $\psi \in \text{Hom}_{A\text{-mod}}(M, N)$ , alors

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

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

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

Donc  $\phi + \psi \in \text{Hom}_{A\text{-mod}}(M, N)$ , donc la proposition est prouvée.  $\square$

**Théorème 55**

Soit  $M$  un  $A$ -module. L'ensemble  $\text{End}_{A\text{-mod}}(M)$  des endomorphismes de  $M$  est un sous-anneau de  $(\text{End}, +, \circ)$  dont le groupe des unités est

$\text{Aut}_{A\text{-mod}}(M)$  ;

de plus, si  $A$  est commutatif,  $\text{End}_{A\text{-mod}}(M)$  possède une structure naturelle de  $A$ -module qui en fait une  $A$ -algèbre.

$\text{End}_{A\text{-mod}}(M)$  est appelée l'algèbre des endomorphismes du  $A$ -module  $M$

**Preuve**

On utilise le critère du sous-anneau.

On sait que  $\phi \circ \psi + \Phi \in \text{End}_{Gr}(M)$ , et on doit vérifier que c'est compatible avec la loi de multiplication externe  $*$

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

## 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 élément 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 rationnelles à coefficients dans  $\mathbb{R}$

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

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

### Proposition 57

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

$$\phi : K \hookrightarrow B$$

### Preuve

Soit  $\phi : K \rightarrow B$  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  $\phi$  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.  $\nmid$

### 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 intègre.

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 intègre, alors il existe un corps  $K$  et un morphisme d'anneau injectif

$$\iota : A \hookrightarrow K$$

de sorte qu'on peut considérer  $A$  comme un sous-anneau de  $K$  en identifiant  $A$  à  $\iota(A) \subset K$  et tel que  $K$  a la propriété de minimalité suivante : pour tout corps  $K'$  et tout morphisme injectif

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

de sorte que  $A$  peut être identifiée à un sous-corps de  $K'$ , il existe un morphisme (nécessairement injectif)

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

prolongeant le morphisme  $\iota'$  (ainsi  $A$  et  $K$  peuvent être vus comme des sous-anneaux de  $K'$ )

**Definition 32**

On appelle ce corps  $K$  le corps des fractions de  $A$ .

**Exemple**

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

**Preuve**

Construisons  $K$ .

$A$  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.

- Symétrique : 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  $(a', b') \sim (a'', b'') \implies a.b' = a'.b = a''.b' = a'.b' = a''.b'$

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

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 classes 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  $A$  intègre.

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  $\frac{a}{b} \neq 0_K \iff a \neq 0_A$  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  $\iota$  est injectif. □

## 6.2 Caractéristique des Corps

$K$  un corps,

$$Can_K : \mathbb{Z} \rightarrow A$$

$$n \rightarrow n.1_K = n_K$$

$$\ker(Can_K) = p\mathbb{Z}, p \geq 0$$

### 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  $K$ .

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

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

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

On dispose d'un morphisme injectif

$$Can_K : \mathbb{Q} \hookrightarrow K$$

$$\frac{a}{b} \rightarrow \frac{a_K}{b_K}$$

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

**Lemme 61**

*Si  $\text{car}(K) > 0$ , alors  $\text{car}(K) = p$  est un nombre premier.*

**Preuve**

Si  $p = 1$ ,  $\ker \text{Can}_K = \mathbb{Z}$

$$\Rightarrow \text{Can}_K(1) = 1_K = 0_K \not\Leftarrow$$

Donc  $p \geq 2$ .

Soit une factorisation

$$p = q_1 \cdot q_2$$

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

$$0_K = \text{Can}_K(p) = \text{Can}_K(q_1 \cdot q_2) = \text{Can}_K(q_1) \cdot \text{Can}_K(q_2)$$

Comme  $K$  est intègre,  $\text{Can}_K(q_1) = 0_K$

$$q_1 \in \ker \text{Can}_K = p\mathbb{Z}$$

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

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

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

Donc  $p$  est premier. □

**Definition 34**

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

**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  $r \in \{0, \dots, p\}$  le reste de la division euclidienne de  $n$  par  $p$

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

$\mathcal{F}_p$  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 être un multiple de  $p$ , donc  $i-j \notin \ker \text{Can}_K$  Donc

$$(i-j)_K = i_K - j_K \neq 0_K \quad \square$$

**Lemme 63**

Un anneau commutatif intègre et fini est un corps

**Preuve**

exercice  $\square$

$\mathbb{F}$  est intègre 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  $\text{car}(K) = 0$  ou bien  $\mathbb{F}_p \subset K$  ( si  $\text{car}(K) = p > 0$ ) 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

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

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

**Definition 36**

Soit  $K$  un corps de caractéristique  $p$ , le morphisme d'anneau précédent s'appelle le morphisme de Frobenius ( ou simplement le Frobenius ) de  $K$  se note

$$\text{frob}_p : x \rightarrow x^p$$

**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 binôme de Newton

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

**Lemme 66**

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

$$p \mid \binom{p}{k}$$

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

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

**Exemple**

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

**Definition 40**

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

**Proposition 70 (Critere d'application linéaire)**

Une application entre espaces vectoriels  $\phi : V \rightarrow W$  est linéaire ssi

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

**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**

$\phi$  une application linéaire.  $\phi$  injective ssi

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

**Definition 41 (Notations)**

On notera

$$\text{Hom}_{K\text{-ev}}(V, W), \text{Isom}_{K\text{-ev}}(V, W), \text{Aut}_{K\text{-ev}}(V) = \text{GL}(V)$$

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

$$V^* := \text{End}_{K\text{-ev}}(V, K)$$

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

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

## 7.1 Familles génératrices

**Definition 43**

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

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

le sous-espace vectoriel engendré 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 )

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

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

$$\begin{aligned} \lambda(x + y) + (x' + y') &= \lambda x + \lambda y + x' + y' \\ &= (\lambda x + x') + (\lambda y + y') \in \{u + v, u \in X, v \in Y\} \end{aligned} \quad \square$$

**Definition 45 (Notations)**

Si  $X \cap Y = \{0\}$ , on dit que  $X$  et  $Y$  sont en somme directe et on écrit

$$X \oplus Y \subset V$$

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

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

Donc  $x - x' = y' - y = 0$

□

**Definition 46 (Famille génératrice)**

Soit  $V$  un  $K$ -ev. Un sous-ensemble  $\mathcal{F} \subset V$  est une famille génératrice si

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

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

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

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

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

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 linéaire, c'est à dire isomorphe à  $K^d$  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  $G = \{e_1, \dots, e_n\}$  une famille de vecteurs.

$$CL_G : K^d \rightarrow V$$

$$(x_1, \dots, x_d) \rightarrow x_1 e_1 + x_2 e_2 + \dots + x_d e_d$$

$CL_G$  est linéaire, suit du critère 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  $\mathcal{F} = \{e_1, \dots, e_d\} \subset V$  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  $\vec{x} = (x_1, \dots, x_n)$  ssi

$$\sum_i x_i e_i = 0$$

**Definition 49**

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

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

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

**Proposition 79**

Une famille à  $d$  éléments  $\mathcal{F} = \{e_1, \dots, e_d\} \subset V$  est liée si et seulement si il existe  $i \in \{1, \dots, d\}$  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  $(x_1, \dots, x_d) \neq 0_V$  tel que

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

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

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

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

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

Donc

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

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

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

Donc

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

□

**Theorème 80**

Soit  $V$  un espace vectoriel non-nul de dimension  $d$  et  $\mathcal{F} = \{v_1, \dots, v_f\} \subset V$  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  $\mathcal{F} = \{v_1, \dots, v_f\} \subset V = K.e$  avec  $v_i = x_i.e$   $f \geq 2$  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  $\mathcal{F} = \{v_1, \dots, v_f\} \subset V$  avec  $f \geq d + 1$ , on veut montrer que  $\mathcal{F}$  est liée.

Soit  $G = \{e_1, \dots, e_d\}$  une famille génératrice de  $V$  pour  $i = 1, \dots, f$

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

avec  $x_{i,j} \leq d$  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 :  $i \leq f$

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

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

Posons

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

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

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

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  $v'_1$

$$v'_1 = y_2 v'_2 + \dots + y_{f-1} v'_{f-1}$$

Or

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

Donc

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

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

### Corollaire 81

$$\dim K^d = d$$

### Preuve

On sait que pour  $K^d$ , la base canonique

$$B_d^0 = \{e_1^0, \dots, e_d^0\}$$

est génératrice, donc  $\dim K^d \leq d$ .

Est libre :  $d \leq \dim K^d \quad \square$



### 7.3 Bases

#### Definition 50

Soit  $V$  un espace vectoriel de dimension finie. Une famille  $\mathcal{B} = \{e_1, \dots, e_d\}$  est une base de  $V$  si l'une des conditions équivalentes suivantes est vérifiée :

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

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

est un isomorphisme.

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

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

#### 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 libre 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  $G$ .

$B$  est libre ( et est donc une base)

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

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

Mais alors

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

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

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

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  $\alpha$ .

Soit  $\mathcal{B}'$  une famille génératrice contenant  $\alpha$  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  $\alpha$  ( et même contenue dans  $\alpha \cup \mathcal{B}$ )

Si  $\alpha = \mathcal{B}'$ , on a fini :  $|\alpha| = |\mathcal{B}'|$  et  $\alpha$  est une base.

Quitte à renuméroter  $\mathcal{B}'$  on peut supposer que

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

Soient  $x_1, \dots, x_d' \in K$  tel que

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

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

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

Mais comme  $\alpha$  est libre  $\Rightarrow$

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

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

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

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

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

est génératrice et contient  $\alpha$

**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  $\alpha$  qui est libre.

Soit  $\alpha \subset W$  libre et de cardinal maximal ( parmi les familles libres) On va montrer que  $\alpha$  est génératrice de  $W$  ( et  $\alpha$  sera une base de  $W$ ) .

Si  $\alpha$  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  $|\alpha| = \dim V$ ,  $\alpha$  est libre dans  $V$  et de taille  $\dim V$ .

Donc  $\alpha$  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

$$\text{Vect}(G) = V$$

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

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

**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

$$x_1 e_1 + \dots + x_d e_d = 0_V \iff x_1 = \dots = x_d = 0_K$$

**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 existe 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  $\phi : V \rightarrow W$  une application linéaire avec  $V$  de dimension finie. Soit  $G = \{e_1, \dots, e_g\} \subset V$  une famille génératrice, alors*

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

*est une famille génératrice de  $\text{Im}(\phi)$  et on a*

$$\dim \text{Im} \phi \leq \dim V$$

**Définition 54**

*Soit  $\phi : V \rightarrow W$  une application linéaire. Le rang de  $\phi$  est la dimension de  $\text{Im} \phi$  :*

$$\text{rg}(\phi) = \dim \text{Im} \phi$$

**Preuve**

*Soit  $G = \{e_1, \dots, e_g\} \subset V$  génératrice et soit*

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

*Soit  $w \in \text{Im} \phi$  on veut montrer que  $w$  est  $CL(\phi(G))$ .*

*Comme  $w \in \text{Im} \phi$ ,  $w = \phi(v)$ ,  $v \in V$  et comme  $G$  est génératrice de  $V$*

$$v = x_1 e_1 + \dots + x_g e_g, \quad x_i \in K$$

*Donc*

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

*Soit  $G = B$  une base, alors*

$$|B| = \dim V$$

et

$$\dim \operatorname{Im} \phi(V) \leq |\phi(B)| \leq |B| \quad \square$$

**Corollaire 89**

*Une application linéaire envoyant une base sur une base est un isomorphisme*

**Preuve**

$$\phi : V \rightarrow W$$

$B$  une base de  $V$  et on suppose que

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

Alors  $\phi : V \simeq W$ .

$\phi$  est surjective car  $\phi(B)$  engendre l'image de  $\phi$  et comme  $\phi(B)$  est une base de  $W$

$$\langle \phi(B) \rangle = \operatorname{Im} \phi = W$$

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

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

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

Mais car  $\{\phi(e_1), \dots, \phi(e_d)\}$  est libre dans  $W$ .

Donc  $x_1 = \dots = x_d = 0 \Rightarrow v = 0$   $\square$

**Théorème 90 (Le théorème noyau-image)**

Soit  $\phi : V \rightarrow W$  une application linéaire avec  $V$  de dimension finie. On a

$$\dim V = \dim \ker \phi + \dim \operatorname{Im} \phi$$

**Preuve**

Soit  $\{e_1, \dots, e_k\}$  une base de  $\ker \phi$  ( $k \leq \dim V$ )

Soit  $\{f_1, \dots, f_r\}$  une base de  $\operatorname{Im} \phi$  ( $r \leq \dim V$ ), alors

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

On va montrer que

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

c'est une base de  $V$ . Alors

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

Montrons que la famille est libre :

Soit  $x_1, \dots, x_k, x'_1, \dots, x'_r \in K$  tel que

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

On a

$$\begin{aligned}\phi(0_V) &= \phi(x_1 e_1 + \dots + x'_r e'_r) = 0_W \\ &= x_1 \phi(e_1) + \dots + x'_r \phi(e'_r) \\ &= x'_1 f_1 + \dots + x'_r f_r \Rightarrow x'_1 = \dots = x'_r = 0\end{aligned}$$

Il reste

$$0_V = x_1 e_1 + \dots + x_k e_k$$

Donc  $\{e_1, \dots, e_k\}$  est linre  $\Rightarrow x_1 = \dots = x_k = 0_K$

Montrons que  $\{e_1, \dots, e_k, e'_1, \dots, e'_r\}$  est génératrice.

Soit  $v \in V$  on veut montrer que  $v$  est cl de la famille.

$$\begin{aligned}\phi(v) &= \underbrace{w}_{\in \text{Im}\phi} = x'_1 f_1 + \dots + x'_r f_r \\ &= x'_1 \phi(e'_1) + \dots + x'_r \phi(e'_r) \\ &= \phi(x'_1 e'_1 + \dots + x'_r e'_r)\end{aligned}$$

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

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

Donc

$$v - v' = x_1 e_1 + \dots + x_k e_k$$

donc

$$= x_1 e_1 + \dots + x_k e_k + x'_1 e'_1 + \dots + x'_r e'_r$$

□

## Lecture 13: Applications lineaires

Tue 27 Oct

### Corollaire 91

Soit  $\phi : V \rightarrow W$  une application lineaire entre espaces de dimension finie

- Si  $\phi$  est injective et  $\dim W = \dim V$ , alors  $\phi$  est bijective
- Si  $\phi$  est surjective et  $\dim W = \dim V$ , alors  $\phi$  est bijective

### Preuve

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

$$\dim V = \dim \ker \phi + \dim \text{Im}\phi = \dim \text{Im}\phi = \dim W$$

De même, si  $\phi$  surjective, alors

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

Donc on a

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

□

Donc  $\dim \ker \phi = 0$  et donc  $\phi$  est injective  $\Rightarrow$  bijective.

**Corollaire 92**

*Deux espaces vectoriels de dimension finie sont isomorphes si et seulement si ils ont même 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  $\text{Im} \phi = W$ , on a alors*

$$\dim V = \dim \ker \phi + \dim \text{Im} \phi = 0 + \dim W \quad \square$$

**7.5 Formes linéaires**

$$l : V \rightarrow K$$

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  $l : V \rightarrow K, l \neq \underline{0}_K$ , 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

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

donné par

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

et que

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

**Théorème 93**

*Si  $V$  et  $W$  sont de dimension finie, alors  $\text{Hom}_K(V, W)$  est de dimension finie*

$$\dim(\text{Hom}_K(V, W)) = \dim V \cdot \dim W$$

**Preuve**

On va montrer que

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

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

$$\text{eval}_B : \text{Hom}(V, W) \rightarrow W^{\dim V}$$

$$\phi \rightarrow (\phi(e_1), \phi(e_2), \dots, \phi(e_d))$$

On va montrer que  $\text{eval}_B$  est un isomorphisme d'espaces vectoriels.  
 $\text{eval}_B$  est linéaire :

$$\text{eval}_B(\lambda\phi + \psi) = (\lambda\phi(e_1) + \psi(e_1), \dots, \lambda\phi(e_d) + \psi(e_d)) = \lambda\text{eval}_B(\phi) + \text{eval}_B(\psi)$$

Montrons que  $\text{eval}_B$  est injective, si

$$\text{eval}_B(\phi) = (0_W, \dots, 0_W)$$

Implique

$$\forall v \in V \quad v = x_1 e_1 + \dots + x_d e_d$$

Donc

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

Donc  $\phi$  injectif.

Soit  $(w_1, \dots, w_d) \in W^{\dim V}$  et soit  $\phi$  l'application définie pour tout  $v \in V$  par

$$\phi(v) = x_1 w_1 + \dots + x_d w_d$$

si  $v = x_1 e_1 + \dots + x_d e_d$ .

C'est bien défini car  $B$  est une base de  $V$  et la combinaison linéaire qui représente  $v$  est unique.

Alors  $\phi$  est linéaire et

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

Donc  $\text{eval}_B$  est surjective et donc bijective □

**Remarque**

$$\text{eval}_B : \text{Hom}(V, W) \simeq W^{\dim V}$$

dépend du choix de  $B$ .

**Remarque**

Si on choisit  $B'$  une base de  $W$ ,

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

et donc on obtient un isomorphisme

$$\text{Hom}_K(V, W) = (K^{d'})^d$$



## 7.7 Formes linéaires et dualité

### Definition 55

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

$$V^* = \text{Hom}(V, K)$$

et on l'appelle le dual de  $V$

Comme  $\dim K = 1$ , on a

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

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

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

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

$$\text{eval}_B : l \rightarrow (l(e_1), \dots, l(e_d)) \in K^d$$

### Definition 56

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

$$e_i^* = \text{eval}_B^{-1}(e_i^0)$$

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

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

### Preuve

Calculons  $e_1^* = \text{eval}_B^{-1}((1, 0, 0 \dots))$

Donc

$$\text{eval}_B(e_1^* = (1, 0, 0 \dots)) = (e_1^*(e_1), \dots)$$

□

idem pour  $e_i^*$ .

### Remarque

L'application  $\text{eval}_B$  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  $\phi : V \rightarrow W$  à partir de  $\phi$ , on construit (canoniquement) une application

$$\phi^* : W^* \rightarrow V^* \text{ (application linéaire duale de } \phi \text{)}$$

Soit  $l' \in W^* \rightarrow \phi^*(l')$  donné par

$$\phi^*(l')(v) = l'(\phi(v)) = ' \circ \phi$$

$\phi^*$  est linéaire et

$$\bullet^* : \phi \in \text{Hom}(V, W) \rightarrow \phi^* \in \text{Hom}(W^*, V^*)$$

est linéaire.

**7.8 Représentation paramétrique d'un sev cartésienne**

$W \subset V$ , Soit  $\{e_1, \dots, e_{d'}\}$  une base de  $W$ , alors tout vecteur de  $W$  s'écrit

$$w = x_1 e_1 + \dots + x_{d'} e_{d'}$$

Alors

$$W = \{w = x_1 e_1 + \dots\}$$

On a alors une représentation paramétrique de tout vecteur

$$w \in W, \quad w = x_1 e_1 + \dots + x_{d'} e_{d'}$$

de paramètre  $x_1, \dots, x_{d'}$ .

Note : Il n'est pas nécessaire que  $\{e_1, \dots, e_{d'}\}$  soit une base, il suffit que ce soit une famille génératrice de  $W$ .

Représentation cartésienne

**Proposition 98**

Soit  $W \subset V$  un sev. Il existe  $d_V - d_W$  formes linéaires

$$\mathcal{L}_W^* = \{l_1, \dots, l_{d_v - d_w}\} \subset V^*$$

linéairement indépendantes (ie tq  $\mathcal{L}_W^*$  soit libre) telles que

$$W = \{v \in V, l_1(v) = \dots = l_{d_v - d_w}(v) = 0\}$$

De manière équivalente,  $W = \ker \phi_{\mathcal{L}_W^*}$  avec

$$\phi_{\mathcal{L}_W^*} : v \in V \rightarrow (l_1(v), \dots, l_{d_v - d_w}(v)) \in K^{d_v - d_w}$$

**Preuve**

Soit  $W \subset V$  et soit  $\{e_1, \dots, e_{d'}\}$  une base de  $W$ .

Il existe  $e_{d'+1}, \dots, e_d \in V$  tel que

$$\{e_1, \dots, e_d\}$$

forme une base de  $V$ .

$W$  est l'ensemble des vecteurs  $V$  dont les coordonnées suivant les vecteurs  $e_{d'+1}, \dots, e_d$  sont nulles.

$$v = x_1 e_1 + \dots + x_{d'} e_{d'} + \dots + x_d e_d$$

Donc

$$W = \{v \in V \mid e_{d'+1}^*(v) = \dots = e_d^*(v) = 0_K\} \quad \square$$

**7.9 Une base de  $\text{Hom}_k(V, W)$** 

Soit  $B = \{e_1, \dots, e_d\} \subset V$  et  $B^*$  la base duale

$$B' = \{f_1, \dots, f_{d'}\} \mid i \leq d' = \dim W \quad j \leq d = \dim V$$

Alors

$$e_{ij} : V \rightarrow W$$

$$v \rightarrow e_j^*(v) \cdot f_i$$

On dispose de  $d \cdot d'$  applications  $e_{ij}$

**Lemme 99**

L'application  $e_{ij} : V \rightarrow W$  est linéaire, de rang 1, d'image  $K \cdot f_i$  et de noyau

$$\ker e_{ij} = \langle (\cdot) B - \{e_j\} \rangle$$

L'hyperplan vectoriel engendré par les vecteurs de la base  $B$  moins le vecteur  $e_j$

**Preuve**

$e_{ij}$  est linéaire car

$$e_j^* : V \rightarrow K$$

est linéaire.

Vérification simple avec critère.

On a

$$\text{Im}(e_{ij}) = \text{Im}(e_j^*) \cdot f_i = K \cdot f_i$$

de dimension 1.

$$\ker e_{ij} = \{v \in V \mid \text{tel que } e_j^*(v) \cdot f_i = 0_W\}$$

mais comme  $f_i \neq 0_W$  ( car  $f_i$  fait partie d'une base).

$$e_j^*(v) \cdot f_i = 0_W$$

si et seulement si

$$e_j^* = 0_K$$

Donc

$$\ker e_{ij} = \{v \in V \text{ tel que } e_j^*(v) = 0_K\} \quad \square$$

### Theorème 100

La famille d'applications linéaires

$$B_{B,B'} = \{e_{ij}, i \leq d', j \leq d\} \subset \text{Hom}(V, W)$$

forme une base de  $\text{Hom}(V, W)$

### Preuve

$B_{B,B'}$  est de taille  $d \cdot d' = \dim \text{Hom}(V, W)$  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

$$\sum_{i=1}^{d'} \sum_{j=1}^d m_{ij} e_{ij} = 0_W$$

On veut montrer que  $m_{ij} = 0_K$ .

$$\begin{aligned} & \left( \sum_{i,j} m_{ij} e_{ij} \right) (e_k) \\ &= \sum_i \sum_j m_{ij} e_{ij}(e_k) \\ &= \sum_i \sum_j m_{ij} e_j^*(e_k) \cdot f_i \\ &= \sum_{i=1}^{d'} m_{ik} f_i = 0 \end{aligned} \quad \square$$

Donc  $m_{ik} = 0$  car les  $f_i$  forment une famille libre.

### Proposition 101

Soit  $\phi : V \rightarrow W$  une application linéaire et  $(m_{ij})$  les coordonnées dans la base  $B_{B,B'}$ . Alors pour  $k = 1, \dots, d$  les

$$m_{i,k}$$

sont les coordonnées de  $\phi(e_k)$  dans la base  $B'$

### Preuve

On a

$$\begin{aligned} e_{ij}(e_k) &= \sum_{i \leq d'} \sum_{j \leq d} m_{ij} e_j^*(e_k) \cdot f_i \\ &= \sum_{i \leq d'} m_{ik} \cdot f_i \end{aligned}$$

### 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

$$\phi(v) = \phi\left(\sum_{k=1}^d x_k e_k\right) = \sum_{k=1}^d x_k \phi(e_k) = \sum_{k=1}^d x_k \phi(e_k) = \sum_{k=1}^d x_k \sum_{i \leq d'} m_{ik} f_i = \sum_{i \leq d'} \left(\sum_{k=1}^d m_{ik} x_k\right) f_i$$

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

$$\phi : U \rightarrow V, \psi : V \rightarrow W \text{ et } \psi \circ \phi : U \rightarrow W$$

Soit

$$B = \{e_k, k \leq d\}, B' = \{f_j, j \leq d'\}, B'' = \{g_i, i \leq d''\}$$

et finalement

$$B_{B,B'} = \{e_k^* \cdot f_j\}, B_{B',B''} = \{f_j^* \cdot g_i\}, B_{B,B''} = \{e_k^* \cdot g_i\}$$

### Theorème 103

Soient  $(n_{jk})_{j \leq d', k \leq d}$  les coordonnées de  $\phi$  dans la base  $B_{B,B'}$  et  $(m_{ij})_{i \leq d'', j \leq d'}$  les coordonnées de  $\psi$  dans la base  $B_{B',B''}$ . Alors les coordonnées  $(l_{ik})_{i \leq d'', k \leq d}$  de  $\psi \circ \phi$  dans la base  $B_{B,B''}$  sont données par :

$\psi \circ \phi$  dans la base  $B_{B,B''}$  sont donnees par

$$l_{ik} = \sum_{j=1}^{d'} m_{ij} \cdot n_{jk}$$

**Preuve**

$$\phi = \sum_{j \leq d'} \sum_{k \leq d} n_{jk} e_k^* \cdot f_j$$

et

$$\psi = \sum_{j \leq d'} \sum_{i \leq d''} m_{ij} f_j^* \cdot g_i$$

On veut calculer

$$\psi \circ \phi(e_k) = \sum_{i \leq d''} l_{ik} g_i$$

On voit que

$$\begin{aligned} \phi(e_k) &= \sum_{j \leq d'} \sum_{k' \leq d} n_{jk'} e_{k'}^*(e_k) f_j = \sum_{j \leq d'} n_{jk} f_j \\ &= \psi(\phi(e_k)) = \psi\left(\sum_{j \leq d'} n_{jk} f_j\right) \\ &= \sum_{j \leq d'} n_{jk} \psi(f_j) \\ &= \sum_{j \leq d'} n_{jk} \sum_{i \leq d''} m_{ij} g_i \\ &= \sum_{i \leq d''} \left( \sum_{j \leq d'} n_{jk} m_{ij} \right) g_i \\ &= \sum_{i \leq d''} \left( \sum_{j \leq d'} m_{ij} n_j \right) g_i \end{aligned}$$

## 8 Matrices

On a donc défini l'application linéaire

$$CL_{B_{B,B'}} : (m_{ij})_{i \leq d', j \leq d} \in K^{d' \times d} \mapsto \phi = \sum_{i \leq d'} \sum_{j \leq d} m_{ij} e_{ij} \in \text{hom}(V, W)$$

**Definition 58**

Les système 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  $B_{B,B'} \subset \text{hom}(V, W)$  la base de  $\text{hom}(V, W)$  associee. L'application reciproque  $Cl_{B_{B,B'}}^{-1}$  sera également notee

$$Mat_{B',B} : \text{hom}(V, W) \rightarrow M_{d' \times d}(K)$$

Explicitement, si on a la décomposition  $\phi = \sum_{i \leq d'} \sum_{j \leq d} m_{ij} e_{ij}$ , alors on a

$$Mat_{B',B}(\phi) = (m_{ij}(\phi))_{i \leq d', j \leq d} = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1d} \\ \vdots & \dots & \dots & \dots \\ m_{d'1} & m_{d'2} & \dots & m_{d'd} \end{pmatrix}$$

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 :

$$(m_{ij}) + (n_{ij}) = (m_{ij} + n_{ij})_{i \leq d', j \leq d}$$

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

$$L = (l_{ik})_{i \leq d'', k \leq d} = \left( \sum_{j=1}^{d'} m_{ij} n_{jk} \right)_{i \leq d'', k \leq d} \in M_{d'' \times d}(K)$$

**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  $\phi : V \rightarrow W$  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  $\leq \min(d, d')$ .

rang de  $M =$  dimension d'un espace engendré par  $d$  vecteurs

Sa dimension sera toujours  $\leq d$ .

Cet espace est contenu dans  $Col_{d'}(K)$  qui est de  $\dim d'$



### 8.3 Transposition

Soient  $\phi : V \rightarrow W$  et  $\phi^* : W^* \rightarrow V^*$ .

#### Theorème 107

Soit  $(m_{ij}) = \text{Mat}_{B,B'}(\phi)$ ,  $(m_{ij}^*) = \text{Mat}_{B',B}(\phi^*)$ . Alors on a

$$m_{ij} = m_{ji}^*$$

On dit que  $\text{mat}(\phi^*)$  est la transposée de  $\text{mat}(\phi)$  et on la note  ${}^t\text{mat}(\phi)$

#### 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 :  ${}^t({}^tM) = M$
3. Multiplicativité : pour deux matrices  $M$  et  $N$ , alors on a

$${}^t(M.N) = {}^tN.{}^tM$$

#### Preuve

Il suffit de montrer que

$$\phi : U \mapsto V \quad \psi : V \rightarrow W$$

et

$$\psi \circ \phi : U \mapsto W$$

Alors

$$(\psi \circ \phi)^* = \phi^* \circ \psi^*$$

On a

$$(\psi \circ \phi)^* : l'' \rightarrow l'' \circ \psi \circ \phi = (l'' \circ \psi) \circ \phi = \phi^*(l'' \circ \psi) = \phi^*(\psi^*(l'')) \quad \square$$

#### Proposition 109

Soit  $M \in M_{d' \times d}(K)$  on a

$$\text{rg}(M) = \text{rg}({}^tM).$$

Soit  $\varphi \in \text{Hom}(V, W)$ , on a

$$\text{rg}(\phi) = \text{rg}(\phi^*)$$

**Preuve**

Soit une base  $B = \{e_1, \dots, e_d\} \subset V$ , alors on a

$$\phi(B) = \{\phi(e_1), \dots, \phi(e_d)\}$$

engendre  $\phi(V)$  si  $\dim \phi(V) = r = \text{rg} \phi$  on peut extraire de  $\phi(B)$  une base de  $\phi(V)$ .

Supposons que cette base soit

$$\{\phi(e_1) = f_1, \dots, \phi(e_r) = f_r\} \subset W$$

C'est une famille libre de  $W$ .

On peut la compléter pour former une base de  $W$  :

$$B' = \{f_1, \dots, f_r, f_{r+1}, \dots, f_{d'}\}$$

On regarde

$$B' = \{f_1, \dots, f_r, f_{r+1}, \dots, f_{d'}\}$$

et on lui associe

$$B'^* = \{f_1^*, \dots, f_{d'}^*\}$$

On considère donc

$$\phi^* : W^* \rightarrow V^*$$

On a

$$\text{rg} \phi^* = \dim \phi^*(W^*) = \dim \langle \phi^*(f_1^*), \dots \rangle$$

On va montrer que

$$\{\phi^*(f_1^*), \dots\} \subset V^*$$

est libre.

Soient  $x_1, \dots, x_r \in K$  tel que

$$x_1 \phi^*(f_1^*) + \dots = 0_K$$

On a que  $\forall j \leq d$  et  $\forall e_j \in B$

$$\begin{aligned} & (x_1 \phi^* + \dots)(e_j) \\ &= x_1 \phi^*(f_1^*) e_j + \dots = x_j f_j^*(\phi(e_j)) = x_j f_j^*(f_j) = x_j \end{aligned}$$

Et donc

$$\text{rg}(\phi^*) \leq \text{rg}(\phi)$$

Donc pour toute matrice  $M$ , on a  $rg({}^t M) \geq rg(M)$ .

Donc en particulier

$$rg({}^t({}^t(M))) \geq rg({}^t(M))$$

Et donc

$$rg(M) = rg({}^t M)$$

Et donc

$$rg(\phi) = rg({}^* \phi) \quad \square$$

## 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 neutre 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

$$\begin{aligned} \text{End}(V) = \text{Hom}(V, W) &\rightarrow M_d(K) \\ \phi &\rightarrow \text{mat}_{B,B}(\phi) \end{aligned}$$

$\text{mat}_{B,B}(\bullet)$  est un isomorphisme de  $K$ -ev mais c'est également un isomorphisme d'anneaux.

On a

$$\text{mat}_{B,B}(\psi \circ \phi) = \text{mat}_{B,B}(\psi) \cdot \text{mat}_{B,B}(\phi)$$

## 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  $\text{Id}_d$

**Theorème 111**

Soit  $V$  de dimension finie  $d$  et  $B$  une base de  $V$ , l'application

$$\text{Mat}_B : \text{End}(V) \mapsto M_d(K)$$

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

$\text{End}(V)^\times = \{\phi \in \text{End}(V) \text{ qui sont bijectifs et donc inversible pour la composition} \}$

On note

$$M_d(K)^\times = GL_d(K) = \text{le groupe lineaire de } K^d$$

Donc

$$\begin{aligned} \text{mat}_B : GL(V) &\mapsto GL_d(K) \\ \phi &\mapsto \text{mat}_B(\phi) \end{aligned}$$

**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  $\text{Col}(M)$  forme une famille libre.

**Preuve**

Si  $M = \text{mat}_B(\phi) \in \text{End}(V)$ .

Si  $\text{Col}(M)$  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  $\phi$  est surjective et injective.  $\square$

**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

$$\forall M, N \in GL_d(K) \quad {}^t M^{-1} = {}^t M^{-1}, {}^t (M.N) = {}^t N. {}^t M$$

**Preuve**

Si  $M$  est inversible

$$\exists N = M^{-1}$$

tel que

$$M.M^{-1} = Id \quad M^{-1}M = Id \quad \square$$

On utilise la formule de transposition sur  $M.M^{-1}$

**8.6 Changement de Base**

Soient  $B \subset V$  et  $B' \subset W$  et  $\phi : V \rightarrow W$ .

A nouveau, supposons que  $B_n \subset V$  et  $B'_n \subset W$ , avec

$$\phi \rightarrow mat_{B'_n B_n}(\phi) = M_n$$

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

$$Mat_{B'_n B_n}(\phi) = Mat_{B'_n B'}(\text{Id}_w) Mat_{B' B}(\phi). Mat_{B, B_n}(\text{Id}_v)$$

**Preuve**

On a

$$\phi = \text{Id}_w \circ \phi \circ \text{Id}_v$$

On utilise le calcul des matrices associee a des compositions d'applications lineaires dans ces bases convenables.

On a

$$\phi : V \rightarrow V \rightarrow W$$

avec

$$mat_{B' B'}(\phi \circ \text{Id}_v) = mat_{B' B}(\phi) mat_{B B_n}(\phi) \quad \square$$

**Definition 63 (Matrice de Passage)**

$M_{BB_n} = M_{BB_n}(\text{Id}_v) =$  la matrice exprimant les coordonnees de  $\left\{ \text{Id}_v(e_{nj}j \leq d) \right\} = B_n$

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

$$Mat_{BB_1} Mat_{BB_1} = Id_d$$

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

$$Mat_{BB_2} = Mat_{BB_1} Mat_{B_1B}$$

### Preuve

Consequence directe de la formule de la matrice associee a la composition de 2 applications lineaires appliquees a

$$\phi = Id_V \quad \psi = Id$$

□

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

$$mat_{B_n B} = mat_{BB_n}^{-1}$$

Donc la formule de changement de base de  $\phi$ .

$$mat_{B_n B_n}(\phi) = mat_{BB_n}^{-1} mat_{BB}(\phi) mat_{BB_n}$$

Si la base de depart egal a la base d'arrivee, on le note

$$mat_{B_n}(\phi) = mat_{B_n B} mat_B(\phi) mat_{B_n B}^{-1}$$

### 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 équivalents 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 linéaire  $\phi : V \rightarrow W$  telles que

$$M = \text{mat}_{B'B}(\phi)N = \text{mat}_{B'_n B_n}(\phi)$$

**Preuve**

Si  $M = \text{mat}_{B'B}(\phi)$  et  $N = \text{mat}_{B'_n B_n}(\phi)$ , alors

$$N = \text{mat}_{B'_n B'} M \cdot \text{mat}_{B B_n} \quad \square$$

**Proposition 119**

Si  $M$  et  $N$  sont équivalents alors

$$\text{rg}(M) = \text{rg}(N)$$

**Preuve**

$$\text{rg}(M) = \text{rg}(\phi) = \text{rg}(N) \quad \square$$

**Remarque**

La relation “être équivalent” est une relation d’équivalence.

**8.7 Conjugaison****Définition 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’algèbre  $M_d(K)$

**Preuve**

$$C.(\lambda M + N).C^{-1} = \lambda Ad(C).M + Ad(C).N$$

*Multiplicativité*

$$CMNC^{-1} = CM \text{Id} N C^{-1} = CMC^{-1}CNC^{-1}$$

*Identité*

$$C^{-1}CMC^{-1}C = M \quad \square$$

**Definition 66 (Application Adjointe)**

$$Ad : C \in GL_d(K) \rightarrow Ad(C) \in GL(M_d(K))$$

*Ad est un morphisme de groupe.*

*On le verifie...*

On donne un nom a  $\mathfrak{Z}(Ad) = Ad(GL_d)$ , 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*

$$\ker Ad = K^\times \text{ Id}$$

**Preuve**

*Si  $C = \lambda \cdot \text{Id}$ , avec  $\lambda \neq 0$ ,  $\lambda \in K^\times$ , alors*

$$C^{-1} = \lambda^{-1} \text{ Id}$$

*Donc*

$$CMC^{-1} = M$$

*Donc*

$$K^\times \text{ Id} \subset \ker Ad(\bullet)$$

*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  $M \rightarrow [C, M]$  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)**

$$E_{ij} = \text{mat}_{B_0} E_{ij}$$

*Donc*

$$E_{ij}(v) = e_j^* \cdot e_i$$

*Donc*

$$E_{ij}E_{kl}(v) = E_{ij}(E_l^*(v)e_k) = e_l^*(v)E_{ij}(e_k) = e_l^*(v)e_j^*(e_k)e_i$$

$$\text{Or } e_j^*(e_k) = \delta_{jk}.$$

*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*

$$\begin{aligned} E_{ij} \cdot C &= E_{ij} \left( \sum_{k,l} c_{kl}E_{kl} \right) \\ &= \sum_{k,l} c_{kl}E_{ij}E_{kl} \\ &= \sum_{k,l} c_{kl}\delta_{jk}E_{il} \\ &= \sum_{l \leq d} c_{jl}E_{il} \end{aligned}$$

*De meme*

$$\begin{aligned} C \cdot E_{ij} &= \sum_{k,l \leq d} c_{kl}E_{kl}E_{ij} \\ &= \sum_{k,l \leq d} c_{kl}\delta_{li}E_{kj} \\ &= \sum_{k \leq d} c_{ki}E_{kj} \end{aligned}$$

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.  $\square$

### Definition 67

On dit que deux matrices  $M, N$  sont semblables ou conjuguées 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

$$M = \text{Id } M \text{Id}^{-1}$$

— Symmetrique si  $N = CMC^{-1}$

$$M = C^{-1}NC$$

— Transitive

$$N = CMC^{-1} \text{ et } O = DND^{-1}$$

Alors

$$O = DCMC^{-1}D^{-1} = (DC)M(DC)^{-1} \quad \square$$

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  $\phi \in \text{End}(V)$  tel que

$$M = \text{mat}_B \phi$$

et

$$N = \text{mat}_{B_n} \phi$$

## 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 engendré par  $\text{Id}$  et  $I$

$$\mathbb{C} = \mathbb{R} \cdot \text{Id} + \mathbb{R} \cdot I$$

### Theorème 126

L'espace des nombres complexes est de dimension 2 et  $\{\text{Id}, I\}$  en forme une base.

De plus  $\mathbb{C}$  est une sous-algèbre commutative de  $M_2(\mathbb{R})$  et est en fait un corps. Le corps des nombres réels s'injecte dans  $\mathbb{C}$  via l'application

$$x \in \mathbb{R} \mapsto x \cdot \text{Id} \in \mathbb{C}$$

(les nombres réels s'identifient aux matrices scalaires).

### Preuve

La famille  $\{\text{Id}, I\}$  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

$$I^2 = -\text{Id}$$

En particulier,  $I$  est inversible et

$$I^{-1} = -I = {}^t I$$

Soit  $z = x \text{Id} + yI$  et  $z' = x' \text{Id} + y'I$ .

$$\begin{aligned} z \cdot z' &= xx' \text{Id} + x'yI + xy'I - yy' \text{Id} \\ &= (xx' - yy') \text{Id} + (xy' + yx')I \end{aligned}$$

Donc  $\mathbb{C}$  est un sous-anneau de  $M_2(\mathbb{R})$ .

Montrons que  $\mathbb{C}$  est un corps.

$\mathbb{C}$  est un corps :  $0_{\mathbb{C}} = 0_{\mathbb{C}} \neq \text{Id} = 1_{\mathbb{C}}$ .

Il reste à montrer que  $z \in \mathbb{C} \setminus 0_{\mathbb{C}}$  est inversible.

$$\begin{aligned} z^2 - 2xz &= (x^2 - y^2) \text{Id} + 2xyI - 2x(x \text{Id} + yI) \\ &= -(x^2 + y^2) \text{Id} \end{aligned}$$

Or  $z \neq 0_{\mathbb{C}} \iff (x, y) \neq (0, 0) \iff x^2 + y^2 \neq 0$ .

Et donc

$$\text{Id} = \frac{-1}{x^2 + y^2} (z^2 - 2xz)$$

Donc

$$z^{-1} = \frac{-1}{x^2 + y^2} (z - 2x)$$

On trouve, en développant que

$$\frac{1}{x^2 + y^2} {}^t z = z^{-1}$$

□

### Remarque

On peut identifier  $\mathbb{R}$  avec l'algèbre  $\mathbb{R} \text{Id}$  des matrices scalaires

$$x \in \mathbb{R} \rightarrow x \text{Id}$$

### Definition 69

Le réel  $x$  est appelé partie réelle de  $z$  et le réel  $y$  est la partie imaginaire de  $z$

$$x = \text{Re } z, y = \text{Im } z$$

Dans la notation matricielle, la transposition  $z \mapsto {}^t z$  envoie

$$x + iy \mapsto x - iy$$

Avec la notation simplifiée, on note

$$\bar{z} = x - iy$$

et s'appelle la conjugaison complexe de  $z$ . On a alors

$$z \cdot \bar{z} = x^2 + y^2 \geq 0$$

Le nombre  $(z \cdot \bar{z})^{\frac{1}{2}}$  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 propriétés suivantes

1. Les applications partie réelle et imaginaire sont linéaires
2. La conjugaison 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**

$\text{Re}, \text{Im}$  sont linéaires car ce sont les formes linéaires 1ère et 2ème coordonnées de  $z \in \mathbb{C}$  dans la base  $\{\text{Id}, I\}$ .

De même  $z \mapsto \bar{z}$  est linéaire.

etc

□

On remarque que  $|\bullet|$  est un morphisme de groupe multiplicatif

**Proposition 130**

On a un isomorphisme de groupes

$$\text{pol} : \mathbb{C}^\times \simeq \mathbb{R}_{>0} \times \mathbb{C}^{(1)}$$

donne par

$$z \in \mathbb{C}^\times \mapsto \text{pol}(z) = (|z|, \frac{z}{|z|})$$

**Preuve**

On a que

$$\frac{z.z'}{|z.z'|} = \left(\frac{z}{|z|}\right)\left(\frac{z'}{|z'|}\right)$$

et

$$\left|\frac{z}{|z|}\right| = \frac{(x^2 + y^2)^{\frac{1}{2}}}{|(x^2 + y^2)^{\frac{1}{2}}|}$$

□

Donc l'application  $\text{pol}$  est un morphisme.

## Lecture 19: Nombres Complexes 2

Tue 17 Nov

### Definition 70

$pol(z)$  s'appelle la décomposition polaire de  $z$ . Le premier terme  $|z|$  est le module et se note aussi  $\rho(z)$  et le second terme  $\frac{z}{|z|}$  est appelé argument complexe de  $z$  et on le note

$$\frac{z}{|z|} = e^{i\theta(z)}$$

Si on décompose l'argument complexe en partie réelle et imaginaire

$$\frac{z}{|z|} = e^{i\theta(z)} = c(z) + is(z)$$

On a donc

$c(z) \in [-1, 1]$  s'appelle le cosinus de  $z$

$s(z) \in [-1, 1]$  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'inversion

$$e^{i\theta(\frac{1}{z})} = c(z) - is(z)$$

— Formule de l'angle double

$$c(z^2) = c(z)^2 - s(z)^2, s(z^2) = 2s(z)c(z)$$

et plus généralement

— 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

$$k' = 2\left[\frac{k}{2}\right], \quad k = k' + \begin{cases} 0 & \text{si pair} \\ 1 & \text{si impair} \end{cases}$$

on obtient que

$$\begin{aligned} e^{i\theta(z^n)} &= (e^{i\theta(z)})^n = (c(z) + is(z))^n \\ &= \sum_{k'=0}^{\frac{n}{2}} C_n^{2k'} (-1)^{k'} c(z)^{n-2k'} s(z)^{2k'} + \sum_{k'=0}^{\frac{n}{2}} C_n^{2k'+1} (-1)^{k'} i c(z)^{n-(2k'+1)} s(z)^{2k'+1} \end{aligned}$$

### Theorème 132

Il existe un unique morphisme de groupe

$$\theta \in (\mathbb{R}, +) \mapsto \exp i\theta \in (\mathbb{C}^{\times}, \times)$$

qui est derivable et qui verifie

$$e^{i\bullet'}(0) = i$$

Ce morphisme est surjectif et son noyau est de la forme

$$\ker e^{i\bullet} = 2\pi \cdot \mathbb{Z}$$

On dit que  $\theta \rightarrow e^{i\theta}$  est derivable si les fonctions partie reelle et partie imaginaires sont derivables

$$(e^{i\theta})' = (\operatorname{Re} e^{i\theta})' + i(\operatorname{Im} e^{i\theta})'$$

Theoreme sans preuve.

### Definition 71

Soit  $z$  un nombre complexe de module 1.

L'argument de  $z$

$$\arg(z) = \theta \pmod{2\pi}$$

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.